Oracle® Cloud

Installing and Managing Oracle Management Cloud Agents

E89261-30
August 2021

Oracle Cloud Installing and Managing Oracle Management Cloud Agents,

E89261-30

Primary Author: Oracle Corporation

Contributors: Oracle Corporation

Contents

6 Agent Administration Tasks

Preface

The *Installing and Managing Oracle Management Cloud Agents* guide provides information on installing and managing Oracle Management Cloud agents.

Topics:

Audience

This document is intended for the administrators of Oracle Management Cloud.

Related Resources

For more information, see these Oracle resources:

- `http://cloud.oracle.com`
- About Application Performance Monitoring
- Getting Started with Oracle Infrastructure Monitoring Cloud Service
- About IT Analytics
- About Log Analytics

Conventions

This table describes the text conventions 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.
italic	Italic type indicates the 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

Before You Begin

As the administrator of an Oracle Management Cloud, you can deploy agents that can collect log and metric data from entities that you want to monitor and upload the data to Oracle Management Cloud.

Oracle Management Cloud Agent Terminology

Here are some of the common terms and basic concepts regarding agent deployment and lifecycle management.

Oracle Management Repository is a schema in an Oracle database where all the information collected by your **on-premises** Oracle Enterprise Manager Cloud Control Management Agents is stored. It consists of objects such as database jobs, packages, procedures, tables, views, tablespaces, and so on.

The **agent software ZIP file** is a ZIP file that contains a software installation script and software binaries for agent installation.

A **registration key** identifies the Oracle Cloud identity domain you have access to, and it is used to verify data sent by agents that are deployed on your on-premises hosts. You can use a single key for various agent installations. When you install an agent, you must provide the registration key value as a parameter. You can get the value of the key from the Agents screen of Oracle Management Cloud.

A **gateway** is an agent that acts as a channel between Oracle Management Cloud and data collector or cloud agents. Multiple data collector or cloud agents can communicate with Oracle Management Cloud through a single gateway.

A **data collector** is an agent that reads data from the customer's on-premises Oracle Management Repository and uploads it to Oracle Management Cloud. A data collector also collects log information from entities.

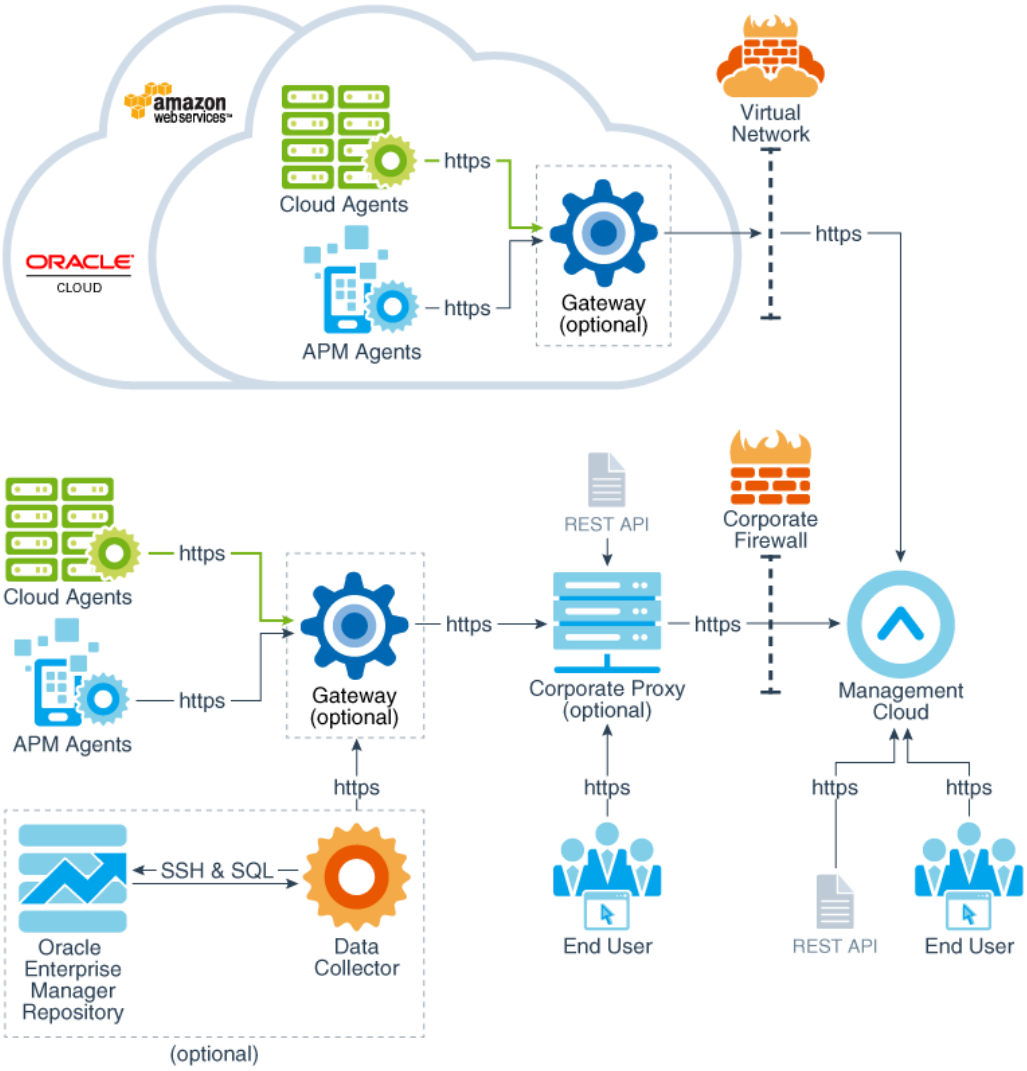
A **cloud agent** collects the host, entity, and log data from the host where you deploy the cloud agent. It can connect to Oracle Management Cloud directly or through a gateway.

On-premises **Oracle Enterprise Manager Agents** are software components deployed on monitored hosts. They are responsible for monitoring and managing all of the targets running on those hosts, communicating that information to the middle-tier Oracle Management Service.

A **security certificate**, or a **digital certificate**, is an electronic document that proves the ownership of a public key used for secure communication over a network.

Understand the Architecture of Oracle Management Cloud

This graphic shows all the Oracle Management Cloud components and their communication flow. The components communicate with each other using https protocol, except for the data collector that uses SSH and SQL to communicate with the OMR.



- Software or hardware resources as well as business objects whose properties, configuration, status, and performance are tracked and analyzed are known to Oracle Management Cloud as **entities**.
- The **cloud agents** monitor and collect data (for example, metrics, configuration information, and logs) from entities that reside on hosts, or on virtual hosts in a cloud. Typically, you deploy cloud agents on the same hosts as the entities of interest. In some cases, cloud agents can also collect metrics for entities on other hosts using various protocols that allow remote connections.
- A **gateway** is an optional agent type. Even though cloud agents can directly transmit their data over the Internet to Oracle Management Cloud, for security reasons, many companies do not have all of their machines accessible on Internet. Since, they have limited set of machines accessible on Internet through a proxy in most cases, installing a gateway on such machines helps route the data from a set of cloud agents to Oracle Management Cloud. A gateway is installed on a host that has Internet access to Oracle Management Cloud and can be reached by all hosts where cloud agents are deployed. All Oracle Management Cloud agents can use a common gateway.

- A **data collector** is an optional agent type. It reads data from an on-premises Oracle Enterprise Manager Cloud Control Management Repository (OMR) and/or collects log information from the Cloud Control managed entities. The repository data and logs are then uploaded to Oracle Management Cloud. A data collector can communicate directly with Oracle Management Cloud or through a gateway or a proxy server. A data collector is deployed on a host with SSH and SQL access to the OMR. You must deploy a data collector only if you have an existing Oracle Enterprise Manager setup and you want to extract data or logs from it. Typically, a data collector is installed on the OMR host because it adds only a small amount of overhead. However, you can choose to install a data collector on a different host as well. The data collected can be used by the IT Analytics and Log Analytics services.
- Typical data centers will have a corporate proxy server or a firewall configured. If your organization has a proxy server set up, then you must provide the proxy details when installing agents. This enables the agents to communicate to Oracle Management Cloud over a proxy or a firewall.

The various Oracle Management Cloud services use all, or a subset of the following components:

- If deployed, a **data collector** collects different types of data from the Oracle Management Repository, including target properties, configuration and performance metrics, or events.
- When **cloud agents** are installed on hosts, they automatically detect these hosts as monitored entities. To enable monitoring, add entities to cloud agents and those entities are monitored by that particular cloud agent. Cloud agents then collect status, performance, and configuration metrics for these entities. Depending on their configuration, cloud agents also collect logs from their entities.
- The **gateway** authenticates cloud agents in the client security service layer. If the cloud agents are found valid, then it receives the data or logs from the cloud agents.
- The **gateway** uploads the data and/or logs using a data pipeline using a proxy/firewall, if it is configured, and stores them in the distributed file system of the Oracle Management Cloud.
- Individual **Oracle Management Cloud Services** receive data from the common distributed file system, and save the data in their own service schemas.

Workflow for Installing Oracle Management Cloud Agents

Oracle Management Cloud Agent Installation Video

This short video shows you how to install an Oracle Management Cloud agent.

Video

Perform the following tasks to install Oracle Management Cloud agents.

Tasks	More Information
Review the prerequisites.	Before you start installing Oracle Management Cloud agents, ensure that you review the generic prerequisites. See Generic Prerequisites for Deploying Oracle Management Cloud Agents.

Tasks	More Information
Evaluate the type of Oracle Management Cloud agent you need to install.	You can install three different types of Oracle Management Cloud agents: Gateway, Data Collector or Cloud Agents. You need to decide which type of agent you want to install. See Understand the Architecture of Oracle Management Cloud.
Download the agent software install ZIP file.	The first step to deploy Oracle Management Cloud agents in your environment is downloading the agent software ZIP file. See Download the Oracle Management Cloud Agent Software.
Create or download a registration key.	You need a registration key to install a new agent. You can create a new one or you can also download an existing registration key. See Manage Registration Keys.
Customize the response file.	The agent installer reads parameters specific to your environment from a response file. Response files (`.rsp` files) are included in the agent software install ZIP file and, depending on the type of agent you are installing, you customize them per your environment. See Understanding Response Files.
Install a gateway (optional).	Determine if using a gateway is appropriate for your environment with Understand the Architecture of Oracle Management Cloud. If it is not, skip to the next task **Install a data collector**. If a gateway is appropriate, then determine which gateway installation is best for your environment. A gateway is service agnostic. After you install a gateway, it works for any Oracle Management Cloud service. See Install a Gateway.
Install a data collector (optional).	Determine if using a data collector is appropriate for your environment with Understand the Architecture of Oracle Management Cloud. If it is not, skip to the next task **Install cloud agents**. If a data collector is appropriate then determine which data collector installation is best for your environment. A data collector is service agnostic. After you install a data collector, it works for any Oracle Management Cloud service. See Install a Data Collector.
Install cloud agents.	A cloud agent is required to use Oracle Management Cloud. A cloud agent is service agnostic. After you install a cloud agent, it works for any Oracle Management Cloud service. See Install Cloud Agents.
Defining entities for monitoring and analysis.	After you install agents, you must define and add the entities that you want to monitor. See Next Steps: Defining Entities for Monitoring and Analysis.

2

Generic Prerequisites for Deploying Oracle Management Cloud Agents

Before deploying Oracle Management Cloud agents (gateways, data collectors, or cloud agents) in your data center, ensure that the following prerequisites are met:

Supported Operating Systems

The following table lists the supported operating systems:

Table 2-1 Supported Operating Systems

Operating System	Version
Red Hat Enterprise Linux	Red Hat Enterprise Linux 6 or later (64 bit) Red Hat Enterprise Linux 7 or later (64 bit)
Oracle Linux	Oracle Linux 6 or later (64 bit) Oracle Linux 7 or later (64 bit) Oracle Linux 8 or later (64 bit)
SUSE Linux	SUSE Linux Enterprise Server 11 (x86_64)
Ubuntu Linux	Ubuntu Linux 14.02
AIX	AIX 6.1 Technology Level 9 or later AIX 7.1 Technology Level 3 or later AIX 7.2 (base) and later
Oracle Solaris	Oracle Solaris 10 or later for SPARC (64 bit) Oracle Solaris 11 or later for SPARC (64 bit)
Microsoft Windows	Microsoft Windows Server 2012 Standard (64 bit) Microsoft Windows Server 2016 Standard (64-bit) Microsoft Windows Server 2019 Standard (64-bit)

Environment Requirements

- You require the *unzip* utility to decompress the initial software zip file. Ensure you have it installed or download *unzip* to decompress the initial agent software zip file.

- To download the Oracle Management Cloud agents install software bundle and perform other administration tasks from the Oracle Management Cloud interface, you must sign in as a user with the OMC Administrator role. See Add Users and Assign Roles in *Getting Started with Oracle Management Cloud.*
- Oracle recommends installing the Oracle Management Cloud agent as the same user who installed the Oracle software, if they want to discover and monitor Oracle software. Typically this user is `oracle`.
- If you plan to use the IT Analytics or Log Analytics components and if you want to collect data from an existing on-premises Oracle Enterprise Manager setup, then you must have an existing deployment of any one of the following in your data center.
  - Oracle Enterprise Manager Cloud Control 12.1.0.3
  - Oracle Enterprise Manager Cloud Control 12.1.0.4
  - Oracle Enterprise Manager Cloud Control 12.1.0.5
  - Oracle Enterprise Manager Cloud Control 13.1.0.x
  - Oracle Enterprise Manager Cloud Control 13.2.0.x
  - Oracle Enterprise Manager Cloud Control 13.3.0.x
  - Oracle Enterprise Manager Cloud Control 13.4.0.x
- Agents installation requires fully qualified domain names (FQDN) for your hosts. For UNIX environments, add the FQDN in the `/etc/hosts` file and ensure that it maps to the correct host name and IP address of the host. The recommended format is as follows:

  `<ip> <fully_qualified_host_name> <short_host_name>`

  For example:

  If your host name is *myhost* and your domain is *example.com (IPv4)*:

  ```
  172.16.0.0 myhost.example.com myhost
  ```

  If your host name is *myhost* and your domain is *example.com (IPv6)*:

  ```
  aaaa::111:2222:3333:4444 myhost.example.com myhost
  ```

  You can run the following commands to verify. You should see the same host name and IP address displayed.

  ```
  getent hosts `hostname`
  host `hostname`
  ```

  In the output, the FQDN must appear in the second field as specified in the `/etc/hosts` file. For example, the previous commands should return the following output:

  $ getent hosts `*hostname*`

  ```
  172.16.0.0 myhost.example.com myhost
  ```

  $ host `*hostname*`

  ```
  myhost.example.com has address 172.16.0.0
  ```

- Ensure that you deploy the Oracle Management Cloud agents in the following sequence:

1. Gateway (if needed).
2. Data collector (if integrating with Oracle Enterprise Manager).
3. Cloud agents (for collecting availability, configuration and performance metrics).

- For UNIX environments, the file system where the agent will be installed needs to allow executable binaries to run. Ensure that the file system was not mounted with the `noexec` option. If this parameter is set, then the entire file system does not allow the execution. You can use the `mount` command or check the file system in the mount options (`/etc/fstab`) to verify if the `noexec` option has been set.

Permissions on Windows Systems

You must deploy an agent on Windows as an administrator and ensure that necessary permissions are set as follows:

- From the **Start** menu, click **Settings**, then click **Control Panel**. From the Control Panel window, click **Administrative Tools**, and then click **Local Security Policy**. Expand the **Local Policies** folder and open the **User Rights Assignment** folder and set the following permissions:
  - Act as part of the operating system
  - Adjust memory quota for a process
  - Log on as a batch job
  - Replace process level tokens

Permissions Required on the Agent Base Directory

- The Agent Base Directory is the directory where the agent will be installed. Ensure only the *root* user and *agent installation* user have write permission on the Agent Base Directory and its parent directory even after the agent installation, to make sure all agent life cycle operations such as update or delete complete successfully.
- If the Agent Base Directory is created before the installation, ensure the directory is empty. The agent installation user must have write access to the directory.
- If the Agent Base Directory is not created before installation, it will be created by default under the directory where the agent software zip file was extracted. Ensure the agent installation user has write access to the parent directory where the Agent Base Directory will be created.

Network Prerequisites

Oracle Management Cloud Agents communicate to Oracle Management Cloud. If your network setup has a firewall, ensure you allow HTTPS communication from the host on which the agent is to be deployed to `*.oraclecloud.com` to allow outbound communication. You can use any available network connectivity tool to verify connectivity with the data center.

Oracle Management Cloud Agents (Cloud Agents, Data Collectors, Gateways) do not support NTLM Authorization Proxy Servers (APS).

The following example table lists the ports that need to be open for communication.

Direction	Port	Protocol	Reason
Data Collector to OMR host	22 or user defined	SSH	Data collector to connect with OMR host.

Direction	Port	Protocol	Reason
Proxy server to external	443	HTTPS	Communication with Oracle Management Cloud services.
Cloud agent node to gateway	Gateway host port	TCP	Communication with gateway.

Requirement for Integrating With Oracle Enterprise Manager

If you want to collect data from Oracle Enterprise Manager (EM), including Oracle Database Diagnostics Pack or Oracle WebLogic Server Management Pack, you must deploy a Data Collector. For collecting database performance data used by IT Analytics, ensure that the Data Collector owner (host user) is the same as the Oracle Enterprise Manager on-premises agent host user. This allows connections to the EM database targets using the EM monitoring credentials and ensures database performance data can be collected.

Requirement for Logs Collection on Unix

If you are deploying the agents for using Oracle Log Analytics on UNIX-based hosts, ensure that the cloud agent has the correct privileges to read the log files from where data has to be collected.

You can use either one of the following ways (in order of best practice) to make the log files readable to the cloud agent:

- Use Access Control Lists (ACLs) to enable the cloud agent user to read the log file path and log files. An ACL provides a flexible permission mechanism for file systems. Ensure that the full path to the log files is readable through the ACL.

  To set up an ACL in a UNIX-based host:

  1. Determine whether the system that contains the log files has the `acl` package:

     ```
     rpm -q acl
     ```

     If the system contains the `acl` package, then the previous command should return:

     ```
     acl-2.2.39-8.el5
     ```

     If the system doesn't have the `acl` package, then download and install the package.

  2. Grant the cloud agent user read access to the required log file:

     ```
     setfacl -m u:<agentuser>:r file <path to the log file/log file name>
     ```

     Grant the cloud agent user read access to the leading path or folders by running the following command:

     ```
     setfacl -d -m u:<agentuser>:r file <path to the parent folder of the log file>
     ```

- Place the cloud agent and the product that generates the logs in the same user group, and make the files readable to the entire group.
- Install the cloud agent as the user that also owns the logs. This is difficult to achieve if there are a lot of different logs owned by different users on same host.

- Make the log files readable to all users. For example, `chmod o+r <file>`

3

Download the Oracle Management Cloud Agent Software

The Oracle Management Cloud agent software is provided in a downloadable ZIP file which contains the required files to install Oracle Management Cloud agents.

This section covers the following:

- Download the Oracle Management Cloud Agent Software
- Extract the Agent Software ZIP File
- Create Registration Keys

Download the Oracle Management Cloud Agent Software

You can download the agent software ZIP file using one of the following options:

- Download Using Oracle Management Cloud User Interface
- Download Using a Web Browser

Download Using Oracle Management Cloud User Interface

The preferred method to download the agent installation software is using the Oracle Management Cloud User Interface.

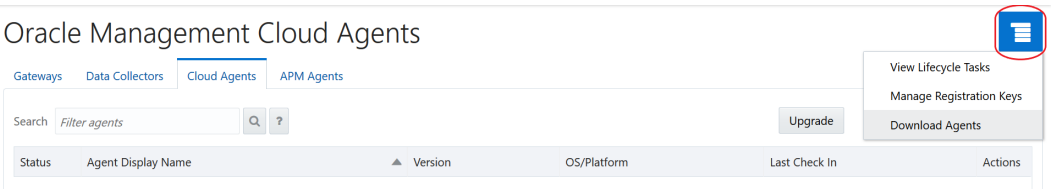
The agent installation software ZIP file is tenant agnostic: You can download it from any tenant and use it to install agents against other tenants.

Perform the following steps to download the agent software ZIP file:

1. On the Oracle Management Cloud home page, click the **OMC Navigation** icon on the top left corner to view the Management Cloud navigation pane, if it isn't already displayed.
2. Select **Agents** under **Administration**.

   The Oracle Management Cloud Agents page is displayed.

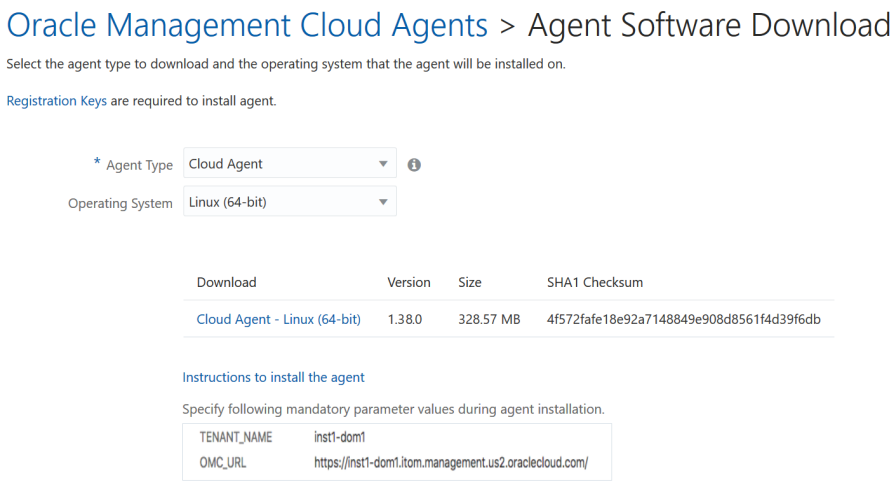
3. On the Oracle Management Cloud Agents page, click the Action Menu on the top right corner of the page and select **Download Agents**.



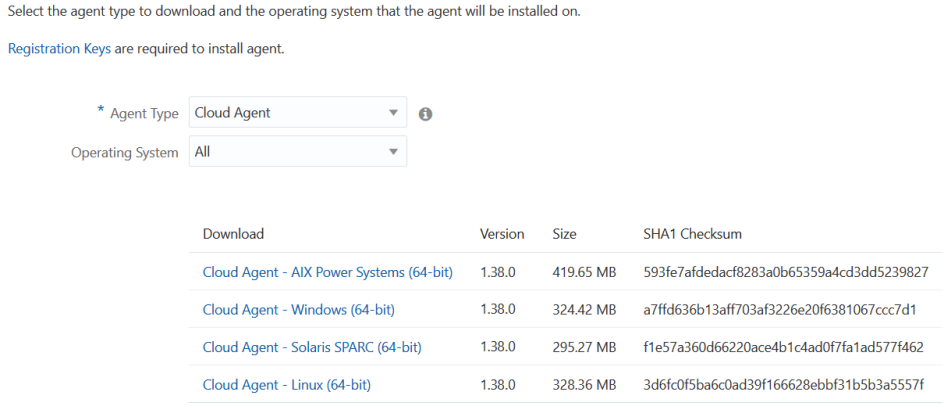
   The Agent Software Download page is displayed.

4. Select the agent type from the **Agent Type** drop-down list, and select the operating system that the agent will be installed on from the **Operating System** drop-down list.

   The agent software link for the agent you have selected is displayed.



If you want to view a list of agent installers for all available and supported operating systems, then select **All** from the **Operating System** drop-down list.



5. Click the agent software link to download the agent software ZIP file.

Ensure that you verify if the downloaded ZIP file is downloaded completely. Run the following command to verify if the value of the *SHA1 Checksum* column in the user interface matches the output.

- Linux: `sha1sum <cloudagent_linux.x64_1.33.0.zip>`

This agent software ZIP file is now saved on your host.

Download Using a Web Browser

You can also download the agent software ZIP file using a Web Browser. This is an alternative method provided in case you don't have access to the Oracle Management Cloud User Interface or you have internet, network or firewall restrictions.

Click one of the following platform-specific links of your choice:

Cloud Agents and Data Collectors

- Cloud Agent and Data Collector ZIP file for Solaris
- Cloud Agent and Data Collector ZIP file for Linux
- Cloud Agent and Data Collector ZIP file for AIX
- Cloud Agent and Data Collector ZIP file for Windows

Gateways

- Gateway ZIP file for Solaris
- Gateway ZIP file for Linux
- Gateway ZIP file for AIX
- Gateway ZIP file for Windows

When downloading the agent software using this method, you still need to connect to the Oracle Management Cloud to gather parameters values before you start installing the agent. To gather the required parameters values, you need to perform the following:

1. On the Oracle Management Cloud home page, click the **OMC Navigation** icon on the top left corner to view the Management Cloud navigation pane, if it isn't already displayed.
2. Select **Agents** under **Administration**.
3. On the Oracle Management Cloud Agents page, click the Action Menu  on the top right corner of the page and select **Download Agents**.

   The Agent Software Download page is displayed.
4. Select the agent type from the **Agent Type** drop-down list, and select the operating system that the agent will be installed on from the **Operating System** drop-down list.

   The agent software link for the agent you've selected is displayed.
5. Make a note of the `TENANT_NAME` and `OMC_URL` parameter values displayed under the agent link. When installing the agent, you'll have to update the response file with these values. See Understanding Response Files

Extract the Agent Software ZIP File

To extract the agent software ZIP file, perform the following steps:

- Navigate to the directory where you have downloaded the agent software ZIP file.
- Run the following command to unzip the file: unzip <your zip file name>
- For example, unzip cloudagent_linux.x64_1.31.0.zip

Create Registration Keys

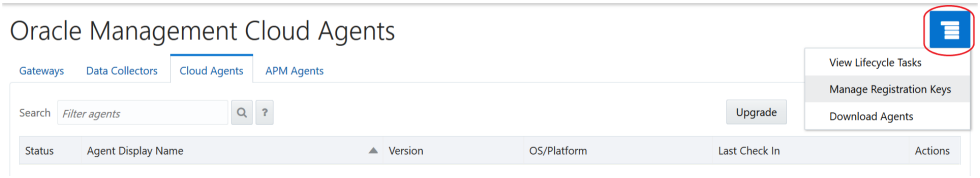
You need a registration key to install Oracle Management Cloud Agents.

A registration key is issued against your identity domain. You can create a new registration key and use that key for installing a new agent by updating the response file and specifying the AGENT_REGISTRATION_KEY=<NewKeyValue> parameter. The registration key is only used during installation. Once an agent is installed with the registration key, that key can be removed from Oracle Management Cloud.

To create a registration key:

1. On the Oracle Management Cloud home page, click the global navigation menu on the top left, then click **Agents** under **Administration**.

   The Oracle Management Cloud Agents page is displayed.
2. On the Oracle Management Cloud Agents page, click the Action Menu  on the top right corner of the page and select **Manage Registration Keys**.



The Registration Keys page displays a list of all registration keys.

3. Enter the required details in the Registration Keys page:
   a. In the **Name** field, specify a name to identify the registration key.
   b. In the **Registration Limit** field, enter a number that indicates the maximum number of agents, data collectors, and gateways that can be associated with the registration key.
   c. Click **Create New Key**.

   A new registration key is created. You can now pass the value of this key to the `AgentInstall` script at the time of installation.

You can also download a registration key. For more information, see Manage Registration Keys.

4
Understanding Response Files

The Oracle Management Cloud agent installation script (`AgentInstall.sh|bat`) uses response files to read the installation parameters specific to your environment.

About Response Files

When you download and extract any set of the agent installation files (either for cloud agent, data collector or gateway), you receive the following:

- A response file template (`.rsp`).
- An agent installation script (`AgentInstall.sh|bat`).
- Other agent installation software files.

You can have one of the following response file templates:

- `agent.rsp` if you download agent software for a cloud agent or a data collector.
- `gateway.rsp` if you download agent software for a gateway.

You need to customize the corresponding `.rsp` response file with your own parameter values. It is recommended to create a copy of the original `.rsp` response file, and then edit the copy specifying the values of your parameters for your installation.

Keep in mind the following facts regarding response files:

- Response files should always be a plain text (UTF-8) character set file.
- Response files list all the supported parameters. At a minimum, edit the mandatory parameters. If your environment details remain the same, you can reuse this response file in the future.
- Response files are not platform-specific or release-specific. You can use the same response file on multiple equivalent platforms. Be sure to check for possible new parameters in a new release.
- When you install agents, the response file resides in the same location as the agent installation script (`AgentInstall.sh|bat`) by default.
- A cloud agent and data collector are installed using the same set of agent installation files. If the response file has data collector parameter values specified, then the installer starts the data collector installation. Otherwise, the installer looks for cloud agent parameters and starts the cloud agent installation.

> **Note:**
>
> Because the passwords that you specify in the response file are in plain text, you need to adequately protect the response file or delete the it as soon as the installation process completes.

You are now ready to:

- Review and use the Cloud Agent Response File to Install Cloud Agents.
- Review and use the Data Collector Response File to Install a Data Collector.
- Review and use the Gateway Response File to Install a Gateway.

Parameters for Installing a Cloud Agent

This section describes the parameters that are required for installing a cloud agent.

If you want to install a cloud agent then you need to edit the response file (`agent.rsp`) and provide values for the parameters that are required to install a cloud agent.

The following are the list of parameters that are specified in the response file:

- Registration Parameters
- Communication Parameters
- Proxy Parameters (Optional)
- Other Optional Parameters

For response files samples, see Sample Response Files.

Registration Parameters

This section lists the registration parameters that are required to install a cloud agent. All registration parameters are mandatory. Ensure that your response file has the correct values for the following parameters.

Parameter	Parameter Type	Description	Notes
`TENANT_NAME` **or** `TENANT_ID` (supported in older versions and it remains backwards compatible)	Mandatory	Name of the tenant where Oracle Management Cloud is running. You can get the `TENANT_NAME` value for an agent by navigating to **Administration** > **Agents** > **Download**, and selecting an agent type from the **Agent Type** drop-down list. The `TENANT_NAME` value is displayed at the bottom of the page.	Example: *`inst1-dummytenantid`*
`AGENT_REGISTRATION_KEY`	Mandatory	Key to validate the identity of the tenant and the authenticity of the installation. You can get the registration key from Oracle Management Cloud Dashboard, by navigating to **Administration** > **Agents** > **Registration Keys**.	Example: `R5bokWss0EC9R1pJlf2SqiAJ9p`

Parameter	Parameter Type	Description	Notes
AGENT_BASE_DIRECTORY	Optional	Empty directory where the agent must be installed on the host machine. If a parameter value is provided and the provided value (a directory) does not exist then a directory is created by the installer. If the parameter AGENT_BASE_DIRECTORY is not provided, the installer will create a new directory, omcagent, in the directory the installer is running from. **Note:** For Windows, the length of the directory path including the drive letter should be less than 23 characters.	Example: Linux: /omc_agent/dc Windows: D:\omc_agent\dc

Communication Parameters

This section lists the communication parameters that are required to install a cloud agent.

Parameter	Parameter Type	Description	Notes
OMC_URL **or** UPLOAD_ROOT (supported in older versions and it remains backwards compatible)	Mandatory	The absolute URL including the protocol that is required to connect to Oracle Management Cloud for uploading data for the specific TENANT_NAME. To get this value, navigate to **Administration** > **Agents** > **Download**, and select an agent type from the **Agent Type** drop-down list. The OMC_URL value is displayed at the bottom of the page.	Example: https://*dummytenantid*.itom.<*datacenter*>.oraclecloud.com

Parameter	Parameter Type	Description	Notes
GATEWAY_HOST	Mandatory if cloud agent communicates via gateway	If cloud agent or data collector is communicating to OMC using a gateway, then provide the Fully Qualified Domain Name (FQDN) of the gateway. When you install the cloud agent, make sure you provide the same gateway host name that was used to install the gateway. For example, when deploying the gateway, if you specify ORACLE_HOSTANME=abc.xyz.com and when installing the cloud agent, you specify GATEWAY_HOST=abc, it will result in cloud agent registration failures. A gateway agent must be installed on the host and should be up and running.	Example: GATEWAY_HOST=testgateway.test.oracle.com
GATEWAY_PORT	Mandatory if cloud agent communicates via gateway	If cloud agent or data collector is communicating to OMC using a gateway, the gateway port must be specified. You can obtain the port number by executing the following command: $Gateway_Agent_Home/agent_inst/bin/omcli status agent	Example: GATEWAY_PORT=4472
ADDITIONAL_GATEWAYS	Mandatory if cloud agent communicates via gateway	For gateway high availability, additional gateway hosts (comma separated list of gateway URLs) can be specified. You can obtain the URL by running the following command on respective gateway hosts: $Gateway_Agent_Home/agent_inst/bin/omcli status agent **Note:** This parameter should only be used while deploying a cloud agent or a data collector.	Example: ADDITIONAL_GATEWAYS=https://abc.us.com:1872,https://xyz.us.com:4475

Proxy Parameters (Optional)

If you're installing the cloud agent over a proxy server, then apart from specifying the Registration Parameters and Communication Parameters, ensure that you specify the correct values for the following parameters in your response file.

Parameter	Description	Notes
OMC_PROXYHOST	Address of your proxy server to be used for connection. Ensure that you don't pass the https:// value with the proxy host details.	Required only if you're deploying the agent over a proxy server. Example: OMC_PROXYHOST=www-proxy.example.com
OMC_PROXYPORT	Port of your proxy server.	Required only if you're deploying the agent over a proxy server. Example: OMC_PROXYPORT=80
OMC_PROXYUSER	User name required to access your proxy server.	Required only if you are using a proxy server to communicate with Oracle Management Cloud. It requires a username and password. Example: OMC_PROXYUSER=johndoe
OMC_PROXYPWD	Password required to access your proxy server.	Required only if you're deploying the agent over a proxy server. Example: OMC_PROXYPWD=password
OMC_PROXYREALM	Authentication realm (if any) to be used to access your proxy server.	Required only if you're deploying the agent over a proxy server. Example: OMC_PROXYREALM=McAfee Web Gateway

If you are using authenticated proxy servers, you need to set the following proxy parameters: OMC_PROXYHOST, OMC_PROXYPORT, OMC_PROXYUSER, OMC_PROXYPWD and OMC_PROXYREALM. The value of the OMC_PROXYREALM parameter is specific to the authenticated proxy server in use.

- For McAfee Web Gateway, the default value is OMC_PROXYREALM=McAfee Web Gateway.
- For Squid proxy, the default value is OMC_PROXYREALM=Squid proxy-caching web server.
- For other vendors, contact your proxy vendor for instructions about how to get the realm value from the proxy settings.

Other Optional Parameters

This section lists the parameters that you can optionally specify in your response file for installing a cloud agent. However, you need to ensure that your response file contains values for the Registration Parameters and Communication Parameters.

Parameter	Description	Notes
AGENT_PORT	The port number to which the agent process will be bound. The AgentInstall script stops the installation process if this port is occupied at the time of installation. If you don't specify any value, the default port (4459) or an available port in the range 4460-4479 is used. This applies to new installations only. If you have older agents already running on other port numbers, you can continue to run them as such.	Example: 4461
ORACLE_HOSTNAME	The host name where the agent will be installed. If specified, the value is validated to check if it resembles the agent host name and that it is neither an IP address nor a junk value (such as foobar, test, and so on). It must match the fully qualified domain name (FQDN) specified in the /etc/hosts (in UNIX) and C:\Windows\System32\drivers\etc\hosts (in Windows) file and must map to the correct FQDN and IP address of the host. **Note:** Use this parameter when you want to provide a network-resolvable hostname instead of installer-computed hostname. **Note:** Ensure the parameter is a fully qualified domain name as most of the services in Oracle Management Cloud require the host to be an FQDN. It must resolve to a valid IP address.	Example: example1.tst.example.com If you don't specify any value, the AgentInstall script evaluates the host name using the INetAddress Java class methods.
REINSTALL	A flag to enable the agent reinstall option. See Install the Cloud Agent Using Reinstall Option for more details.	• Valid values: true or false • Default value: false To enable the agent reinstall option, change the value to true, REINSTALL=true.

Parameter	Description	Notes
IGNORE_VALIDATIONS	A flag to disable all validations and prerequisite checks.	• Valid values: true or false • Default value: false To ignore validations, change the value to true, IGNORE_VALIDATIONS=true.
IGNORE_ULIMIT_CHECK	A flag to disable ulimit checks (only on non-windows platforms).	• Valid values: true or false • Default value: false To ignore ulimit checks, change the value to true, IGNORE_ULIMIT_CHECK=true.
DISPLAY_NAME	A display name for the tenant management agent as given by the user.	The default value is <agent host>: <agent port>. For example, myhost:4459.
AGENT_HOST_DISPLAY_NAME	A display name for the tenant management agent host as given by the user.	The default value is <agent host>: <agent port>. For example, myhost:4459.

Parameters for Installing Data Collector

This section describes the parameters that are required for installing a data collector.

If you want to install a data collector then you need to edit the response file (agent.rsp) and provide values for the parameters that are required to install a cloud agent (See, Parameters for Installing a Cloud Agent). In addition, you must also specify the values for the data collector parameters from the following list:

- Data Collector Parameters
- Optional Data Collector Parameters

For response files samples, see Sample Response Files.

Data Collector Parameters

The following are data collector specific parameters that are required to install a data collector.

Parameter	Parameter Type	Description	Notes
DATA_COLLECTOR_USERNAME	Mandatory	User that's created for the data collector in the Oracle Management Repository and is used to collect Oracle Enterprise Manager Cloud Control data. The user name must be a minimum of 5 characters and a maximum of 26 characters in length and must start with a string (a-z or A-Z).	Example: testdcjlr
DATA_COLLECTOR_USER_PASSWORD	Mandatory	Password to be set for DATA_COLLECTOR_USERNAME (must be 5-8 alphanumeric characters and must start with a letter). The password rules of the data collector are the same as that of the Oracle Management Repository database password rules, because the data collector creates a schema in the Oracle Management Repository database. However, data collector passwords can't have a special character or numeric as the first character.	Example: jDC5878
OMR_USERNAME	Mandatory	Privileged database user name to sign in to the Oracle Management Repository; must have the SYS role. The user should have access to create DATA_COLLECTOR_USERNAME user in the OMR to collect data from it.	Example: sys
OMR_USER_PASSWORD	Mandatory	Password used to sign in to the Oracle Management Repository in your data center.	Example: password_4u
OMR_HOST_USERNAME	Mandatory	User name (of the install user of Oracle Management Repository) for the host where Oracle Management Repository is running in your data center.	Example: johndoe

Parameter	Parameter Type	Description	Notes
OMR_STAGE_DIR	Mandatory	Directory where the data collector stores the harvested data in an archived form. OMR_STAGE_DIR should be present in OMR_HOSTNAME and the user deploying the data collector must have read or write permissions to OMR_STAGE_DIR. This directory must have at least 2048 MB free space available. The directory name can be up to 4000 characters.	Example: /stage/test
OMR_HOST_USER_PASSWORD	Mandatory	Password for the host where the Oracle Management Repository is running in your data center.	Example: AUPA0fgQ1 Leave this parameter blank if OMR_HOST_USER_SSH_KEY is provided.
OMR_HOST_USER_SSH_KEY	Mandatory	Path to the private SSH key to be used to connect to your Oracle Management Repository.	Example: $HOME/.ssh/id_rsa Leave this parameter blank if OMR_HOST_USER_PASSWORD is provided.
OMR_CONNECT_STRING	Mandatory	Connection string to be used to connect to Oracle Management Repository. The OMR_CONNECT_STRING, or a combination of OMR_HOSTNAME, OMR_PORT, and either OMR_SID or OMR_SERVICE_NAME is required to connect to the Oracle Management Repository.	Example: mytestconnectstring Leave this parameter blank if a combination of OMR_HOSTNAME, OMR_PORT, and either OMR_SID or OMR_SERVICE_NAME is provided.
OMR_HOSTNAME	Mandatory	Fully qualified name of the host where the Oracle Management Repository is running.	Example: example1.test.example.com Leave this parameter blank if OMR_CONNECT_STRING is provided.
OMR_PORT	Mandatory	Listen port of the Oracle Management Repository in your data center.	Example: 1845 Leave this parameter blank if OMR_CONNECT_STRING is provided.

Parameter	Parameter Type	Description	Notes
OMR_SID	Mandatory	SID of the Oracle Management Repository (mutually exclusive with OMR_SERVICE_NAME).	Example: orcl Leave this parameter blank if OMR_CONNECT_STRING or OMR_SERVICE_NAME is provided.
OMR_SERVICE_NAME	Mandatory	Service name of the Oracle Management Repository (mutually exclusive with OMR_SID).	Example: orcl.example.com Leave this parameter blank if OMR_CONNECT_STRING or OMR_SID is provided.

Optional Data Collector Parameters

The following are optional parameters required to install a data collector.

Parameter	Description	Notes
OMR_USER_ROLE	User role to connect to the Oracle Management Repository, such as sysdba.	Example: sysdba
OMR_HOST_SSH_PORT	Optional SSH port (default=22) on which the Oracle Management Repository host is configured to listen on.	Example: 22
NAMESPACE	Namespace (default host:port) used to identify the data collector.	Example: dcagent.test.example.com:1845
IGNORE_DATA_COLLECTOR_VALIDATIONS	Flag to disable all data collector validations.	Valid values: true or false

Parameters for Installing a Gateway

This section describes the parameters that are required for installing a gateway.

If you want to install a gateway then you need to edit the response file (gateway.rsp) and provide values for the parameters that are required to install a gateway.

The following are the list of parameters specified in the response file:

- Registration Parameters
- Communication Parameters
- Proxy Parameters (Optional)
- Other Optional Parameters

For response files samples, see Sample Response Files.

Registration Parameters

This section lists all the registration parameters that are required to install a gateway. All registration parameters are mandatory. Ensure your response file has the correct values for the these parameters.

The following table lists the Registration Parameters required for gateway installation.

Parameter	Parameter Type	Description	Notes
`TENANT_NAME` **or** `TENANT_ID` (supported in older versions and it remains backwards compatible)	Mandatory	Name of the tenant where Oracle Management Cloud is running. You can get the `TENANT_NAME` value for an agent by navigating to **Administration** > **Agents** > **Download**, and selecting an agent type from the **Agent Type** drop-down list. The `TENANT_NAME` value is displayed at the bottom of the page. The `TENANT_NAME` must be in the format: <instance_name>-<identity_domain>	Example: *`inst1-dummytenantid`*
`AGENT_REGISTRATION_KEY`	Mandatory	Key to validate the identity of the tenant and the authenticity of the installation. You can get the registration key from Oracle Management Cloud Dashboard, by navigating to **Administration** > **Agents** > **Registration Keys**.	Example: `R5bokWss0EC9R1pJlf2SqiAJ9p`
`AGENT_BASE_DIRECTORY`	Optional	Empty directory where the agent must be installed on the host machine. If a parameter value is provided and the provided value (a directory) does not exist then a directory is created by the installer. If the parameter `AGENT_BASE_DIRECTORY` is not provided, the installer will create a new directory, `omcagent`, in the directory the installer is running from. **Note:** For Windows, the length of the directory path including the drive letter should be less than 23 characters.	Example: Linux: `/omc_agent/dc` Windows: `D:\omc_agent\dc`

Communication Parameters

The following table lists the Communication Parameters required for gateway installation.

Parameter	Parameter Type	Description	Notes
`OMC_URL` **or** `UPLOAD_ROOT` (supported in older versions and it remains backwards compatible)	Mandatory	The absolute URL including the protocol that is required to connect to Oracle Management Cloud for uploading data for the specific `TENANT_NAME`. To get this value, navigate to **Administration** > **Agents** > **Download**, and select an agent type from the **Agent Type** drop-down list. The `OMC_URL` value is displayed at the bottom of the page.	Example: `https://`*`dummytenantid`*`.itom.<`*`datacenter`*`>.oraclecloud.com`

Proxy Parameters (Optional)

If you're installing a gateway over a proxy server, then apart from specifying the Registration Parameters and Communication Parameters, ensure that you specify the correct values for the following parameters in your response file.

Parameter	Description	Notes
`OMC_PROXYHOST`	Address of your proxy server to be used for connection. Ensure that you don't pass the `https://` value with the proxy host details.	Required only if you're deploying the agent over a proxy server. Example: `OMC_PROXYHOST=www-proxy.example.com`
`OMC_PROXYPORT`	Port of your proxy server.	Required only if you're deploying the agent over a proxy server. Example: `OMC_PROXYPORT=80`
`OMC_PROXYUSER`	User name required to access your proxy server.	Required only if you are using a proxy server to communicate with Oracle Management Cloud. It requires a username and password. Example: `OMC_PROXYUSER=johndoe`
`OMC_PROXYPWD`	Password required to access your proxy server.	Required only if you're deploying the agent over a proxy server. Example: `OMC_PROXYPWD=password`

Parameter	Description	Notes
OMC_PROXYREALM	Authentication realm (if any) to be used to access your proxy server.	Required only if you're deploying the agent over a proxy server. Example: OMC_PROXYREALM=McAfee Web Gateway

If you are using authenticated proxy servers, you need to set the following proxy parameters: OMC_PROXYHOST, OMC_PROXYPORT, OMC_PROXYUSER, OMC_PROXYPWD and OMC_PROXYREALM. The value of the OMC_PROXYREALM parameter is specific to the authenticated proxy server in use.

- For McAfee Web Gateway, the default value is OMC_PROXYREALM=McAfee Web Gateway.
- For Squid proxy, the default value is OMC_PROXYREALM=Squid proxy-caching web server.
- For other vendors, contact your proxy vendor for instructions about how to get the realm value from the proxy settings.

Other Optional Parameters

This section lists the parameters that you can optionally specify in your response file for installing a gateway. However, you need to ensure that your response file contains values for the Registration Parameters and Communication Parameters.

Parameter	Description	Notes
AGENT_PORT	The port number to which the agent process will be bound. The AgentInstall script stops the installation process if this port is occupied at the time of installation. If you don't specify any value, the default port (4459) or an available port in the range 4460-4479 is used. This applies to new installations only. If you have older agents already running on other port numbers, you can continue to run them as such.	Example: 4461

Parameter	Description	Notes
ORACLE_HOSTNAME	The host name where the agent will be installed. If specified, the value is validated to check if it resembles the agent host name and that it is neither an IP address nor a junk value (such as foobar, test, and so on). It must match the fully qualified domain name (FQDN) specified in the /etc/hosts (in UNIX) and C:\Windows\System32\drivers\etc\hosts (in Windows) file and must map to the correct FQDN and IP address of the host. **Note:** Use this parameter when you want to provide a network-resolvable hostname instead of installer-computed hostname. **Note:** Ensure the parameter is a fully qualified domain name as most of the services in Oracle Management Cloud require the host to be an FQDN. It must resolve to a valid IP address.	Example: example1.tst.example.com If you don't specify any value, the AgentInstall script evaluates the host name using the INetAddress Java class methods.
REINSTALL	A flag to enable the agent reinstall option. See Install a Gateway Using Reinstall Option for more details.	• Valid values: true or false • Default value: false To enable the agent reinstall option, change the value to true, REINSTALL=true.
IGNORE_VALIDATIONS	A flag to disable all validations and prerequisite checks.	• Valid values: true or false • Default value: false To ignore validations, change the value to true, IGNORE_VALIDATIONS=true.
IGNORE_ULIMIT_CHECK	A flag to disable ulimit checks (only on non-windows platforms).	• Valid values: true or false • Default value: false To ignore ulimit checks, change the value to true, IGNORE_ULIMIT_CHECK=true.
DISPLAY_NAME	A display name for the tenant management agent as given by the user.	The default value is <agent host>:<agent port>. For example, myhost:4459.
AGENT_HOST_DISPLAY_NAME	A display name for the tenant management agent host as given by the user.	The default value is <agent host>:<agent port>. For example, myhost:4459.

5

Install Oracle Management Cloud Agents

You must install agents to collect data from entities that you want to manage and monitor from Oracle Management Cloud.

Topics:

Install a Gateway

A gateway is an agent that acts as a channel between Oracle Management Cloud and all other Oracle Management Cloud agents.

A gateway is optional, but it's considered a best practice to install one for future use and security needs. For security reasons, enterprises typically allow one or a few hosts to connect to the Internet. You install a gateway on the hosts that have access to the Internet, so that all other agents communicate with Oracle Management Cloud using the hosts that have the gateway installed.

It's recommended that you install multiple gateways, because this provides high availability for other Oracle Management Cloud agents. So, if one gateway goes down, then the agents can transmit data through another working gateway.

Topics:

Minimum System Requirements for Installing a Gateway

Minimum System Requirements

The following table lists the minimum system requirements to install a gateway.

RAM	Kernel Parameters	Port Number	Free Disk Space
4 GB*	Ulimit value for maximum user processes >=4000	4459 to 4479	4 GB**

*It will increase if you have more cloud agents communicating to a gateway.

**A gateway default buffer size is 100GB. If the connectivity to Oracle Management Cloud is not available, the gateway will buffer the data to disk. In order to avoid loss of monitoring data during this period of no connectivity, it is recommended to have at least the default buffer size free.

Prerequisites for Installing a Gateway

Before you install a gateway, you must meet a set of prerequisites.

This section lists the key considerations and prerequisites for installing a gateway and covers the following:

- General Guidelines
- Prerequisites Check Option

General Guidelines

- It is recommended not to deploy cloud agents as a `root` user.
- Installing a gateway is an optional task. In your data center, if the hosts on which you want to install cloud agents have access to the Internet, either directly or through a proxy server, then you can skip installing a gateway. Typically, in large organizations that have an enterprise setup, access to Internet is controlled, and only a few hosts are configured as gateways through which other hosts access the Internet. This helps ensure the security of the setup against malicious cyber attacks.
- Before proceeding, ensure that you understand and follow the instructions listed in Generic Prerequisites for Deploying Oracle Management Cloud Agents and Download the Oracle Management Cloud Agent Software.

Prerequisites Check Option

Before you install a gateway, you can check if you have met all the prerequisites to perform a seamless gateway installation. The `AgentInstall.sh` script reads the parameters values from the `gateway.rsp` response file and performs automated checks to ensure that your environment fulfills the basic requirements for the gateway installation.

Perform the following steps to run the prerequisites check:

1. On your Linux host, navigate to the gateway installation directory where you have saved the `gateway.rsp` file.
2. Open the `gateway.rsp` response file using any standard editor.
3. Enter values for the mandatory parameters: `TENANT_NAME`, `OMC_URL`, and `AGENT_REGISTRATION_KEY`.

   Based on your requirement, edit the optional parameters if the default values are not in line with your best practices.
4. Save the `gateway.rsp` response file.
5. Run the `AgentInstall` script passing the parameter `EXECUTE_PREREQ=true` using the command line interface.

   For example, `./AgentInstall.sh|bat EXECUTE_PREREQ=true`

If the prerequisite check fails, the script stops with relevant error message.

If the prerequisite check completes successfully, you get the following message:

```
$ ./AgentInstall.sh EXECUTE_PREREQ=true
Unzipping agent software, this may take some time...
Installing Gateway...
Executing Pre-requisite checks only for Gateway..
Gateway parameter validation started...
Gateway pre-requisite checks started...
Pre-requisite checks successfully completed for [Gateway].
```

Alternatively, you can pass the required parameter values using the command line interface to perform the prerequisite check.

For example, `./AgentInstall.sh|bat TENANT_NAME=<`*`TENANT_NAME`*`> OMC_URL=<`*`OMC_URL`*`> AGENT_REGISTRATION_KEY=<`*`AGENT_REGISTRATION_KEY`*`> EXECUTE_PREREQ=true`

Please refer to the log file located under `<`*`AGENT_ZIP_FILE_EXTRACTED_DIRECTORY`*`>/AgentInstall_<`*`timestamp`*`>.log` for more details.

Gateway: Typical Installation

This section discusses the typical installation of a gateway.

- It is recommended not to use `root` user to install a gateway.
- You install a gateway by running the `AgentInstall` script from the command line. The `AgentInstall` script reads a set of parameters that can be specified in a response file (`gateway.rsp`) or they can be passed along in the command line.
- A typical installation assumes the `gateway.rsp` response file is saved under the same directory where you have saved the `AgentInstall` script. If that's not the case, then you must pass the `AGENT_RSP_FILE` parameter in the command line with the location of the response file when you run the `AgentInstall` script. See Install a Gateway Specifying Parameters in the Command Line.
- If you have a proxy server or using custom certificates, be sure to check the steps listed in Install a Gateway Over a Proxy Server and Install a Gateway with Custom Certificates.

To perform a typical installation:

1. Identify a host in your data center with Internet access to Oracle Management Cloud.
2. Ensure that you have performed the steps listed in Prerequisites for Installing a Gateway.
3. Log in to the host where you will install a gateway and navigate to the directory where you have already extracted the gateway software ZIP file.

   For example, if you extracted the ZIP file to a directory named `gway_agent` under the `/u01/stage` directory on your host, then the `AgentInstall` script will be present in the `/u01/stage/gway_agent` directory after the ZIP file is extracted. Navigate from your present working directory to the `/u01/stage/gway_agent` directory.
4. Edit the `gateway.rsp` response file.

   Ensure you have updated the `gateway.rsp` response file and specified the correct values of the parameters listed in the Registration Parameters for Installing a Gateway.

   Based on your requirement, you may also need to update the `gateway.rsp` response file with values of the parameters listed in Optional Parameters for Installing a Gateway.

Once you are done editing, save the `gateway.rsp` response file under the same directory where `AgentInstall` script is located.

If you have a proxy server or using custom certificates, be sure to check the steps listed in Install a Gateway Over a Proxy Server and Install a Gateway with Custom Certificates.

5. Run the agent installation script to install a gateway.
   - If you are installing a gateway on a UNIX-based host:

     `./AgentInstall.sh`

     Alternatively, you can run `sh AgentInstall.sh`
   - If you are installing a gateway on a Windows host, right-click and select **Run as administrator** to open an Administrator command prompt and run the following:

     `AgentInstall.bat`

> **Note:**
>
> The user installing the agent must have permissions to act as part of the operating system, adjust memory quota for a process, replace process level tokens, and log on as a batch job. To verify the permissions, from the **Start** menu, click **Settings**, then click **Control Panel**. From the Control Panel window, click **Administrative Tools**, and then click **Local Security Policy**. Expand the **Local Policies** folder and open the **User Rights Assignment** folder.

Your gateway installation is now complete. Next step is to Verify the Gateway Installation.

Gateway: Other Installation Use Cases

This section discusses other gateway installation use cases.

Before you install a gateway, review the information in Prerequisites for Installing a Gateway.

- It is recommended not to use `root` user to install a gateway.
- You install a gateway by running the `AgentInstall` script from the command line. The `AgentInstall` script requires a set of parameters that can be specified in a response file (`gateway.rsp`) or they can be passed along through command line.
- If you haven't saved the `gateway.rsp` response file in the *same directory* where you have saved the `AgentInstall` script, then you must pass the `AGENT_RSP_FILE` parameter in the command line when you run the `AgentInstall` script. See Install a Gateway Specifying Parameters in the Command Line.

The following gateway installation use cases are covered:

- Install a Gateway Specifying Parameters in the Command Line
- Install a Gateway Over a Proxy Server
- Install a Gateway With Custom Certificates

- Install a Gateway Using Reinstall Option

Install a Gateway Specifying Parameters in the Command Line

This section discusses installing a gateway specifying parameters in the command line.

Perform the following before proceeding:

1. Review the Prerequisites for Installing a Gateway.
2. Ensure you have correctly configured the `gateway.rsp` response file. See Registration Parameters for Installing a Gateway and based on your requirements also, Optional Parameters for Installing a Gateway.

You can perform a gateway installation specifying parameters in the command line or you can specify a combination of command line parameters and the use of a response file. You can do one of the following:

- Specify parameters only in the response file (See Gateway: Typical Installation).
- Specify parameters only in the command line.
- Specify parameters in the command line and the response file. In this case, the parameter values specified in the command line gets priority over the same values specified in the response file.

Example 5-1 Specify parameters only in the command line:

```
./AgentInstall.sh|bat TENANT_NAME=<TENANT_NAME> OMC_URL=<OMC_URL>
AGENT_REGISTRATION_KEY=<AGENT_REGISTRATION_KEY>
AGENT_BASE_DIRECTORY=<AGENT_BASE_DIRECTORY>
```

In the above example, you specify the values of the parameters in the command line. The installation script will use the values of the mandatory parameters: `TENANT_NAME`,`OMC_URL`, `AGENT_REGISTRATION_KEY` and the optional parameter: `AGENT_BASE_DIRECTORY`.

Example 5-2 Specify parameters in the command line and the response file:

```
./AgentInstall.sh|bat AGENT_BASE_DIRECTORY=<AGENT_BASE_DIRECTORY>
```

In the above example, you specify the value of `AGENT_BASE_DIRECTORY` parameter in the command line and the rest of the parameters values are specified in the response file.

Example 5-3 Specify parameters in the command line and the response file if response file doesn't reside in the default location:

```
./AgentInstall.sh|bat AGENT_RSP_FILE=<absolute path to the gateway.rsp file>
```

In the above example, you specify the value of `AGENT_RSP_FILE` parameter in the command line since it resides in a different location than the `AgentInstall` installation script file (by default, both files reside in the same directory). The rest of the parameters are specified in the response file.

Install a Gateway Over a Proxy Server

This section discusses installing a gateway over a proxy server.

Install a Gateway Over a Proxy Server

If you are installing a gateway over a proxy server, then ensure to perform the following before proceeding:

- Review the Prerequisites for Installing a Gateway.
- Specify the values of the Parameters for Installing a Gateway Over a Proxy Server in the `gateway.rsp` response file.

To perform a gateway installation over a proxy server:

1. Log on to the host where you will install a gateway and navigate to the directory where you extracted the gateway software ZIP file that you previously downloaded.
2. Have your `gateway.rsp` response file ready. Ensure that you have specified the parameters for installing a gateway over a proxy server in the response file (`gateway.rsp`), and it's saved under the same directory where the `AgentInstall` script is located. The `AgentInstall` script reads and obtains the values of the installation parameters from the `gateway.rsp` response file at installation time.
3. Run the `AgentInstall` agent installation script to install a gateway.

- If you are installing a gateway on a UNIX-based host:

  ```
  ./AgentInstall.sh
  ```

- If you are installing a gateway on a Windows host, right-click and select **Run as administrator** to open an Administrator command prompt and run the following:

  ```
  AgentInstall.bat
  ```

> **Note:**
>
> Oracle Management Cloud Agents (Cloud Agents, Data Collectors, Gateways) do not support NTLM Authorization Proxy Servers (APS).

Install a Gateway with Custom Certificates

This section discusses installing a gateway over a proxy server when the proxy server has custom certificates.

Install a Gateway with Custom Certificates on UNIX-based hosts

To perform a gateway installation over a proxy server when your proxy server has custom certificates on UNIX-based hosts:

1. Contact the IT Security team within your organization and obtain the correct custom certificate (root certificate) before proceeding. See Custom Certificates for more details.

   Confirm the custom certificate is saved in DER format. Typically these certificate files would have a `.der` extension. For example, it can be saved as `mycert.der`.
2. Review and confirm that you have performed the steps listed in Generic Prerequisites for Deploying Oracle Management Cloud Agents, Download the Oracle Management Cloud Agent Software and Prerequisites for Installing a Gateway.
3. Ensure that you have correctly updated and saved the response file (`gateway.rsp`). See Registration Parameters for Installing a Gateway and based on your requirements also, Optional Parameters for Installing a Gateway .

4. Log in to the host where you are planing to install the gateway, navigate to the directory where you have extracted the gateway installation software ZIP file and confirm `agentcoreimage.zip` file exists.

   ```
   cd <path to the stage location>
   ls -la agentcoreimage.zip
   ```

5. Update the `agentcoreimage.zip` file with your custom certificate file and name it `trustCertProxy`. Your custom certificate file will be placed in the `trustedcerts` directory in the .zip file.

   ```
   cd <path to the stage location>
   mkdir -p core/1.<nn>.0/stage/sysman/config/server/trustedcerts
   cp <your proxy custom certificate> core/1.<nn>.0/stage/sysman/config/
   server/trustedcerts/trustCertProxy
   zip -u agentcoreimage.zip core/1.<nn>.0/stage/sysman/config/server/
   trustedcerts/trustCertProxy
   ```

   For example if you have 1.42 version and extracted the installation software under `/u01/stage`directory, you can run the following:

   ```
   cd /u01/stage
   mkdir -p core/1.42.0/stage/sysman/config/server/trustedcerts
   cp mycert.der core/1.42.0/stage/sysman/config/server/trustedcerts/
   trustCertProxy
   zip -u agentcoreimage.zip core/1.42.0/stage/sysman/config/server/
   trustedcerts/trustCertProxy
   ```

6. Run the agent installation script to install a gateway.

   ```
   ./AgentInstall.sh
   ```

7. Your gateway installation is now complete. Next step is to Verify the Gateway Installation.

Install a Gateway with Custom Certificates on Windows hosts

To perform a gateway installation over a proxy server when your proxy server has custom certificates on Windows, ensure to do a right-click and select **Run as administrator** to open an Administrator command prompt and perform the following:

1. Contact the IT Security team within your organization and obtain the correct custom certificate (root certificate) before proceeding. See Custom Certificates for more details.

   Confirm the custom certificate is saved in DER format. Typically these certificate files would have a `.der` extension. For example, it can be saved as `mycert.der`.

2. Review and confirm that you have performed the steps listed in Generic Prerequisites for Deploying Oracle Management Cloud Agents, Download the Oracle Management Cloud Agent Software and Prerequisites for Installing a Gateway.

3. Ensure that you have correctly updated and saved the response file (`gateway.rsp`). See Registration Parameters for Installing a Gateway and based on your requirements also, Optional Parameters for Installing a Gateway.

4. Log in to the host where you are planing to install the gateway, open Windows Explorer, navigate to the directory where you have staged the gateway installation software ZIP file and double-click the ZIP file to confirm `agentcoreimage.zip` file exists.

5. Update the `agentcoreimage.zip` file with your custom certificate file and name it `trustCertProxy`: Using Windows Explorer, navigate into the zipped file `agentcoreimage.zip` up to the `trustedcerts` directory (`core\<version number>\stage\sysman\config\server\trustedcerts`) and copy the custom certificate (root certificate) as file `trustCertProxy` into it. This will automatically update the `agentcoreimage.zip` ZIP file.
6. Run the agent installation script to install a gateway.

   ```
   AgentInstall.bat
   ```

7. Your gateway installation is now complete. Next step is to Verify the Gateway Installation.

Install a Gateway Using Reinstall Option

This section discusses installing a gateway using the `REINSTALL` parameter from the response file.

Install a Gateway Using Reinstall Option

You can use the `REINSTALL` parameter to reinstall a gateway that has been deleted manually from a host or it was running on a host which was decommissioned or it had a hardware failure. It is very useful in environments where hosts are being provisioned and reprovisioned on demand.

The reinstall option works in the following case:

- The gateway was not deleted from OMC before the host went down and it is still registered/listed in OMC.
- The old and new hosts must have the same OS type and same host name.

  Different OS types/versions or different host names are not supported.

The gateway must be reinstalled from a stage (`ZIP` file) of the same version as the gateway registered/listed in OMC. For example, if the gateway from the old host had a gateway with agent version 1.39 installed on it, then you must perform the reinstallation using the same agent software version, in this case version 1.39. Also, the values for the parameters: `AGENT_PORT` and `AGENT_BASE_DIRECTORY` need to be the same in both the old and new hosts.

Before proceeding, be sure to:

- Review the Prerequisites for Installing a Gateway.
- Specify the values of the Registration Parameters in the response file.
- Review the Install the Cloud Agent from a Shared Location for environments where the agent installation is automated and you have a shared/central location to stage the agent software and/or the response file.

To perform the gateway installation using the reinstall option:

1. Log on to the host where you will install the gateway and navigate to the directory where you extracted the gateway ZIP file that you previously downloaded. See Download the Oracle Management Cloud Agent Software for more details.
2. Have your response file ready. Ensure that you have entered the values for the mandatory parameters: `TENANT_NAME`, `OMC_URL` and `AGENT_REGISTRATION_KEY` in the response file (`gateway.rsp`).

Confirm that the values for the parameters: `AGENT_BASE_DIRECTORY` and `AGENT_PORT` are the same as the old host.

Edit the optional parameter `REINSTALL` and enter the value: `true`.

```
REINSTALL=true
```

Based on your requirement, edit any additional parameters if the default values are not in line with your best practices. See Parameters for Installing a Gateway for more details.

3. Run the `AgentInstall` agent installation script to install a gateway.
   - If you are installing a gateway on a UNIX-based host:

     ```
     ./AgentInstall.sh
     ```

   - If you are installing a gateway on a Windows host, right-click and select **Run as administrator** to open an Administrator command prompt and run the following:

     ```
     AgentInstall.bat
     ```

Your gateway installation using reinstall option is now complete. The gateway you just installed will attach to the old gateway you have in OMC and inherit its historical data. Next step is to Verify the Gateway Installation.

Verify the Gateway Installation

After installing the gateway, you must verify the installation.

To verify the gateway installation, perform the following steps:

1. Click the **OMC Navigation** menu, and then click **Agents** under **Administration**.

   The Oracle Management Cloud Agents page is displayed.

2. Click **Gateways** on the left navigation pane.
3. Check **Agent Display Name** column from the agent list to see if the host name of your deployed gateway exists on the list of available gateways.

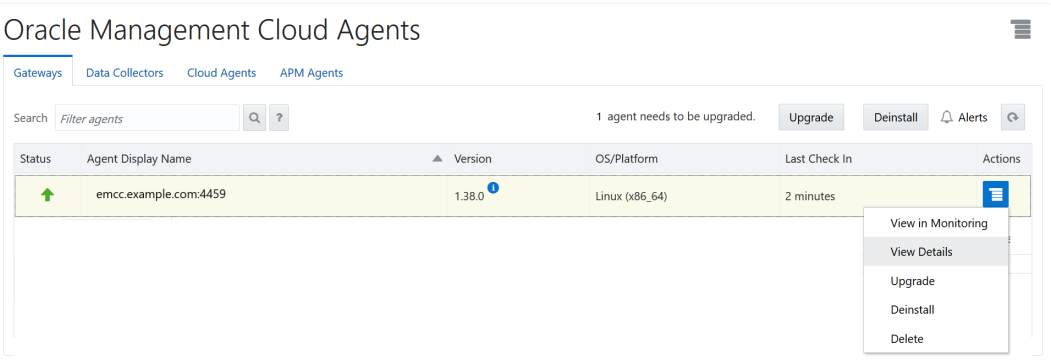
   You can right click on the agent list to select the specific columns that you want to see on the list.

4. Select your deployed gateway.

   The **Last Check In** column displays how much time has passed since the agent was last checked in/deployed.

   The **Actions** column displays a menu with different actions available.

5. Click Actions menu and select **View Details**.



The **View Details** action opens up a window with agent details like host name, agent version, OS platform and logs location. You can also see the registration key value that you used when you deployed the agent. At the bottom of the window, you can see a History section with **Operation Type** and **Status** information. **Operation Type** will list the operations performed on the specific agent (for example: install, upgrade, deinstall or delete) along with a link to the Lifecycle Tasks details page to see details of the specific operation. See Agent Lifecycle Tasks for more details.

You can also use the following `omcli` command from the *<AGENT_BASE_DIRECTORY>*`/agent_inst/bin` directory to verify whether the gateway was successfully deployed:

```
./omcli status agent
```

```
$  ./omcli status agent
Oracle Management Cloud Gateway
Copyright (c) 1996, 2018 Oracle Corporation.  All rights reserved.
------------------------------------------------------------
Version             : 1.38.0
State Home          : /scratch/emaas/gateway/gateway_home/agent_inst
Log Directory       : /scratch/emaas/gateway/gateway_home/agent_inst/sysman/log
Binaries Location   : /scratch/emaas/gateway/gateway_home/core/1.38.0
Process ID          : 17336
Parent Process ID   : 17249
URL                 : https://emcc.example.com:4459/emd/main/
Started at          : 2019-01-17 15:59:31
Started by user     : oracle
Operating System    : Linux version 3.8.13-118.24.2.el6uek.x86_64 (amd64)
Registered entities : 2
Sender Status               : FUNCTIONAL
Data Receiver Upload Status : FUNCTIONAL
Last successful upload      : 2019-01-21 19:13:12
Last attempted upload       : 2019-01-21 19:13:12
Gateway Pending Files (MB)  : 0
Gateway Pending Files       : 4
Backoff Expiration          : (none)

------------------------------------------------------------
Agent is Running and Ready
```

Enable Gateway Monitoring

You can monitor the gateway using the dashboard. This option is enabled by default.

If you're an existing customer and have purchased standalone Oracle Management Cloud services, you must enable the monitoring services to view the gateways in the monitoring user interface.

Perform the following steps to enable monitoring for gateways:

1. Log in to Oracle Management Cloud console with Admin privileges.
2. Click the **OMC Navigation** icon.
3. Under **Administration**, click **Entities Configuration**.
4. In the Entities Configuration screen, click **Enable/Disable Services**.
5. In the Enable/Disable Services dashboard, click the Select Entities drop-down list and select the gateway that you want to monitor.
6. Click **Enable Services**.
7. Select Monitoring Services, then click **Enable Services**.

Install Cloud Agents

This section discusses how to install cloud agents.

The cloud agents monitor and collect data (for example, metrics, configuration information, and logs) from entities that reside on hosts, or on virtual hosts in a cloud.

Topics:

Minimum System Requirements for Installing Cloud Agents

Minimum System Requirements

The following table lists the minimum system requirements to install cloud agents with default Host entity.

RAM	Kernel Parameters	Port Number	Free Disk Space
1 GB	Ulimit value for maximum user processes >=4000	4459 to 4479	1 GB*

*A cloud agent default buffer size is 100MB. If the gateway or the connectivity to Oracle Management Cloud is not available, the cloud agent will buffer the data to disk. In order to avoid loss of monitoring data during this period of no connectivity, it is recommended to have at least the default buffer size free.

Prerequisites for Installing Cloud Agents

Before you install cloud agents, you must meet a set of prerequisites.

This section lists the key considerations and prerequisites for installing cloud agents and covers the following:

General Guidelines

Follow these guidelines for installing cloud agents:

- It is recommended not to install cloud agents as a `root` user.
- An on-premises Oracle Enterprise Manager agent is not mandatory for installing cloud agents. But if there is an existing on-premises Oracle Enterprise Manager Cloud Control

in the data center, then the cloud agents can be installed either on the host on which the Oracle Enterprise Manager agent was installed or on any other host without the Oracle Enterprise Manager agent.

- The user for installing cloud agents can be the same as the user for installing the on-premises Oracle Enterprise Manager agent.

  If an Enterprise Manager agent was installed on the host on which the Oracle Management Cloud agent is to be installed, it is recommended that the cloud agent is installed under the same user as the Oracle Enterprise Manager agent. This allows the Oracle Management Cloud agent to access information about the managed entities such as databases, hosts, and so on.

  If the cloud agent has to be installed under a different user than the Oracle Enterprise Manager agent user, then the cloud agent must have read access to the files and directories under the `AGENT_HOME` directory of the Oracle Enterprise Manager agent. Otherwise, the cloud agent can't access information related to Oracle Enterprise Manager managed entities.

- Before proceeding, ensure that you understand and follow the instructions listed in Generic Prerequisites for Deploying Oracle Management Cloud Agents and Download the Oracle Management Cloud Agent Software.

Prerequisites Check Option

Before you install a cloud agent, you can check if you have met all the prerequisites to perform a seamless cloud agent installation. The `AgentInstall.sh` script reads the parameters values from the `agent.rsp` file and performs automated checks to ensure that your environment fulfills the basic requirements for the cloud agent installation.

Perform the following steps to run the prerequisites check:

1. On your Linux host, navigate to the agent directory where you saved the `agent.rsp` response file.
2. Open the response file using any standard editor.
3. Enter values for the mandatory parameters: `TENANT_NAME`, `OMC_URL`, and `AGENT_REGISTRATION_KEY`.

   Based on your requirement, edit the optional parameters if the default values are not in line with your best practices.
4. Save the response file.
5. Run the `AgentInstall.sh` script passing the parameter `EXECUTE_PREREQ=true` using the command line interface.

   For example, `./AgentInstall.sh|bat EXECUTE_PREREQ=true`

   If the prerequisite check fails, the script stops with relevant error message.

   If the prerequisite check completes successfully, you get the following message:

```
Unzipping agent software, this may take some time...
Installing Cloud Agent...
Executing Pre-requisite checks only for Cloud Agent...
Cloud Agent parameter validation started...
Cloud Agent pre-requisite checks started...
Pre-requisite checks completed for [Cloud Agent].
```

Alternatively, you can pass the required parameter values using the command line interface to perform the prerequisite check.

For example, `./AgentInstall.sh|bat TENANT_NAME=<TENANT_NAME> OMC_URL=<OMC_URL> AGENT_REGISTRATION_KEY=<AGENT_REGISTRATION_KEY> EXECUTE_PREREQ=true`

Please refer to the log file located under `<AGENT_ZIP_FILE_EXTRACTED_DIRECTORY>/AgentInstall_<timestamp>.log` for more details.

Cloud Agents: Typical Installation

This section discusses the typical installation of cloud agents.

- It is recommended not to use `root` user to install cloud agents.
- You install cloud agents by running the `AgentInstall` script from the command line. The `AgentInstall` script reads a set of parameters that can be specified in a response file (`agent.rsp`) or they can be passed along in the command line.
- A typical installation assumes the `agent.rsp` response file is saved under the *same directory* where you have saved the `Agentinstall` script. If that's not the case, then you must pass the `AGENT_RSP_FILE` parameter in the command line with the location of the response file when you run the `AgentInstall` script. See Install the Cloud Agent Specifying Parameters in the Command Line.
- If you have a proxy server or using custom certificates, be sure to check the steps listed in Install the Cloud Agent Over a Proxy Server and Install the Cloud Agent with Custom Certificates.

To perform a typical installation:

1. Identify a host in your data center with Internet access to Oracle Management Cloud.
2. Ensure that you have performed the steps listed in Prerequisites for Installing Cloud Agents.
3. Log on to the host where you will install the cloud agent and navigate to the directory where you have already extracted the cloud agent software ZIP file.

   For example, if you extracted the ZIP file to a directory named `cloud_agent` under the `/u01/stage` directory on your host, then the `Agentinstall` script will be present in the `/u01/stage/cloud_agent` directory after the ZIP file is extracted. Navigate from your present working directory to the `/u01/stage/cloud_agent` directory.
4. Edit the `agent.rsp` response file.

   Ensure you have updated the `agent.rsp` response file and specified the correct values of the parameters listed in Registration Parameters and Communication Parameters.

   Based on your requirement, you may also need to update the `agent.rsp` response file with values of the parameters listed in Optional Parameters.

   Once you are done editing, save the `agent.rsp` response file under the same directory where `AgentInstall` script is located.

   If you have a proxy server or using custom certificates, be sure to check the steps listed in Install the Cloud Agent Over a Proxy Server and Install the Cloud Agent with Custom Certificates.
5. Run the agent installation script to install a cloud agent.

- If you are installing a cloud agent on a UNIX-based host:

  ```
  ./AgentInstall.sh
  ```

  Alternatively, you can run: `sh AgentInstall.sh`

- If you are installing a cloud agent on a Windows host, right-click and select **Run as administrator** to open an Administrator command prompt and run the following:

  ```
  AgentInstall.bat
  ```

Your cloud agent installation is now complete. Next step is to Verify the Cloud Agent Installation.

Cloud Agents: Other Installation Use Cases

This section discusses other cloud agents installation use cases.

- It is recommended not to use `root` user to install a cloud agent.
- You install a cloud agent by running the `AgentInstall` script from the command line. The `AgentInstall` script requires a set of parameters that can be specified in a response file (`agent.rsp`) or they can be passed along through command line.
- If you haven't saved the `agent.rsp` response file in the *same directory* where you have saved the `AgentInstall` script, then you must pass the `AGENT_RSP_FILE` parameter in the command line when you run the `AgentInstall` script. See Install the Cloud Agent Specifying Parameters in the Command Line.

The following cloud agent use cases are covered:

- Install the Cloud Agent Specifying Parameters in the Command Line
- Install the Cloud Agent Over a Proxy Server
- Install the Cloud Agent with Custom Certificates
- Install the Cloud Agent Over a Gateway
- Gateway High Availability Use Cases
- Install the Cloud Agent from a Shared Location
- Install the Cloud Agent Using Reinstall Option

Install the Cloud Agent Specifying Parameters in the Command Line

This section discusses installing the cloud agent specifying parameters in the command line.

Perform the following before proceeding:

1. Review the Prerequisites for Installing Cloud Agents.
2. Ensure you have correctly configured the `agent.rsp` response file. See Registration Parameters and Communication Parameters.

You can perform a cloud agent installation specifying parameters in the command line or you can specify a combination of command line parameters and the use of a response file. You can do one of the following:

- Specify parameters only in the response file (See Cloud Agents: Typical Installation).

- Specify parameters only in the command line.
- Specify parameters in the command line and the response file. In this case, the parameter values specified in the command line gets priority over the same values specified in the response file.

Example 5-4 Specify parameters only in the command line:

```
./AgentInstall.sh|bat TENANT_NAME=<TENANT_NAME> OMC_URL=<OMC_URL>
AGENT_REGISTRATION_KEY=<AGENT_REGISTRATION_KEY>
AGENT_BASE_DIRECTORY=<AGENT_BASE_DIRECTORY>
```

In the above example, you specify the values of the parameters in the command line. The installation script will use the values of the mandatory parameters: `TENANT_NAME`,`OMC_URL`, `AGENT_REGISTRATION_KEY` and the optional parameter: `AGENT_BASE_DIRECTORY`.

Example 5-5 Specify parameters in the command line and the response file:

```
./AgentInstall.sh|bat AGENT_BASE_DIRECTORY=<AGENT_BASE_DIRECTORY>
```

In the above example, you specify the value of `AGENT_BASE_DIRECTORY` parameter in the command line and the rest of the parameters values are specified in the response file.

Example 5-6 Specify parameters in the command line and the response file if response file doesn't reside in the default location:

```
./AgentInstall.sh|bat AGENT_RSP_FILE=<absolute path to the agent.rsp file>
```

In the above example, you specify the value of `AGENT_RSP_FILE` parameter in the command line since it resides in a different location than the `AgentInstall` installation script file (by default, both files reside in the same directory). The rest of the parameters are specified in the response file.

Install the Cloud Agent Over a Proxy Server

This section discusses installing the cloud agent over a proxy.

Install the Cloud Agent Over a Proxy Server

If you are installing a cloud agent over a proxy server and haven't deployed a gateway, then ensure to perform the following before proceeding:

- Review the Prerequisites for Installing Cloud Agents.
- Specify the values of the Registration Parameters and Communication Parameters in the response file.
- Specify the values of the parameters listed in Parameters for Installing a Cloud Agent Over a Proxy Server in the response file.

To perform the cloud agent installation over a proxy server:

1. Log on to the host where you will install the cloud agent and navigate to the directory where you extracted the cloud agent ZIP file that you previously downloaded.
2. Have your response file ready. Ensure that you have specified the parameters for installing a cloud agent over a proxy server in the response file (`agent.rsp`), and it's saved under the same directory where the `AgentInstall` script is located. The `AgentInstall` script reads and obtains the values of the installation parameters from the response file at installation time.
3. Run the `AgentInstall` agent installation script to install a cloud agent.

- If you are installing a cloud agent on a UNIX-based host:

  ```
  ./AgentInstall.sh
  ```

- If you are installing a cloud agent on a Windows host, right-click and select **Run as administrator** to open an Administrator command prompt and run the following:

  ```
  AgentInstall.bat
  ```

If your organization decides to change the proxy server settings for security reasons after completing the agent installation, then you can modify the proxy server settings for your installed agents. See Change Proxy Server Settings After Installing Cloud Agents.

> **Note:**
>
> Oracle Management Cloud Agents (Cloud Agents, Data Collectors, Gateways) do not support NTLM Authorization Proxy Servers (APS).

Install the Cloud Agent with Custom Certificates

This section discusses installing a cloud agent over a proxy server when the proxy server has custom certificates.

Install the Cloud Agent with Custom Certificates on UNIX-based hosts

To perform a cloud agent installation over a proxy server when your proxy server has custom certificates on UNIX-based hosts:

1. Contact the IT Security team within your organization and obtain the correct custom certificate (root certificate) before proceeding. See Custom Certificates for more details.

   Confirm the custom certificate is saved in DER format. Typically these certificate files would have a `.der` extension. For example, it can be saved as `mycert.der`.

2. Review and confirm that you have performed the steps listed in Generic Prerequisites for Deploying Oracle Management Cloud Agents, Download the Oracle Management Cloud Agent Software and Prerequisites for Installing Cloud Agents.

3. Ensure that you have correctly updated and saved the response file (`agent.rsp`). See Registration and Communication Parameters. Also, based on your requirements see Proxy Parameters (Optional) and Other Optional Parameters .

4. Log in to the host where you are planing to install the cloud agent, navigate to the directory where you have extracted the cloud agent installation software and confirm `agentcoreimage.zip` file exists.

   ```
   cd <path to the stage location>
   ls -la agentcoreimage.zip
   ```

5. Update the `agentcoreimage.zip` file with your custom certificate file and name it `trustCertProxy`. Your custom certificate file will be placed in the `trustedcerts` directory in the `.zip` file.

   ```
   cd <path to the stage location>
   mkdir -p core/1.<nn>.0/stage/sysman/config/server/trustedcerts
   cp <your proxy custom certificate> core/1.<nn>.0/stage/sysman/config/
   server/trustedcerts/trustCertProxy
   zip -u agentcoreimage.zip core/1.<nn>.0/stage/sysman/config/server/
   trustedcerts/trustCertProxy
   ```

   For example if you have 1.42 version and extracted the installation software under `/u01/stage`directory, you can run the following:

   ```
   cd /u01/stage
   mkdir -p core/1.42.0/stage/sysman/config/server/trustedcerts
   cp mycert.der core/1.42.0/stage/sysman/config/server/trustedcerts/
   trustCertProxy
   zip -u agentcoreimage.zip core/1.42.0/stage/sysman/config/server/
   trustedcerts/trustCertProxy
   ```

6. Run the agent installation script to install a cloud agent.

   ```
   ./AgentInstall.sh
   ```

7. Your cloud agent installation is now complete. Next step is to Verify the Cloud Agent Installation.

Install a Cloud Agent with Custom Certificates on Windows hosts

To perform a cloud agent installation over a proxy server when your proxy server has custom certificates on Windows, ensure to do a right-click and select **Run as administrator** to open an Administrator command prompt and perform the following:

1. Contact the IT Security team within your organization and obtain the correct custom certificate (root certificate) before proceeding. See Custom Certificates for more details.

   Confirm the custom certificate is saved in DER format. Typically these certificate files would have a `.der` extension. For example, it can be saved as `mycert.der`.

2. Review and confirm that you have performed the steps listed in Generic Prerequisites for Deploying Oracle Management Cloud Agents, Download the Oracle Management Cloud Agent Software and Prerequisites for Installing Cloud Agents.

3. Ensure that you have correctly updated and saved the response file (`agent.rsp`). See Registration and Communication Parameters. Also, based on your requirements see Proxy Parameters (Optional) and Other Optional Parameters.

4. Log in to the host where you are planing to install the cloud agent, open Windows Explorer, navigate to the directory where you have staged the cloud agent installation software ZIP file and double-click the ZIP file to confirm `agentcoreimage.zip` file exists.

5. Update the `agentcoreimage.zip` file with your custom certificate file and name it `trustCertProxy`: Using Windows Explorer, navigate into the zipped file `agentcoreimage.zip` up to the `trustedcerts` directory `(core\<version number>\stage\sysman\config\server\trustedcerts)` and copy the custom certificate (root certificate) as file `trustCertProxy` into it. This will automatically update the `agentcoreimage.zip` ZIP file.

6. Run the agent installation script to install a cloud agent.

   ```
   AgentInstall.bat
   ```

7. Your cloud agent installation is now complete. Next step is to Verify the Cloud Agent Installation.

Install the Cloud Agent Over a Gateway

This section discusses installing the cloud agent over a gateway.

Install the Cloud Agent Over a Gateway

If your cloud agent communicates with Oracle Management Cloud through a gateway, then ensure to perform the following before proceeding:

- Review the Prerequisites for Installing Cloud Agents.
- Specify the values of the Registration Parameters and Communication Parameters in the response file.
- Specify the values of the gateway parameters listed in Communication Parameters in the response file.

> **Note:**
>
> The gateway host name you specify here must be the same name that was used to install the gateway. For example, if you deployed the gateway with `ORACLE_HOSTNAME=abc.xyz.com`, and you specify `GATEWAY_HOST=my.example.com` in the response file while installing the cloud agent, then the cloud agent registration will fail.

To perform the cloud agent installation over a gateway:

1. Log on to the host where you will install the cloud agent and navigate to the directory where you extracted the cloud agent ZIP file that you previously downloaded.
2. Have your response file ready. Ensure that you have specified the parameters for installing a cloud agent over a gateway in the response file (`agent.rsp`), and it's saved under the same directory where the `AgentInstall` script is located.
3. Run the `AgentInstall` agent installation script to install a cloud agent.
   - If you are installing a cloud agent on a UNIX-based host:

     ```
     ./AgentInstall.sh
     ```

   - If you are installing a cloud agent on a Windows host, right-click and select **Run as administrator** to open an Administrator command prompt and run the following:

     ```
     AgentInstall.bat
     ```

Gateway High Availability Use Cases

This section discusses gateway high availability use cases.

Gateway High Availability Use Cases

If you have deployed the cloud agent with a single gateway, and the gateway goes down, no data will be transmitted to Oracle Management Cloud. To avoid this, you can implement gateway high availability: you can deploy a second gateway and ensure that the cloud agent uses the second gateway to communicate with Oracle Management Cloud if the first gateway is down.

High availability of gateways is supported by configuring cloud agents with two or more gateway URLs. Cloud agents will load-balance between the two gateways. Since there are multiple paths for the data to flow to Oracle Management Cloud, loss of a single gateway will not affect the communication to Oracle Management Cloud.

The following use cases are supported:

- **Adding Additional Gateways while Deploying the Cloud Agent**

  You can deploy two gateways (`gateway_1 and gateway_2`) before you deploy the cloud agent. When you install the cloud agent, you must first specify the `gateway_1` host and port number and then specify `gateway_2` by passing the `ADDITIONAL_GATEWAYS` parameter. Run the following command on the host on which cloud agent is being deployed:

  `./AgentInstall.sh GATEWAY_HOST=<gateway_host_1> GATEWAY_PORT<gateway_port_1> ADDITIONAL_GATEWAYS=<https://<gateway_host_2>:<gateway_port_2>`

  where:

  – `gateway_host_1` is the host on which the first gateway is deployed.

  – `gateway_port_1` is the port number of the host on which the first gateway is deployed.

  – `gateway_host_2` is the host on which the second gateway is deployed.

  – `gateway_port_2` is the port number of the host on which the second gateway is deployed.

  > **Note:**
  >
  > You can get the gateway information by running the following command on the hosts on which the gateways are deployed: `<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli status agent`

- **Adding Additional Gateways to an Existing Deployed Cloud Agent**

  To add additional gateways to a cloud agent that has already been deployed with a gateway, follow these steps:

  1. Run the following command on the host on which you want to deploy the cloud agent with the first gateway:

     `./AgentInstall.sh AGENT_TYPE=cloud_agent AGENT_BASE_DIRECTORY=<the absolute path to the agent base directory>`

```
AGENT_REGISTRATION_KEY=<registration key value>
GATEWAY_HOST=<gateway_host_1> GATEWAY_PORT=<gateway_port_1>
```

2. Run the following command on the host on which you want to deploy the second gateway:

   ```
   ./AgentInstall.sh AGENT_TYPE=gateway AGENT_BASE_DIRECTORY=<the
   absolute path to the agent base directory>
   AGENT_REGISTRATION_KEY=<registration key value>
   ```

3. Run the following command on the host on which the second gateway was deployed to get the gateway URL.

   ```
   ./<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli status agent
   ```

   Example result of the preceding command:: `https://my.example.com:1838/test/main/`

4. Create a plain text file, `gateway.txt`, as follows:

   ```
   vi gateway.txt
   ```

   Insert the URL for the second gateway in the following format and save the file.

   ```
   gatewayUrls=https://<gateway_host_2>:<gateway_port_2>
   ```

5. Navigate to the `/bin` directory of the cloud agent and run the following command to add the gateway:

   ```
   ./<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli add_gateway agent
   <full path to the gateway.txt file>
   ```

6. Stop the cloud agent.

   ```
   ./omcli stop agent
   ```

7. Navigate to the `<AGENT_BASE_DIRECTORY>/core/1.<n>.0/stage/sysman/config/server/` directory on the gateway host that was added above and copy the `importCert` file to the cloud agent host as follows:

   ```
   <AGENT_BASE_DIRECTORY>/core/1.<n>.0/stage/sysman/config/server/
   trustedcerts/trustCertGateway_<gateway-host-added>
   ```

   Example: `<AGENT_BASE_DIRECTORY>/core/1.<n>.0/stage/sysman/config/server/trustedcerts/trustCertGateway_my_example_com_3476`

8. Back up the existing certificates directory.

   ```
   mv <AGENT_BASE_DIRECTORY>/agent_inst/sysman/config/server
    <AGENT_BASE_DIRECTORY>/agent_inst/config/server_bak

   mkdir  <AGENT_BASE_DIRECTORY>/agent_inst/sysman/config/server
   ```

9. Secure the cloud agent.

   ```
   ./omcli secure agent
   ```

10. Start the cloud agent.

    ```
    ./omcli start agent
    ```

11. Update the associations between Cloud Agent and the new Gateway.

    a. Click on the hamburger menu at the top left corner of the Console UI.

    b. Navigate to **Administration**>**Discovery**>**Entity Associations**.

c. Select the Cloud Agent from the drop down list which you have added the new Gateway.

d. Click **+ Add Associations**.

e. In the Popup, select Association Type: "**Uses**", click on **+ Add Destination Entities** and select the Gateways.

f. Once you are done, click the **Save**.

Install the Cloud Agent from a Shared Location

This section discusses installing the cloud agent from a shared location.

Install the Cloud Agent from a Shared Location

You can download the agent software ZIP file in a shared location and use it to install cloud agents on multiple hosts. This saves space on the host where you are installing the agent and ease of use in multi-host environments.

The agent software ZIP file required to install the agents can be saved and unzipped in a shared location. You can then install agents on multiple hosts that have access to this shared location.

Follow these steps to download the software ZIP file in a shared location.

As an administrator with full access to a shared location, perform the following:

1. Create or identify an existing shared directory. This will be referred to as `AGENT_IMAGE_LOCATION`.
2. Download and unzip the agent software ZIP file in this shared directory.

   `unzip` <your zip file name> -d <shared directory location>

   For example, `unzip cloudagent_linux.x64_1.29.0.zip -d /net/cloud_agent_bundle`

On the host(s) where you want to install the agents, perform the following:

1. Log in as the agent installation user (typically `oracle`).
2. Create a new local directory with write privileges. For example, `/u01/my_agent_install`
3. Copy the `AgentInstall.sh` script file from the shared location to a local directory on your host or run it from the shared location. You can have different possible scenarios for files location. See below for details of some example scenarios.

The install command format is the following:

```
<agent_image_location>/AgentInstall.sh [AGENT_IMAGE_LOCATION=<your shared
directory full path>] [EXTRACTION_LOCATION=<local temp directory>]
[AGENT_RSP_FILE=<full path to the agent.rsp, local or on the shared location>]
```

For example,

```
/net/cloud_agent_bundle/AgentInstall.sh AGENT_IMAGE_LOCATION=/net/
cloud_agent_bundle EXTRACTION_LOCATION=/tmp AGENT_RSP_FILE=/u01/
my_agent_install/agent.rsp
```

Notes:

- The values for AGENT_IMAGE_LOCATION, EXTRACTION_LOCATION, and AGENT_RSP_FILE parameters are passed through the command line only.

- If EXTRACTION_LOCATION is not specified, it defaults to AGENT_IMAGE_LOCATION.
- If the AGENT_IMAGE_LOCATION is not specified, it defaults to the directory where the `AgentInstall.sh` script resides.
- If AGENT_IMAGE_LOCATION is not writable, then the AGENT_IMAGE_LOCATION will be set to the current (.) directory. For Windows, the length of the directory path including the drive letter for the AGENT_IMAGE_LOCATION should be less than 23 characters.
- AGENT_RSP_FILE is the full path to the agent response file, `agent.rsp`. This file can be local or in the shared location. The shared location can be the same location as the shared software bundle or any other shared location. If the AGENT_RSP_FILE is not mentioned on the command line, then the script looks for it in the AGENT_IMAGE_LOCATION. Typically, if installing on multiple hosts you will want a local response file for each host. Copy the original `agent.rsp` file from the shared location to a local directory and customize it per your environment. For details on customizing your response file, see Parameters for Installing a Cloud Agent.
- If the response file and the `AgentInstall.sh` script are not co-located, then you must pass the `AGENT_RSP_FILE=<absolute path to the agent.rsp file>` parameter in the command line when you run the `Agentinstall.sh` script.

When you run the installer (`AgentInstall.sh`), by default, it checks for the `agentcoreimage.zip` in the same location where the shell script is present. If the `agentcoreimage.zip` is placed in another location, you have to specify the path to the directory where the agent software ZIP file is extracted. Edit the response file to pass the respective parameters to the installer. Specify the directory of the unzipped agent software bundle on the shared location. This directory should have read permission for the agent installation user and should be accessible from the host where the agent is being installed. The `agentcoreimage.zip` is extracted in the same location where the agent software ZIP file is extracted. If you want to extract the zip file on a different location, you must provide the extraction location.

The following are some example scenarios:

Scenario 1:
The software bundle (agent image) is on a shared location (host2). The `AgentInstall.sh` script and the response file (agent.rsp) are on the installation host (host1). The AGENT_IMAGE_LOCATION and EXTRACTION_LOCATION parameter values are provided. For example,

```
cd <directory where AgentInstall.sh resides>

./AgentInstall.sh AGENT_IMAGE_LOCATION=<your shared directory full path on
host2> EXTRACTION_LOCATION=<local temp directory on host2>
AGENT_RSP_FILE=<directory path to host1>/agent.rsp
```

Scenario 2:
The software bundle (agent image) is on a shared location (host2). The `AgentInstall.sh` script is on the installation host (host1). The AGENT_IMAGE_LOCATION, EXTRACTION_LOCATION, and AGENT_RSP_FILE parameter values that point to host2 are provided.

For example,

```
cd <directory where AgentInstall.sh resides>
```

```
./AgentInstall.sh EXTRACTION_LOCATION=<local temp directory on host2>
AGENT_IMAGE_LOCATION=<your shared directory full path on host2>
AGENT_RSP_FILE=<directory path to host2>/agent.rsp
```

Scenario 3:
The software bundle (agent image) and the `AgentInstall.sh` script are on a shared location (host2). The `AgentInstall.sh` has execute permission set for “others” (to provide execute permission: `chmod 777 AgentInstall.sh`). The AGENT_IMAGE_LOCATION and EXTRACTION_LOCATION parameter values are not provided.

For example,

```
cd <shared directory on host2 where AgentInstall.sh resides>

./AgentInstall.sh
```

In this case, the EXTRACTION_LOCATION will first default to AGENT_IMAGE_LOCATION. If AGENT_IMAGE_LOCATION is not writable, then the EXTRACTION_LOCATION will be set to the current directory. The agent installation user must have write permission in the current directory.

Scenario 4:
The software bundle (agent image) is on a shared location (host2). The AgentInstall.sh script is on host1. The AGENT_IMAGE_LOCATION and EXTRACTION_LOCATION parameter values that point to host2 are provided. The response file (agent.rsp) is on a different location, host3.

For example,

```
cd <directory where AgentInstall.sh resides>

./AgentInstall.sh EXTRACTION_LOCATION=<local temp directory on host2>
AGENT_IMAGE_LOCATION=<your shared directory full path on host2>
AGENT_RSP_FILE=<directory path to host3>/agent.rsp
```

Scenario 5:
The software bundle (agent image) and the `AgentInstall.sh` script are on a shared location (host2). The `AgentInstall.sh` has execute permission for “others”(to provide execute permission: `chmod 777 AgentInstall.sh`). Only the EXTRACTION_LOCATION parameter value is provided. Ensure that the EXTRACTION_LOCATION is writable by "others" (`chmod 777 local temp directory`).

For example,

```
cd <shared directory on host2 where AgentInstall.sh resides>

./AgentInstall.sh EXTRACTION_LOCATION=<local temp directory on host2>/tmp
```

In this case, the default value for AGENT_IMAGE_LOCATION is the directory in which the agent installation script resides.

Install the Cloud Agent Using Reinstall Option

This section discusses installing the cloud agent using the REINSTALL parameter from the response file.

Install the Cloud Agent Using Reinstall Option

You can use the REINSTALL parameter to reinstall a cloud agent that has been deleted manually from a host or it was running on a host which was decommissioned or it had a hardware failure. It is very useful in environments where hosts are being provisioned and reprovisioned on demand.

The reinstall option works in the following case:

- The cloud agent was not deleted from OMC before the host went down and it is still registered/listed in OMC.
- The old and new hosts must have the same OS type and same host name.

  Different OS types/versions or different host names are not supported.

The agent must be reinstalled from a stage (ZIP file) of the same version as the agent registered/listed in OMC. For example, if the agent from the old host had an agent with version 1.39 installed on it, then you must perform the reinstallation using the same agent software version, in this case version 1.39. Also, the values for the parameters: AGENT_PORT and AGENT_BASE_DIRECTORY need to be the same in both the old and new hosts.

Before proceeding, be sure to:

- Review the Prerequisites for Installing Cloud Agents.
- Specify the values of the Registration Parameters and Communication Parameters in the response file.
- Review the Install the Cloud Agent from a Shared Location for environments where the agent installation is automated and you have a shared/central location to stage the agent software and/or the response file.

To perform the cloud agent installation using the reinstall option:

1. Log on to the host where you will install the cloud agent and navigate to the directory where you extracted the cloud agent ZIP file that you previously downloaded. See Download the Oracle Management Cloud Agent Software for more details.
2. Have your response file ready. Ensure that you have entered the values for the mandatory parameters: TENANT_NAME, OMC_URL and AGENT_REGISTRATION_KEY in the response file (agent.rsp).

   Confirm that the values for the parameters: AGENT_BASE_DIRECTORY and AGENT_PORT are the same as the old host.

   Edit the optional parameter REINSTALL and enter the value: true.

   ```
   REINSTALL=true
   ```

   Based on your requirement, edit any additional parameters if the default values are not in line with your best practices. See Parameters for Installing a Cloud Agent for more details.

3. Run the `AgentInstall` agent installation script to install a cloud agent.
   - If you are installing a cloud agent on a UNIX-based host:

     `./AgentInstall.sh`
   - If you are installing a cloud agent on a Windows host, right-click and select **Run as administrator** to open an Administrator command prompt and run the following:

     `AgentInstall.bat`

```
./AgentInstall.sh
Unzipping agent software, this may take some time...
Installing Cloud Agent...
Cloud Agent parameter validation started...
Cloud Agent pre-requisite checks started...
REINSTALL flag is enabled, attempting to re-install the Agent...
Cloud Agent base directory creation started...
Security artifacts download started...
Cloud Agent setup started...
Registering Cloud Agent...
Starting Cloud Agent...
Cloud Agent started.
Cloud Agent installation completed.
Cloud Agent post installation checks started.
Cloud Agent is up and running.
Cloud Agent is communicating to Oracle Management Cloud.
Cloud Agent is monitored in Oracle Management Cloud.
Cloud Agent post installation checks completed.
To start Cloud Agent upon Operating System restart include '/omc_agent/ca/
agent_inst/bin/omcli start agent' in the start-up scripts.
For further details please refer http://www.oracle.com/pls/topic/lookup?
ctx=en/cloud/paas/management-cloud&id=deploy_agent.
```

Your cloud agent installation using reinstall option is now complete. The cloud agent you just installed will attach to the old cloud agent you have in OMC and inherit its historical data. Next step is to Verify the Cloud Agent Installation.

Post installation task: Add entities to the cloud agent.

You must add all the previous entities that were being monitored before on the old host.

You can use the `omcli` command line utility to add entities to Oracle Management Cloud. The `omcli add_entity` command adds the entities to Oracle Management Cloud by reading the entity details from JSON files that you create and pass as parameters to the command.

See Typical Workflow for Adding Entities in *Working with Oracle Management Cloud*.

Verify the Cloud Agent Installation

After installing the cloud agent, you must verify the installation.

To verify cloud agent installation, perform the following:

1. Click the **OMC Navigation** menu, and then click **Agents** under **Administration**.

   This displays the Oracle Management Cloud Agents page.
2. Click **Cloud Agents** on the left navigation pane.

3. Check **Agent Display Name** column from the agent list to see if the host name of your deployed cloud agent exists on the list of available cloud agents.

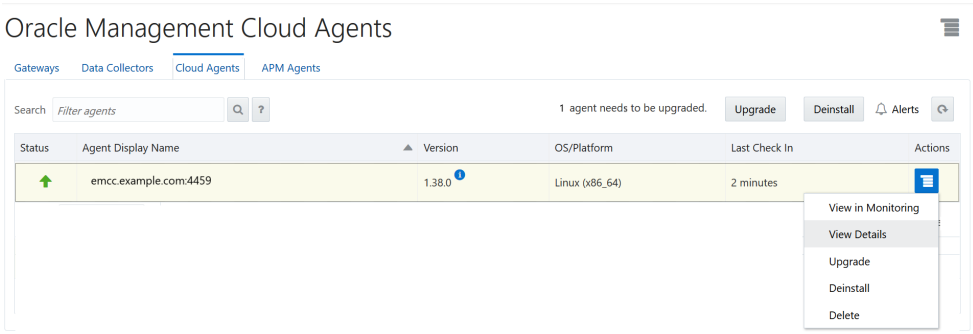
   You can right click on the agent list to select the specific columns that you want to see on the list.

4. Select your deployed cloud agent.

   The **Last Check In** column displays how much time has passed since the agent was last checked in/deployed.

   The **Actions** column displays a menu with different actions available.

5. Click Actions menu and select **View Details**.



   The **View Details** action opens up a window with agent details like host name, agent version, OS platform and logs location. You can also see the registration key value that you used when you deployed the agent. At the bottom of the window, you can see a History section with **Operation Type** and **Status** information. **Operation Type** will list the operations performed on the specific agent (for example: install, upgrade, deinstall or delete) along with a link to the Lifecycle Tasks details page to see details of the specific operation. See Agent Lifecycle Tasks for more details.

You can also use the following `omcli` command from the *<AGENT_BASE_DIRECTORY>*`/agent_inst/bin` directory to verify whether the cloud agent was successfully deployed:

```
./omcli status agent
```

```
$ ./omcli status agent
Oracle Management Cloud Agent
Copyright (c) 1996, 2018 Oracle Corporation.  All rights reserved.
---------------------------------------------------------------
Version                : 1.38.0
State Home             : /omc_agent/ca/agent_inst
Log Directory          : /omc_agent/ca/agent_inst/sysman/log
Binaries Location      : /omc_agent/ca/core/1.38.0
Process ID             : 16792
Parent Process ID      : 16668
URL                    : https://emcc.example.com:4459/emd/main/
Started at             : 2019-01-27 20:05:43
Started by user        : oracle
Operating System       : Linux version 3.8.13-98.1.2.el6uek.x86_64 (amd64)
Data Collector enabled : false
Sender Status          : FUNCTIONAL
Gateway Upload Status  : FUNCTIONAL
Last successful upload : 2019-01-27 20:12:18
Last attempted upload  : 2019-01-27 20:12:18
Pending Files (MB)     : 0.0z
Pending Files          : 66
Backoff Expiration     : (none)

---------------------------------------------------------------
Agent is Running and Ready
```

Next Steps: Defining Entities for Monitoring and Analysis

Software or hardware resources, as well as business objects whose properties, configuration, status, and performance are tracked and analyzed are known to Oracle Management Cloud as **entities**.

After you install agents, you must add the entities that you want to monitor.

> **Note:**
>
> Wait for a few minutes before using the newly installed cloud agent to add entities from the Add Entity page in the Oracle Management Cloud Administration console.

You use the Oracle Management Cloud agent command-line interface tool, `omcli`, to add the entities in your IT ecosystem to Oracle Management Cloud. The `omcli add_entity` command adds the entities to Oracle Management Cloud by reading the entity details from JSON-formatted files that you create and pass as parameters to the command.

See Typical Workflow for Adding Entities in *Working with Oracle Management Cloud* .

Install a Data Collector

This section discusses how to install a data collector.

A data collector can be used with an existing Oracle Enterprise Manager installation for collecting metrics and logs from the entities managed and monitored by the Oracle Enterprise Manager. For more information review Understand the Architecture of Oracle Management Cloud.

Topics:

Prerequisites for Installing a Data Collector

Before you install a data collector, you must meet a set of prerequisites.

This section lists the key considerations and prerequisites for installing data collectors and covers the following:

General Guidelines

Follow these guidelines for deploying data collectors:

- You can deploy a data collector without a gateway.
- You can deploy a data collector on a host on which the Oracle Management Repository is present or on another host that has SSH access to the remote host. You do not require an Oracle Enterprise Manager agent to deploy the data collector on either host.
- You can use the following command to access the Oracle Management Repository from an UNIX-based host:

  ```
  ssh -l <the_username_to_log_in_as_on_Oracle_Management_Repository>
  <Oracle_Management_Repository_host_IP_address>
  ```

- You need to create a user in the Oracle Management Repository. This will be the data collector user and it will be used to collect Oracle Enterprise Manager Cloud Control data. You will enter it as the value of DATA_COLLECTOR_USERNAME parameter from the data collector response file.
- Before you deploy data collectors to access Oracle Real Application Cluster (RAC) databases running the Oracle Management Repository (OMR), ensure the following:
  - The staging directory location specified for each RAC database node is the same location that was specified at the time of deploying the data collector.
  - The Oracle database user has read and write privileges on the staging directory.

  - The Oracle Management Repository host user (with SSH privileges to the Oracle Management Repository host) has read write privileges on the staging directory.

- Before proceeding, ensure that you understand and follow the instructions listed in Generic Prerequisites for Deploying Oracle Management Cloud Agents and Download the Oracle Management Cloud Agent Software.

Port Requirements

During the installation, the `AgentInstall` script assigns any available port number to the data collector.

Prerequisites Check

Before you install a data collector, you can check if you have met all the prerequisites to perform a seamless agent installation. The `AgentInstall.sh` script reads the parameters values from the `agent.rsp` file and performs automated checks to ensure that your environment fulfills the basic requirements for the data collector installation.

Perform the following steps to run the automated prerequisite check:

1. On your Linux host, navigate to the installer directory where you have the `agent.rsp` response file.
2. Open the response file using any standard editor.
3. Enter values for the mandatory parameters such as `TENANT_NAME`, `OMC_URL`, `AGENT_REGISTRATION_KEY`, `DATA_COLLECTOR_USERNAME`, `DATA_COLLECTOR_USER_PASSWORD`, `OMR_USERNAME`, `OMR_USER_PASSWORD`, `OMR_HOST_USERNAME`, `OMR_STAGE_DIR`, `OMR_HOST_USER_PASSWORD`, `OMR_HOSTNAME`, `OMR_PORT`, and `OMR_SID`.

   Based on your requirement, edit the optional parameters if the default values are not in line with your best practices.
4. Save the response file.
5. Run the `AgentInstall.sh` script passing the parameter `EXECUTE_PREREQ=true` using the command line interface.

   For example, `./AgentInstall.sh|bat EXECUTE_PREREQ=true`

   If the prerequisite check fails, the script stops with relevant error message.

   Alternatively, you can pass the required parameter values using the command line interface to perform the prerequisite check.

   For example, `./AgentInstall.sh|bat TENANT_NAME=<`*`TENANT_NAME`*`> OMC_URL=<`*`OMC_URL`*`> AGENT_REGISTRATION_KEY=<`*`AGENT_REGISTRATION_KEY`*`> DATA_COLLECTOR_USERNAME=<`*`DATA_COLLECTOR_USERNAME`*`> DATA_COLLECTOR_USER_PASSWORD=<`*`DATA_COLLECTOR_USER_PASSWORD`*`> OMR_USERNAME=<`*`OMR_USERNAME`*`> OMR_USER_PASSWORD=<`*`OMR_USER_PASSWORD`*`> OMR_HOST_USERNAME=<`*`OMR_HOST_USERNAME`*`> OMR_STAGE_DIR=<`*`OMR_STAGE_DIR`*`> OMR_HOST_USER_PASSWORD=<`*`OMR_HOST_USER_PASSWORD`*`> OMR_HOSTNAME=<`*`OMR_HOSTNAME`*`> OMR_PORT=<`*`OMR_PORT`*`> OMR_SID=<`*`OMR_SID`*`> EXECUTE_PREREQ=true`

   Please refer to the log file located under <*`AGENT_ZIP_FILE_EXTRACTED_DIRECTORY`*>/`AgentInstall_<`*`timestamp`*`>.log` for more details.

Create a Dynamic Group in Oracle Enterprise Manager

The owner of a dynamic group specifies the membership criteria during dynamic group creation (or modification) and membership in the group is determined solely by the criteria

specified. Membership in a dynamic group cannot be modified directly. Enterprise Manager automatically adds targets that match the membership criteria when a dynamic group is created. It also updates group membership as new targets are added or target properties are changed and the targets match the group's membership criteria.

To create a dynamic group:

1. Sign in to your on-premises Enterprise Manager Cloud Control as a user with administrative rights.
2. In your on-premises Enterprise Manager Cloud Control, from the Groups page, click **Create** and then select **Dynamic Group** from the drop-down list. Alternately, you can choose **Add Target** from the **Setup** menu and then select **Group**.
3. On the **General** tab of the Create Dynamic Group page, enter `omcgroup` as **Name** of the dynamic group you want to create. To create a regular dynamic group, the View any Target system wide privilege is required as the group owner must be able to view any target that can potentially match the membership criteria.
4. In the **Define Membership Criteria** section, define the criteria for the dynamic group membership by clicking **Define Membership Criteria**.

   The Define Membership Criteria page appears where you can **Add** or **Remove** properties of targets to be included in the group. Group members must match one value in each of the populated target properties. Use the **Member Preview** section to review a list of targets that match the criteria. Click **OK** to return to the General page.

   At least one of the criteria on the Define Membership Criteria page must be specified. You cannot create a dynamic group without at least one of the target types, on hosts or target properties specified. Use the following criteria for dynamic groups:

   - Target type
   - Department
   - On Host
   - Target Version
   - Lifecycle Status
   - Operating System
   - Line of Business
   - Platform
   - Location
   - CSI
   - Cost Center
   - Contact
   - Comment
5. You can add or remove properties using the **Add** or **Remove** Target Properties button on the Define Membership Criteria page.
6. Click **OK** to create the dynamic group.

Grant Permissions to Cloud Agent Files

You can install the cloud agent as an on-premises Oracle Enterprise Manager (EM) agent host user. If the cloud agent user is different than the EM user then both OS users must be part of the same OS user group with the required permissions provided.

The cloud agent obtains the monitoring credentials from the on-premises EM agent from the following files:

- `AGENT_HOME/agent_inst/sysman/emd/targets.xml`
- `AGENT_HOME/agent_inst/sysman/config/private.properties`

Where `AGENT_HOME` is the EM agent installation directory.

If the cloud agent is installed as a different host user, read access to these files must be provided.

For read access, log in to the host as an on-premises EM agent host user and grant the following permissions:

```
cd $AGENT_HOME/agent_inst    # AGENT_HOME is the EM agent installation
directory
chmod g+x sysman
chmod g+x sysman/emd
chmod g+x sysman/config
```

By default, users in the same group should have read permissions on the `sysman/emd/targets.xml` and `sysman/config/private.properties` files. If not, grant the following permissions while still logged in as the EM agent host user:

```
cd $AGENT_HOME/agent_inst    # AGENT_HOME is the EM agent installation
directory
chmod g+r sysman/emd/targets.xml
chmod g+r sysman/config/private.properties
```

Granting execution permissions allows all users in a group to access directories and read the monitoring credentials for other targets. To ensure security, we recommend that you install the cloud agent using the same user as the EM agent.

Data Collection Scenarios

Data Collection Scenarios

By default, a data collector harvests metrics data, such as availability, configuration, and performance from all the entities that are managed and monitored by an existing on-premises Oracle Enterprise Manager Cloud Control. However, you can also collect data from selected entities defined in an on-premises Enterprise Manager Cloud Control. This helps you view data from only the entities that you want to monitor, which lets you troubleshoot problems faster.

- **Collect Data for All Entities**
- **Collect Data for Selected Entities**

Collect Data for All Entities

If you want to collect metrics from all entities that are monitored by an existing on-premises Oracle Enterprise Manager Cloud Control:

1. Ensure that you adhere to the General Guidelines and meet the Generic Prerequisites for Deploying Oracle Management Cloud Agents and Port Requirements.
2. Install the Oracle Management Cloud agents in the following order:
   - Gateway (optional)
   - Data collector
   - Cloud agent

What Data Is Collected?

Scenario 1: If you're an existing customer and have purchased standalone Oracle Management Cloud services (such as Oracle Infrastructure Monitoring, Oracle IT Analytics, and so on), the data collector will harvest:

- All entity data; consists of entity information, entity properties, and associations.
- All metrics for all entities; consists of all availability, configuration, and performance metrics and includes historical and current data after the entity has been discovered.

Scenario 2: If you're a new customer and have purchased Oracle Management Cloud licensed editions (such as Standard Edition or Enterprise Edition):

- Have purchased Oracle Management Cloud Standard Edition:
  - All entity data
  - Current metrics (consists of current availability, configuration, and performance metrics after the entity is enabled or licensed; no history is collected.) only for enabled entities (entities that have been enabled for IT Analytics.)
- Have purchased Oracle Management Cloud Enterprise Edition:
  - All entity data
  - All data only for enabled entities

Collect Data for Selected Entities

If you do not add the entities (host, agent, listener, database machine, and so on) to the `omcgroup`, you cannot enable IT Analytics.

The process of collecting metrics data from selected entities is:

1. Create a dynamic group (see Create a Dynamic Group in Your On-Premises Enterprise Manager) called `omcgroup` in your on-premises Enterprise Manager Cloud Control that will contain only those member entities whose data you want to collect and upload. The Enterprise Manager Agent must also be part of the `omcgroup`.

   If you had not created the `omcgroup` before the data collector was deployed, you can create it after deployment and the entities in the newly created `omcgroup` will be included in the next data collection. You do not have to restart the data collector.

A member entity can be a single entity or a group that contains nested entities and groups. Oracle Management Cloud supports collecting and uploading data from the direct members of `omcgroup` and nested members.

> **Note:**
>
> All the entities on which you want to enable Oracle IT Analytics should exist as members of `omcgroup`.

2. Ensure that you adhere to the General Guidelines and meet the Generic Prerequisites for Deploying Oracle Management Cloud Agents and Port Requirements.
3. Install the Oracle Management Cloud agents in the following order:
   - Gateway (optional)
   - Data collector
   - Cloud agent

What Data Is Collected?

Depending on the type of the Oracle Management Cloud offerings that you've subscribed to, selective data collection varies.

Scenario 1: If you're a new customer and have purchased Oracle Management Cloud licensed editions (such as Standard Edition or Enterprise Edition), even if the `omcgroup` has been created, the metrics will not be loaded until you enable Enterprise Edition (EE) on the entities. However, all entities will be added whether you create a group or not.

Status of `omcgroup`	Standard Edition (SE) Enabled	Enterprise Edition (EE) Enabled
`omcgroup` defined	• Entity data for entities in `omcgroup` collected • Current data only for SE enabled entities	• Entity data for entities in `omcgroup` collected • All data for EE enabled entities
`omcgroup` deleted after initial creation	• Entity data collection changed from `omcgroup` to all entities • No change in current metrics collection (defined by SE enabled entities)	• Entity data collection changed from `omcgroup` to all entities • No change in all metrics collection (defined by EE enabled entities)
`omcgroup` created later	• Entity data updates changed from all entities to `omcgroup` only • No change in current metrics collection (defined by SE enabled entities)	• Entity data updates changed from all entities to `omcgroup` only • No change in all metrics collection (defined by EE enabled entities)

Scenario 2: If you're an existing customer and have purchased standalone Oracle Management Cloud services (such as Oracle Infrastructure Monitoring, Oracle IT Analytics, and so on), the data collector will harvest all entities if `omcgroup` is not created. If you create an `omcgroup` later, then it will harvest just the group, but the entities would have already been harvested and added, and metrics loaded.

Status of omcgroup	Data Collection Use case
omcgroup defined	• Entity data for entities in omcgroup • All metrics for entities in omcgroup
omcgroup deleted after initial creation	• Entity data collection changed from omcgroup only to all entities • All metrics collection changed from omcgroup only to all entities
omcgroup created later	• Entity data updates changed from all entities to omcgroup only • All metrics collection changed from all entities to omcgroup only

Data Collector: Typical Installation

This section discusses the typical installation of a data collector.

- It is recommended not to use root user to install a data collector.
- You install a data collector by running the AgentInstall script from the command line. The AgentInstall script reads a set of parameters that can be specified in a response file (agent.rsp) or they can be passed along in the command line.
- A typical installation assumes the agent.rsp response file is saved under the same directory where you have saved the AgentInstall script. If that's not the case, then you must pass the AGENT_RSP_FILE parameter in the command line with the location of the response file when you run the AgentInstall script. See Install a Data Collector Specifying Parameters in the Command Line.

To perform a typical installation:

If you are installing the data collector without a gateway, then install the data collector on a host that has access to the Internet, either directly or through a proxy server.

To install the data collector, follow these steps:

1. Identify a host in your data center with Internet access to Oracle Management Cloud.
2. Ensure that you have performed the steps listed in Prerequisites for Installing a Data Collector.
3. Log on to the host where you will install the data collector and navigate to the directory where you have already extracted the data collector software ZIP file.

   For example, if you extracted the data collector software ZIP file to a directory named datacollector_agent under the /scratch directory on your host, then the Agentinstall script will be present in the /scratch/datacollector_agent/ directory after the ZIP file is extracted. Navigate from your present working directory to the /scratch/datacollector_agent directory.

   If you haven't completed this step previously, see Download the Oracle Management Cloud Agent Software.
4. Edit the agent.rsp response file.

   When the data collector software ZIP file is downloaded and extracted, a sample response file, agent.rsp, is provided as a template. Ensure that you have updated

the `agent.rsp` response file and specified the correct values of the parameters listed in Registration Parameters for Installing Cloud Agents and Communication Parameters for Installing Cloud Agents based on your requirements.

Also, ensure that you have updated the `agent.rsp` response file with the correct values of the data collector parameters listed in Data Collector Parameters. You may need to specify additional data collector parameters listed in Optional Data Collector Parameters based on your requirements.

5. Run the agent installation script to install the data collector.
   - If you are installing the data collector on a UNIX-based host:

     ```
     ./AgentInstall.sh
     ```

     Alternatively, you can run: `sh AgentInstall.sh`
   - If you are installing the data collector on a Windows host, right-click and select **Run as administrator** to open an Administrator command prompt and run the following:

     ```
     AgentInstall.bat
     ```

Your data collector installation is now complete. Next step is to Verify the Data Collector Installation.

Data Collector: Other Installation Use Cases

This section discusses other data collector installation use cases.

- It is recommended not to use `root` user to install a data collector.
- You install a data collector by running the `AgentInstall` script from the command line. The `AgentInstall` script reads a set of parameters that can be specified in a response file (`agent.rsp`) or they can be passed along in the command line.
- If you haven't saved the `agent.rsp` response file in the same directory where you have saved the `AgentInstall` script, then you must pass the `AGENT_RSP_FILE` parameter in the command line with the location of the response file when you run the `AgentInstall` script. See Install a Data Collector Specifying Parameters in the Command Line.

The following data collector use cases are covered:

- Install a Data Collector Specifying Parameters in the Command Line
- Install a Data Collector Over a Proxy Server
- Install a Data Collector Over a Gateway
- Install a Data Collector with a Locked Account
- Install a Data Collector using Reinstall Option
- Upgrade to Enterprise Manager 13.X after Installing a Data Collector
- Install a Data Collector on Oracle Real Application Clusters
- Modify the Data Collector Connect String or SSH Port After Deployment
- Specify a Custom SSH Port while Deploying the Data Collector

Install a Data Collector Specifying Parameters in the Command Line

This section discusses installing a data collector specifying parameters in the command line.

Perform the following before proceeding:

1. Review the Prerequisites for Installing a Data Collector.
2. Ensure you have correctly configured the `agent.rsp` response file and specified the correct values of the parameters listed in Registration Parameters for Installing Cloud Agents and Communication Parameters for Installing Cloud Agents based on your requirements.

   Also, ensure that you have updated the `agent.rsp` response file with the correct values of the data collector parameters listed in Data Collector Parameters. You may need to specify additional data collector parameters listed in Optional Data Collector Parameters based on your requirements.

You can perform a data collector installation specifying parameters in the command line or you can specify a combination of command line parameters and the use of a response file. You can do one of the following:

- Specify parameters only in the response file (See Data Collector: Typical Installation).
- Specify parameters only in the command line.
- Specify parameters in the command line and the response file. In this case, the parameter values specified in the command line gets priority over the same values specified in the response file.

Example 5-7 Specify parameters only in the command line:

```
./AgentInstall.sh|bat TENANT_NAME=<TENANT_NAME> OMC_URL=<OMC_URL>
AGENT_REGISTRATION_KEY=<AGENT_REGISTRATION_KEY>
AGENT_BASE_DIRECTORY=<AGENT_BASE_DIRECTORY>
DATA_COLLECTOR_USERNAME=<DATA_COLLECTOR_USERNAME>
DATA_COLLECTOR_USER_PASSWORD=<DATA_COLLECTOR_USER_PASSWORD>
OMR_USERNAME=<OMR_USERNAME> OMR_USER_PASSWORD=<OMR_USER_PASSWORD>
OMR_HOST_USERNAME=<OMR_HOST_USERNAME> OMR_STAGE_DIR=<OMR_STAGE_DIR>
OMR_HOST_USER_PASSWORD=<OMR_HOST_USER_PASSWORD>
OMR_HOSTNAME=<OMR_HOSTNAME> OMR_PORT=<OMR_PORT> OMR_SID=<OMR_SID>
```

In the above example, you specify the values of the parameters in the command line. The installation script will use the values of the parameters provided.

Example 5-8 Specify parameters in the command line and the response file:

```
./AgentInstall.sh|bat AGENT_BASE_DIRECTORY=<AGENT_BASE_DIRECTORY>
```

In the above example, you specify the value of `AGENT_BASE_DIRECTORY` parameter in the command line and the rest of the parameters values are specified in the response file.

Example 5-9 Specify parameters in the command line and the response file if response file doesn't reside in the default location:

```
./AgentInstall.sh|bat AGENT_RSP_FILE=<absolute path to the agent.rsp file>
```

In the above example, you specify the value of `AGENT_RSP_FILE` parameter in the command line since it resides in a different location than the `AgentInstall` installation script file (by default, both files reside in the same directory). The rest of the parameters are specified in the response file.

Install a Data Collector Over a Proxy Server

This section discusses installing a data collector over a proxy server.

Install a Data Collector Over a Proxy Server

If you are installing a data collector over a proxy server, ensure to perform the following before proceeding:

- Review the Prerequisites for Installing a Data Collector.
- Specify the values of the Registration Parameters for Installing Cloud Agents and Communication Parameters for Installing Cloud Agents in the response file based on your requirements.
- Specify the values of the Data Collector Parameters and Optional Data Collector Parameters in the response file based on your requirements.
- Specify the values of proxy-related parameters listed in Parameters for Installing Any Agent Over a Proxy Server in the response file.

To perform a data collector installation over a proxy server:

1. Log on to the host where you will install the data collector and navigate to the directory where you extracted the data collector software ZIP file that you previously downloaded.

   If you haven't completed this step previously, see Download the Oracle Management Cloud Agent Software.

2. Edit your `agent.rsp` response file. Ensure that you have specified the parameters for installing a data collector over a proxy server in the response file (`agent.rsp`), and it's saved under the same directory where the `AgentInstall` script is located.

3. Run the `AgentInstall` installation script to install a data collector.

   - If you are installing a data collector on a UNIX-based host:

     ```
     ./AgentInstall.sh
     ```

   - If you are installing a data collector on a Windows host, right-click and select **Run as administrator** to open an Administrator command prompt and run the following:

     ```
     AgentInstall.bat
     ```

> **Note:**
>
> Oracle Management Cloud Agents (Cloud Agents, Data Collectors, Gateways) do not support NTLM Authorization Proxy Servers (APS).

Install a Data Collector Over a Gateway

This section discusses installing a data collector over a gateway.

Install a Data Collector Over a Gateway

If your data collector communicates with Oracle Management Cloud through a gateway, ensure to perform the following before proceeding:

- Review the Prerequisites for Installing a Data Collector.
- Specify the values of the Registration Parameters for Installing Cloud Agents and Communication Parameters for Installing Cloud Agents in the response file based on your requirements.
- Specify the values of the Data Collector Parameters and Optional Data Collector Parameters in the response file based on your requirements.
- Specify the values of the Communication Parameters for Installing a Data Collector or a Cloud Agent Over a Gateway in the response file.
- If your organization connects to the Internet over a proxy server, then you also need to specify the values of the proxy-related parameters listed in Parameters for Installing Any Agent Over a Proxy Server in the response file.

To perform a data collector installation over a gateway:

1. Log on to the host where you will install the data collector and navigate to the directory where you extracted the data collector software ZIP file that you previously downloaded.

   If you haven't completed this step previously, see Download the Oracle Management Cloud Agent Software.

2. Edit your `agent.rsp` response file. Ensure that you have specified the parameters for installing a data collector over a gateway in the response file (`agent.rsp`), and it's saved under the same directory where the `AgentInstall` script is located.
3. Run the `AgentInstall` installation script to install a data collector.
   - If you are installing a data collector on a UNIX-based host:

     ```
     ./AgentInstall.sh
     ```

   - If you are installing a data collector on a Windows host, right-click and select **Run as administrator** to open an Administrator command prompt and run the following:

     ```
     AgentInstall.bat
     ```

Install a Data Collector with a Locked Account

This section discusses installing a data collector when having a locked account.

Install a Data Collector with a Locked Account

If you are installing a data collector and you don't have the password for the `OMR_HOST_USERNAME` (typically `oracle` OS user), then at installation time, you can pass an operating system user instead of `OMR_HOST_USERNAME` that meets the following requirements:

- Ensure that an operating system user (for example, `User_A` has SSH access to Oracle Management Repository), who has read/write permissions on `OMR_STAGE_DIR`, exists.
- Ensure that the operating system user (`oracle`) who owns the Oracle Management Repository database Oracle Home also has read/write permissions on `OMR_STAGE_DIR`.
- When running the `AgentInstall.sh` script, specify `OMR_HOST_USERNAME=User_A` and its password in the response file.
- In case of a Real Application Cluster Oracle Management Repository database environment, ensure that `OMR_STAGE_DIR` is accessible from all the instances and the data collector host, and `OMR_HOST_USERNAME` and the operating system user who owns the Oracle Home of the Oracle Management Repository database both have read/write permissions to `OMR_STAGE_DIR`.

Install a Data Collector using Reinstall Option

This section discusses installing a data collector using the `REINSTALL` parameter from the response file.

Install a Data Collector using Reinstall Option

You can use the `REINSTALL` parameter to reinstall a data collector that has been deleted manually from a host or it was running on a host which was decommissioned or it had a hardware failure. It is very useful in environments where hosts are being provisioned and reprovisioned on demand.

The reinstall option works in the following case:

- The data collector was not deleted from OMC before the host went down and it is still registered/listed in OMC.
- The old and new hosts must have the same OS type and same host name.

  Different OS types/versions or different host names are not supported.

The data collector must be reinstalled from a stage (`ZIP` file) of the same version as the data collector registered/listed in OMC. For example, if the data collector from the old host had an agent with version 1.39 installed on it, then you must perform the reinstallation using the same agent software version, in this case version 1.39. Also, the values for the parameters: `AGENT_PORT` and `AGENT_BASE_DIRECTORY` need to be the same in both the old and new hosts.

Before proceeding, be sure to:

- Review the Prerequisites for Installing a Data Collector.
- Specify the values of the Registration Parameters for Installing Cloud Agents and Communication Parameters for Installing Cloud Agents in the response file.
- Specify the values of the Data Collector Parameters in the response file.
- Review the Optional Parameters for Installing Cloud Agents and Optional Data Collector Parameters in the response file.
- Review the Install the Cloud Agent from a Shared Location for environments where the agent installation is automated and you have a shared/central location to stage the agent software and/or the response file.

To perform the data collector installation using the reinstall option:

1. Log on to the host where you will install the data collector and navigate to the directory where you extracted the data collector ZIP file that you previously downloaded. See Download the Oracle Management Cloud Agent Software for more details.
2. Have your response file ready. Ensure that you have entered the values for the mandatory parameters: `TENANT_NAME`, `OMC_URL` and `AGENT_REGISTRATION_KEY`, and the Data Collector Parameters in the response file (`agent.rsp`).

   Confirm that the values for the parameters: `AGENT_BASE_DIRECTORY` and `AGENT_PORT` are the same as the old host.

   Edit the optional parameter `REINSTALL` and enter the value: `true`.

   ```
   REINSTALL=true
   ```

   Based on your requirement, edit any additional parameters if the default values are not in line with your best practices. See Parameters for Installing Data Collector for more details.
3. Run the `AgentInstall` agent installation script to install a data collector.
   - If you are installing a data collector on a UNIX-based host:

     ```
     ./AgentInstall.sh
     ```
   - If you are installing a data collector on a Windows host, right-click and select **Run as administrator** to open an Administrator command prompt and run the following:

     ```
     AgentInstall.bat
     ```

Your data collector installation using reinstall option is now complete. The data collector you just installed will attach to the old data collector you have in OMC and inherit its historical data. Next step is to Verify the Data Collector Installation.

Upgrade to Enterprise Manager 13.X after Installing a Data Collector

This section discusses upgrading to Enterprise Manager 13.X after installing a data collector.

Upgrade to Enterprise Manager 13.X after Installing a Data Collector

If you have installed a data collector on Oracle Enterprise Manager 12c, and you are planning to upgrade to Oracle Enterprise Manager 13.x, follow the steps listed in the Troubleshoot Oracle Management Cloud Agents.

If you have deployed the data collector on Oracle Enterprise Manager 13.x, then these steps can be ignored.

Install a Data Collector on Oracle Real Application Clusters

This section discusses installing a data collector on Oracle Real Application Clusters.

Install a Data Collector on Oracle Real Application Clusters

If you are installing a data collector on Oracle Real Application Clusters (RAC), then deploy the data collector on any one node, pass the scan host name instead of individual RAC host names and `OMR_SERVICE_NAME` in the response file, and then run the `AgentInstall` script. Using the scan host name, you can retrieve all the associated nodes for that scan host and also check the SSH connectivity to all the nodes.

Modify the Data Collector Connect String or SSH Port After Deployment

This section discusses modifying the data collector connect string or SSH port after deployment.

Modify the Data Collector Connect String or SSH Port After Deployment

If you want to change the connect string or any other details in the connect string for a data collector that was already deployed to the same Oracle Management Repository (OMR), then follow these steps:

1. Stop the data collector.

   `<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli stop agent`

2. Create a file with name `FILENAME`:

   `<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli config_datacollector agent FILENAME`

   This file must contain the following details:

   ```
   UserName: username of the datacollector user.
   UserNamePriv: username of a privileged user.
   UserRolePriv: userrole of a privileged user. Default SYSDBA.
   HarvestHostUserName: username of an OS user for fetching datacollector files.
   StageDir: absolute directory path for staging datacollector files on the OMR host.
   ConnectDescriptor: Connect descriptor for the OMR.
   Host: host of the OMR. (Not required if ConnectDescriptor is specified)
   Port: port of the OMR. (Not required if ConnectDescriptor is specified)
   Service: service name of the OMR. (Not required if ConnectDescriptor is specified)
   Sid: SID of the OMR. (Not required if ConnectDescriptor or Service is specified)
   ```

   Sample File

   ```
   UserName     : omc_collector
   UserNamePriv : sys
   UserRolePriv : SYSDBA
   HarvestHostUserName : oracle
   StageDir : /u01/OMCStageDir
   Host : host.example.com
   Port : 1521
   Service : EMREP.example.com
   ```

3. Start the data collector.

   `<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli start agent`

To modify the SSH port after the data collector has been installed, follow these steps:

1. Stop the data collector.

   `<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli stop agent`

2. Create a file with name `FILENAME`:

   `<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli config_datacollector agent FILENAME`

   This file must contain the following details:

   ```
   UserName: username of the datacollector user.
   StageDir: absolute directory path for staging datacollector files on the OMR host.
   ```

```
HarvestHostUserName: username of an OS user for fetching datacollector files.
Sid: SID of the OMR. (Not required if ConnectDescriptor or Service is
specified)
UserNamePriv: username of a privileged user.
Host: host of the OMR. (Not required if ConnectDescriptor is specified)
OMR_HOST_SSH_PORT: SSH Port Number (For any port change)
Port: port of the OMR. (Not required if ConnectDescriptor is specified)
```

Sample File

```
UserName     : omc_collector
StageDir : /u01/OMCStageDir
HarvestHostUserName : oracle
UserNamePriv : sys
SID: host
Host : host.example.com
OMR_HOST_SSH_PORT: 42
Port : 1111
```

3. Start the data collector.

   `<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli start agent`

> **Note:**
>
> You can't use these steps to redirect the data collector to a different Oracle Management Repository.

Specify a Custom SSH Port while Deploying the Data Collector

This section discusses specifying a custom SSH port while deploying the data collector.

Specify a Custom SSH Port while Deploying the Data Collector

If you want to use a custom SSH port while installing the data collector on a different host other than the Oracle Management Repository (OMR) host, or on the same host as the OMR, you must specify the following additional parameter in the response file during installation:

```
ADDITIONAL_PARAMETERS="OMR_HOST_SSH_PORT=<SSH PORT Number>"
```

You can also specify the parameter value in the command line as the following:

```
./AgentInstall.sh|bat ADDITIONAL_PARAMETERS="OMR_HOST_SSH_PORT=<SSH PORT
Number>"
```

Verify the Data Collector Installation

After installing the data collector, you must verify the installation.

To verify data collector installation, perform the following:

1. Click the **OMC Navigation** menu, and then click **Agents** under **Administration**.

   This displays the Oracle Management Cloud Agents page.

2. Click **Data Collectors** on the left navigation pane.

3. Check **Agent Display Name** column from the agent list to see if the host name of your deployed data collector exists on the list of available data collectors.

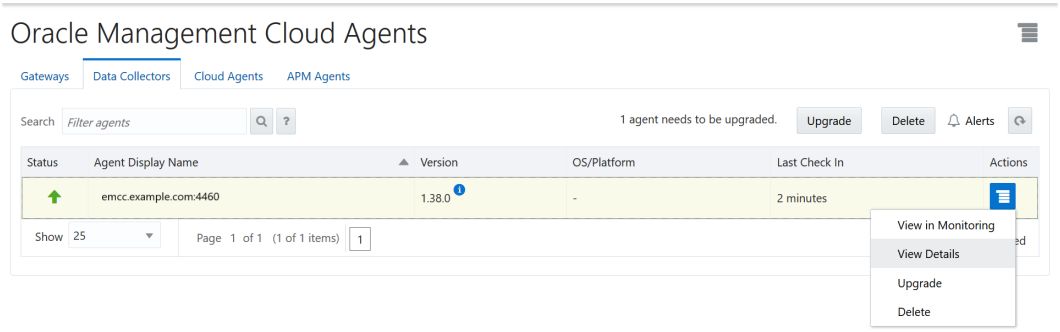
   You can right click on the agent list to select the specific columns that you want to see on the list.

4. Select your deployed data collector.

   The **Last Check In** column displays how much time has passed since the agent was last checked in/deployed.

   The **Actions** column displays a menu with different actions available.

5. Click Actions menu and select **View Details**.



   The **View Details** action opens up a window with agent details like host name, agent version, OS platform and logs location. You can also see the registration key value that you used when you deployed the agent. At the bottom of the window, you can see a History section with **Operation Type** and **Status** information. **Operation Type** will list the operations performed on the specific agent (for example: install, upgrade, deinstall or delete) along with a link to the Lifecycle Tasks details page to see details of the specific operation. See Agent Lifecycle Tasks for more details.

You can also use the following `omcli` command from the *<AGENT_BASE_DIRECTORY>*`/agent_inst/bin` directory to verify whether the data collector was successfully deployed:

```
./omcli status agent
```

6

Agent Administration Tasks

This section covers some agents administration tasks.

Topics

Configure Automatic Restart of a Cloud Agent

Cloud agents are deployed to collect log and metric data from entities. For seamless collection of data, the cloud agent must not stop or fail. To keep the cloud agent running, you must configure it to automatically restart the agent service after a hardware or software failure or whenever your cloud agent host machine restarts.

Ensure that only the *root* user and *agent installation* user have write permission on the *Agent_Base_Directory*. The *root* user and *agent installation* user must be the owner of the directory and it's parent directory.

The following sections contain examples of how you can configure an agent as a service in different operating systems.

> **Note:**
>
> You may need to edit the examples based on your own directory structure.

Linux

1. Login as the *root* user.
2. Create a shell script under the `/etc/init.d` directory using any standard text editor with the following:
   - `#!/bin/sh`
   - `su – <Agent_Install_User> –c <Agent_Base_Directory>/agent_inst/bin/omcli start agent`

   For example, if the agent is installed under the `/agent/base/cloudagent` directory and agent installation owner is *emga*, then the content of the shell script should be as follows:
   `#!/bin/sh`

```
su - “emga” -c “/agent/base/cloudagent/agent_inst/bin/omcli start
agent”
```

3. Save the script file.
4. Change the permission of the file to 755. Ensure that the owner of the script file and all the other files in the /etc/init.d directory is *root*.
5. Create symbolic links under /etc/rc.d/rc2.d, /etc/rc.d/rc3.d, /etc/rc.d/rc5.d, and /etc/rc.d/rc6.d directories. Prefix the symbolic link with *S* and the priority level.
   - To create the above symbolic link, run the following command:

     ```
     ln -s /etc/init.d/S81startomcagent.sh /etc/rc2.d/
     S81startomcagent.sh
     ```

   For example, if the file *startomcagent* is created under /etc/init.d with priority level 81, then the symbolic link will be as follows:

   ```
   lrwxrwxrwx 1 root root 30 Apr  2 04:39 /etc/rc.d/rc2.d/
   S81startomcagent.sh -> /etc/init.d/startomcagent.sh
   ```

6. Restart the host machine.

Solaris

1. Login as the *root* user.
2. Create a shell script under the /etc/init.d directory using any standard text editor and paste the following into the file.
   - `#!/bin/sh`
   - `su – <Agent_Install_User> –c <Agent_Base_Directory>/agent_inst/bin/omcli start agent`

   For example, if the agent is installed under the /agent/base/cloudagent directory and agent installation owner is *emga*, then the content of the shell script should be as follows:

   ```
   #!/bin/sh
   ```

   ```
   su - “emga” -c “/agent/base/cloudagent/agent_inst/bin/omcli start
   agent”
   ```

3. Save the script file.
4. Change the permission of the file to 755. Ensure that the owner of the script file and all the other files in the /etc/init.d directory is *root*.
5. Create symbolic links under /etc/rc2.dand /etc/rc3.d directories. Prefix the symbolic link with *S* and the priority level.
   - To create the above symbolic link, execute the following command:

     ```
     ln -s /etc/init.d/S81startomcagent.sh /etc/rc.d/rc2.d/
     S81startomcagent.sh
     ```

For example, if the file *startomcagent* is created under `/etc/init.d` with priority level `81`, then the symbolic link will be as follows:

```
lrwxrwxrwx 1 root root 30 Apr 2 04:39 /etc/rc2.d/S81startomcagent -> /etc/
init.d/startomcagent.sh
```

6. Restart the host machine.

AIX

1. Login as the *root* user.
2. Create a shell script under the `/etc/rc.d/init.d` directory using any standard text editor and paste the following into the file.
   - `#!/bin/sh`
   - `su – <Agent_Install_User> –c <Agent_Base_Directory>/agent_inst/bin/omcli start agent`

   For example, if the agent is installed under the `/agent/base/cloudagent` directory and agent installation owner is *emga*, then the content of the shell script should be as follows:
   `#!/bin/sh`

   ```
   su - “emga” -c “/agent/base/cloudagent/agent_inst/bin/omcli start agent”
   ```
3. Save the script file.
4. Change the permission of the file to `755`. Ensure that the owner of the script file and all the other files in the `/etc/rc.d/init.d` directory is *root*.
5. Create symbolic links under `/etc/rc.d/rc2.d`, `/etc/rc.d/rc3.d`, and `/etc/rc.d/rc5.d` directories. Prefix the symbolic link with *S* and the priority level.
   - To create the above symbolic link, execute the following command:

     ```
     ln -s /etc/rc.d/init.d/S81startomcagent.sh /etc/rc.d/rc2.d/
     S81startomcagent.sh
     ```

   For example, if the file *startomcagent* is created under `/etc/rc.d/init.d` with priority level `81`, then the symbolic link will be as follows:

   ```
   lrwxrwxrwx 1 root root 30 Apr 2 04:39 /etc/rc.d/rc2.d/S81startomcagent -
   > /etc/rc.d/init.d/startomcagent.sh
   ```
6. Restart the host machine.

Set Up Alert Rules for Agents

You can monitor the availability status of your agents by setting up alert rules that send email notifications when an agent is down. You can also set up alert rules for agents using the IM alert rules.

If Oracle Management Cloud does not receive data for the agent for at least 30 minutes, then the agent is considered as unavailable. The status of the agent and the host is set to **Not Heard From** and an alert is automatically generated.

An alert is triggered for any of the following conditions:

- The cloud agent, gateway, or data collector is down.
- The cloud agent was installed with a gateway. If the gateway is down, an alert is generated for both the cloud agent and the gateway.
- The data collector was installed with a gateway. If the gateway is down, an alert is generated for both the data collector and the gateway.

You can define alert rules to specify email notifications for agent availability.

To define an alert rule, follow these steps:

1. Click **Alerts** in the common navigation menu. You will see a list of alerts that have been triggered for the various entities.
2. Click the link in the Message column to view the alert details.
3. Click the **Alert Rules** icon on the top right corner.
4. On the Alert Rules page, select **Agent** from the **Service** drop-down list, then click **Create Alert Rule**.

> **Note:**
>
> If you don't select **Agent**, then **Create Alert Rules** will remain disabled.

5. On the **Create Alert Rule** dialog box, enter the following details:
   - Name and description for the alert rule.
   - Select the entity type for the which the rule is applicable. You can select either of the following:
     - Entity types: Select the agent type from the drop down menu. You can select Gateways, Cloud Agents, Data Collectors, or all agent types. The rule that you define is applicable to all agents that are selected here.
     - Individual entities: You can select one or more agents from the list and click **Select**. The rule you define will be applicable only to the agents that are selected here.
   - Click **Add Condition** to add the Availability condition.
   - Specify one or more email addresses separated by commas. Alert notifications will be sent to the email addresses specified here.
6. Click **Save** to save the alert rule. When an agent specified in this rule is down, an email alert is triggered.

   You can disable notifications using the **Disable Notifications** link on the Alert Rules page. Alerts will continue to be generated but all notifications for all alerts will be disabled.

> **Note:**
>
> When an agent that is associated with an alert rule becomes operational, the alerts triggered for that agent are cleared.

Adjust Data Buffering and Disk Sizing

You can increase the local storage limit of cloud agents or gateways, depending on your storage capacity and needs.

If you experience network connectivity issues, the data collected by agents is stored locally until the connection to Oracle Management Cloud service is re-established.

Agents have the following default local storage limits:

- 100 MB of local data for each cloud agent
- 100 GB of local data for a gateway

To change the storage limit for any agent, you set a new value for the `senderManagerMaxDiskUsedTotal` parameter by running the following:

- `<AGENT_BASE_DIR>/agent_inst/bin/omcli setproperty agent -allow_new -name senderManagerMaxDiskUsedTotal -value <new value>`

  Note the `<new value>` is in MB.

For example:

- To increase the local storage for a cloud agent to 200 MB, on the host where the agent is installed, run:

  ```
  <AGENT_BASE_DIR>/agent_inst/bin/omcli setproperty agent -allow_new -name
  senderManagerMaxDiskUsedTotal -value 200
  ```

- To increase the local storage for a gateway to 200 GB, on the host where the gateway is installed, run:

  ```
  <AGENT_BASE_DIR>/agent_inst/bin/omcli setproperty agent -allow_new -name
  senderManagerMaxDiskUsedTotal -value 200000
  ```

The changes are in effect immediately. The cloud agent does not need to be restarted when changing this value.

Manage Registration Keys

Managing your registration keys involves creating, downloading, and revoking the keys.

Topics:

About Registration Keys

A registration key is issued against your identity domain, and it's used when you deploy cloud agents.

You can create a new registration key and use that key for installing a new agent by specifying the `AGENT_REGISTRATION_KEY=<NewKeyValue>` parameter in the response file. The

registration key is only used during installation. Once an agent is installed with the registration key, that key can be removed from Oracle Management Cloud.

A registration key can exist in three states:

- `VALID`: The registration key is valid, and it can be used to run the installation script.
- `EXPIRED`: The registration key's usage count is greater or equal to the maximum usage specified at the time of creating the key.
- `DISABLED`: The registration key is explicitly set to be in the disabled state by calling a Cloud Service REST API.

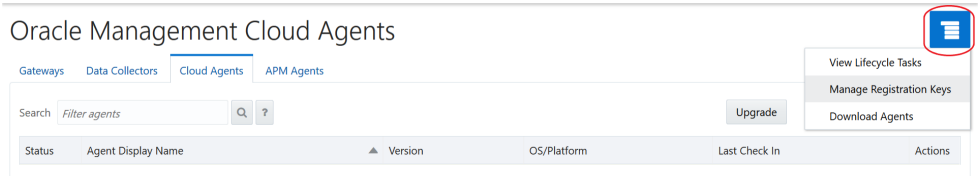
Create a Registration Key

To create a registration key:

1. On the Oracle Management Cloud home page, click the global navigation menu on the top left, then go to **Administration** and click **Agents**.

   The Oracle Management Cloud Agents page is displayed.

2. On the Oracle Management Cloud Agents page, click the Action Menu on the top right corner of the page and select **Manage Registration Keys**.



   The Registration Keys page displays a list of all registration keys.

3. Enter the required details in the Registration Keys page:
   a. In the **Name** field, specify a name to identify the registration key.
   b. In the **Registration Limit** field, enter a number that indicates the maximum number of agents, data collectors, and gateways that can be associated with the registration key.
   c. Click **Create New Key**.

   A new registration key is created. You can now pass the value of this key to the `AgentInstall` script at the time of installation.

Download a Registration Key

You can download a registration key from the Oracle Management Cloud Agents page.

1. On the Oracle Management Cloud Agents page, click the Action Menu on the top right corner of the page and select **Manage Registration Keys**.

   The Registration Keys page displays a list of all registration keys.

2. From the list of registration keys, select the key that you want to download.
3. On the right side of the page, click the actions menu and select **Download**.

   A text file `registrationKey.txt` that contains the value of the registration key is downloaded to your local drive.

4. To view the key value, open the `registrationKey.txt` file.

Revoke a Registration Key

You can revoke a registration key when you feel that any unauthorized user has obtained the value of a key.

To revoke a key:

1. On the Oracle Management Cloud Agents page, click the Action Menu  on the top right corner of the page and select **Manage Registration Keys**.

   The Registration Keys page displays a list of all registration keys.
2. From the list of registration keys, click the registration key that you want to revoke.
3. On the right side of the page, click the actions menu and select **Revoke**.

Manage Agent Credentials

This section discusses how to manage agent credentials using JSON files.

After the agent installation, you need to add entities for monitoring and analysis. See Typical Workflow for Adding Entities in *Working with Oracle Management Cloud* for details.

Each entity has credentials and this section covers how to manage agent credentials using JSON files and the command line utility `omcli` which is part of the agent files. To find the `omcli` directory location, do the following:

1. Connect to the host where the Oracle Management Cloud agent is installed .
2. Navigate to the agent installation directory. For example: `<AGENT_BASE_DIR>/agent_inst/bin`
3. Confirm that `omcli` utility resides in that directory.

   ```
   $ ls –la omcli
   ```

Topics

- Add a Credential Store
- Add Credentials
- List Credentials
- Enable and Disable Credentials
- Remove Credentials

For more details about credentials commands, see omcli Command Options.

Add a Credential Store

Add an agent credential store:

1. Login as the user who installed the agent.

   ```
   $ su oracle
   ```

2. Navigate to the `omcli` directory location.

   ```
   $ cd <AGENT_BASE_DIR>/agent_inst/bin
   ```

3. Stop the agent.

   ```
   $ omcli stop agent
   ```

4. Add a wallet-based credential store to an agent by using:

   ```
   $ omcli add_credential_store agent [ wallet-file ] [ -no_password ]
   ```

   The command configures the agent to use a wallet-based credential store.

   Where:

   - `wallet–file`: the filename location of the wallet-based credential store. The wallet can be a pre-existing file or a new file.

     If `wallet-file` is not specified, the default wallet file: `cwallet.sso` will be created under `<AGENT_BASE_DIR>/agent_inst/sysman/config/creds` directory.

   - `-no_password`: no password will be used in the wallet and an SSO wallet (protected only by file permissions) will be created/used.

     If `-no_password` is not specified, the user will be prompted for a password to use in the wallet.

   All sensitive credential data will reside in the wallet.

   For example, you can run the following:

   ```
   $ omcli add_credential_store agent -no_password
   Oracle Management Cloud Agent
   Copyright (c) 1996, 2018 Oracle Corporation.  All rights reserved.
   Wallet-based credential store was added successfully.
   ```

   A filename: `cwallet.sso` is created under `<AGENT_BASE_DIR>/agent_inst/sysman/config/creds` directory.

5. Restart the agent.

   ```
   $ omcli start agent
   ```

Add Credentials

Add credentials to an agent credential store:

1. Login as the user who installed the agent.

   ```
   $ su oracle
   ```

2. Navigate to the `omcli` directory location.

   ```
   $ cd <AGENT_BASE_DIR>/agent_inst/bin
   ```

3. Start the agent if it's not already running.

   ```
   $ omcli start agent
   ```

4. Create and save a JSON file with all the credential information.

   For example, you can save it with filename: **`cred.json`**.

   There are different types of credentials:

   - **HostSSHCreds:** This a host credential using SSH Keys.

     ```
     [
       {
         "entity": "omc_host_linux.<HOST_NAME>",
         "name": "omc_oracle_<HOST_NAME>-HostSSHCreds",
         "type": "HostSSHCreds",
         "globalName": "emcosComplianceCredSSHKey",
         "description": "SSH Credential for the agent omcagentuser",
         "properties": [
          { "name":"USERNAME", "value":"CLEAR[omcagentuser]" },
          { "name":"SSH_PVT_KEY", "value":"FILE[<YourUsername>/.ssh/
     id_rsa]" },
          { "name":"SSH_PUB_KEY", "value":"FILE[<YourUsername>/.ssh/
     id_rsa.pub]" }
        ]
       }
     ]
     ```

     Where:

     – **“entity”** is the entity field. If you are working with a Linux agent, use the value: “`omc_host_linux.<HOST_NAME>`”. If you are working with an AIX agent, use the value: “`omc_host_aix.<HOST_NAME>`”. For example: “`omc_host_linux.host1.example.com`” for a Linux agent.

     – **<HOST_NAME>** is the fully qualified name of your host. For example: `host1.example.com`

     – **“name”** is any name for your credential. We recommend that you name this credential your host name followed by `HostSSHCreds`. For example: `"host1.example.com-HostSSHCreds"`.

     – **"type"** is the credential type. “`HostSSHCreds`” is used for SSH Key credentials type.

     – **"globalName"** is the global name for the credential. It is the credential's name within a "global" namespace (where global actually is only global to this Oracle Management Cloud agent, not global throughout Oracle Management Cloud).

     – **"description"** is the credential description.

     – **“SSH_PVT_KEY”** is the OS user's private key, for public/private key-based authentication schemes.

  - **“SSH_PUB_KEY”** is the OS user's public key, for public/private key-based authentication schemes.
  - **<YourUsername>** is the OS user name used as your SSH credential.
  - All other field values must remain as listed. They are reserved values.

- **HostSSHPwdCreds:** This is a host credential using SSH Password.

```
[
  {
    "entity":"omc_host_linux.<HOST_NAME>",
    "name":"<HOST_NAME>-HostSSHPwdCreds",
    "type":"HostSSHPwdCreds",
    "globalName":"emcosComplianceCred",
    "description":"SSH Credential for the host entity",
    "properties":[
      { "name":"USERNAME", "value":"CLEAR[<YourUsername>]"},
      { "name":"PASSWORD", "value":"CLEAR[<YourPassword>]"}
    ]
  }
]
```

  Where:

  - **“entity”** is the entity field. If you are working with a Linux agent, use the value: “`omc_host_linux.<HOST_NAME>`”. If you are working with an AIX agent, use the value: “`omc_host_aix.<HOST_NAME>`”. For example: “`omc_host_linux.host1.example.com`” for a Linux agent.
  - **<HOST_NAME>** is the fully qualified name of your host. For example: `host1.example.com`
  - **“name”** is any name for your credential. We recommend that you name this credential your host name followed by `HostSSHPwdCreds`. For example: `"host1.example.com-HostSSHPwdCreds"`.
  - **"type"** is the credential type. “`HostSSHPwdCreds`” is used for SSH password credentials type.
  - **"globalName"** is the global name for the credential. It is the credential's name within a "global" namespace (where global actually is only global to this Oracle Management Cloud agent, not global throughout Oracle Management Cloud).
  - **"description"** is the credential description.
  - **<YourUsername>** is the OS user name used as your SSH credential.
  - **<YourPassword>** is the OS user’s password for your SSH credential.
  - All other field values must remain as listed. They are reserved values.

- **Other types:** There are other credentials types that are used by different OMC components.

  For example, the credential type: **DBCredsNormal** is a database credential used by Log Analytics for Oracle database instance credentials.

```
[
  {
```

```
    "entity":"omc_oracle_db_instance.<Entity Name>",
    "name":"LCAgentDBCreds",
    "type":"DBCredsNormal",
    "usage":"LOGANALYTICS",
    "globalName":"AgentUserCredential",
    "description":"DB Credentials",
    "properties":[
      { "name":"USERNAME", "value":"CLEAR[<DBUsername>]"},
      { "name":"PASSWORD", "value":"CLEAR[<DBPassword>]"}
      { "name":"ROLE", "value":"CLEAR[<DBRole>]"}
    ]
  }
]
```

Where:

- **“entity”** is the entity field. If you are working with an Oracle database instance, use the value: “`omc_oracle_db_instance.<ENTITY NAME>`”. For example: “`omc_oracle_db_instance.example_instance/orcl`” if your database name is: `example_instance`.
- **“name”** is any name for your credential. For example: `"LCAgentDBCreds"` is used for the name of the database credentials used by the cloud agent to collect the log data from the entity.
- **"type"** is the credential type. “`DBCredsNormal`” is used for Oracle database credentials type.
- **"globalName"** is the global name for the credential. It is the credential's name within a "global" namespace (where global actually is only global to this Oracle Management Cloud agent, not global throughout Oracle Management Cloud).
- **"usage"** is the credentials usage. For example: `"LOGANALYTICS"` since this credential is used for Log Analytics.
- **"description"** is the credential description.
- **<DBUsername>** is the database user name used for the database credential. For example, SYS database user.
- **<DBPassword>** is the database user’s password for your database credential. For example, the password of SYS database user.
- **<DBRole>** is the database role for your database credential. For example, the SYSDBA database role for the database user. The `ROLE` property is optional.
- All other field values must remain as listed. They are reserved values.

5. Add credentials using a JSON file.

```
$ omcli add_credentials agent -credential_file CREDENTIALS_FILE [ -
encryption_method_gpg ] [ -allow_entityless ]
```

The command adds credentials based on the description in the JSON file.

Where:

- `-credential_file`: a credential file will be used.

- `CREDENTIALS_FILE`: the filename of the credential file that will be used. The credentials are listed in the `CREDENTIALS_FILE` file. For example, the name of the JSON file that you just created in step 4: **cred.json**.
- `-encryption_method_gpg`: the credentials file has been encrypted using symmetric GNU Privacy Guard (gpg), and a passphrase may be needed.
- `-allow_entityless`: the agent will not complain about credentials that are missing the entity field. However, a global name should be supplied if an entity is not.

For example, you can run the following:

```
$ omcli add_credentials agent -credential_file cred.json
```

List Credentials

List credentials:

1. Login as the user who installed the agent.

   ```
   $ su oracle
   ```

2. Navigate to the `omcli` directory location.

   ```
   $ cd <AGENT_BASE_DIR>/agent_inst/bin
   ```

3. List credentials by using:

   ```
   $ omcli list_credentials agent [ TARGETNAME:TARGETTYPE | -global ]
   [ -usage USAGE ]
   ```

   The command lists the non-sensitive credential attributes for specified credentials. If no optional parameters are specified, it lists all credentials.

   Where:

   - `TARGETNAME:TARGETTYPE`: lists the specified credential definitions relative to the entity named `TARGETNAME:TARGETTYPE`.

     `TARGETNAME` is the name part of the target id of the credential definition.

     `TARGETTYPE` is the type part of the target id of the credential definition.
   - `-global`: lists credential definitions with global names.
   - `-usage` : it only lists credentials that may be used for that usage. When it's supplied, `USAGE` can be any of the following values: ORCHESTRATION, MONITORING, or INTERNAL.

   For example, you can run the following:

   ```
   $ omcli list_credentials agent

   Oracle Management Cloud Agent Copyright (c) 1996, 2018 Oracle
   Corporation. All rights reserved.
   Credential Name Type Entity Global Name Usage host1.example.com-
   ```

```
HostSSHPwdCreds
HostSSHPwdCreds (host1.example.com) "emcosComplianceCred"
```

Enable and Disable Credentials

Enable credentials:

1. Login as the user who installed the agent.

   ```
   $ su oracle
   ```

2. Navigate to the `omcli` directory location.

   ```
   $ cd <AGENT_BASE_DIR>/agent_inst/bin
   ```

3. Start the agent if it's not already running.

   ```
   $ omcli start agent
   ```

4. Enable a credential by using:

   ```
   $ omcli enable_credential agent CREDENTIAL_NAME [ TARGETNAME:TARGETTYPE |
   -global ]
   ```

   The command enables the specified credential.

   Where:

   - `CREDENTIAL_NAME`: is the credential name.
   - `TARGETNAME:TARGETTYPE`: enables only the credentials with the local name `CREDENTIAL_NAME` within the entity's scope.

     `TARGETNAME` is the name part of the target id of the credential definition.

     `TARGETTYPE` is the type part of the target id of the credential definition.
   - –`global`: enables the credentials with the global name `CREDENTIAL_NAME`.

Disable credentials:

1. Login as the user who installed the agent.

   ```
   $ su oracle
   ```

2. Navigate to the `omcli` directory location.

   ```
   $ cd <AGENT_BASE_DIR>/agent_inst/bin
   ```

3. Start the agent if it's not already running.

   ```
   $ omcli start agent
   ```

4. Disable a credential by using:

```
$ omcli disable_credential agent CREDENTIAL_NAME
[ TARGETNAME:TARGETTYPE | -global ]
```

The command disables the specified credential.

Where:

- `CREDENTIAL_NAME`: is the credential name.
- `TARGETNAME:TARGETTYPE`: disables only the credentials with the local name `CREDENTIAL_NAME` within the entity's scope.

  `TARGETNAME` is the name part of the target id of the credential definition.

  `TARGETTYPE` is the type part of the target id of the credential definition.
- `–global`: disables only the credentials with the global name `CREDENTIAL_NAME`.

Remove Credentials

Remove credentials:

1. Login as the user who installed the agent.

```
$ su oracle
```

2. Navigate to the `omcli` directory location.

```
$ cd <AGENT_BASE_DIR>/agent_inst/bin
```

3. Start the agent if it's not already running.

```
$ omcli start agent
```

4. Remove a credential by using:

```
$ omcli remove_credential agent CREDENTIAL_NAME
[ TARGETNAME:TARGETTYPE | -global ]
```

The command removes a credential from the agent with name `CREDENTIAL_NAME`.

Where:

- `CREDENTIAL_NAME`: is the credential name.
- `TARGETNAME:TARGETTYPE`: is the entity name. You want to remove a credential from the agent with the specific entity name: `TARGETNAME:TARGETTYPE`.

  `TARGETNAME` is the name part of the target id of the credential definition.

  `TARGETTYPE` is the type part of the target id of the credential definition.
- `–global`: removes a credential from the agent with global name `CREDENTIAL_NAME`.

Change Proxy Server Settings After Installing Cloud Agents

Your organization may decide to change the proxy server settings for security reasons. If your cloud agent connects to Oracle Management Cloud over the proxy server, then you must modify the proxy server settings of the cloud agent.

To modify the proxy server settings after the agent was deployed:

1. View the current proxy server details being used by the cloud agent.

```
<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli getproperty agent -name OMC_PROXYHOST
Oracle Management Cloud Agent
Copyright (c) 1996, 2016 Oracle Corporation.  All rights reserved.
OMC_PROXYHOST=www-xyz.abc.oracle.com

<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli getproperty agent -name OMC_PROXYPORT
Oracle Management Cloud Agent
Copyright (c) 1996, 2016 Oracle Corporation.  All rights reserved.
OMC_PROXYPORT=20
```

2. Clear the current proxy server settings.

```
<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli clear_property agent -name
OMC_PROXYHOST
Oracle Management Cloud Agent
Copyright (c) 1996, 2016 Oracle Corporation.  All rights reserved.
EMD clear_property succeeded

<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli getproperty agent -name OMC_PROXYHOST
Oracle Management Cloud Agent Copyright (c) 1996, 2016 Oracle Corporation.  All
rights reserved.
OMC_PROXYHOST=null

<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli clear_property agent -name
OMC_PROXYPORT
Oracle Management Cloud Agent
Copyright (c) 1996, 2016 Oracle Corporation.  All rights reserved.
EMD clear_property succeeded

<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli getproperty agent -name OMC_PROXYPORT
Oracle Management Cloud Agent
Copyright (c) 1996, 2016 Oracle Corporation.  All rights reserved.
OMC_PROXYPORT=null
```

3. Set the new or updated proxy.

```
<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli setproperty agent -name OMC_PROXYHOST -
value "www-abc.xyz.example.com"
Oracle Management Cloud Agent
Copyright (c) 1996, 2016 Oracle Corporation.  All rights reserved.
EMD setproperty succeeded

<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli setproperty agent -name OMC_PROXYPORT -
value 80
Oracle Management Cloud Agent
Copyright (c) 1996, 2016 Oracle Corporation.  All rights reserved.
EMD setproperty succeeded

<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli getproperty agent -name OMC_PROXYHOST
Oracle Management Cloud Agent
```

```
Copyright (c) 1996, 2016 Oracle Corporation.  All rights reserved.
OMC_PROXYHOST=www-abc.xyz.example.com

<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli getproperty agent -name
OMC_PROXYPORT
Oracle Management Cloud Agent
Copyright (c) 1996, 2016 Oracle Corporation.  All rights reserved.
OMC_PROXYPORT=80
```

4. Stop and then restart the cloud agent.

```
<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli stop agent
Oracle Management Cloud Agent
Copyright (c) 1996, 2016 Oracle Corporation.  All rights reserved.
Stopping agent ... stopped.

<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli start agent
Oracle Management Cloud Agent
Copyright (c) 1996, 2016 Oracle Corporation.  All rights reserved.
Starting agent ................... started.
```

7

Upgrade Oracle Management Cloud Agents

This section describes how to upgrade gateways, data collectors and cloud agents.

About Upgrading Oracle Management Cloud Agents

Upgrading Oracle Management Cloud agents is a seamless process without any data loss. The data feed generated during the upgrade process is stored in the agent state directory. After the agent comes back online, the data files get uploaded to Oracle Management Cloud.

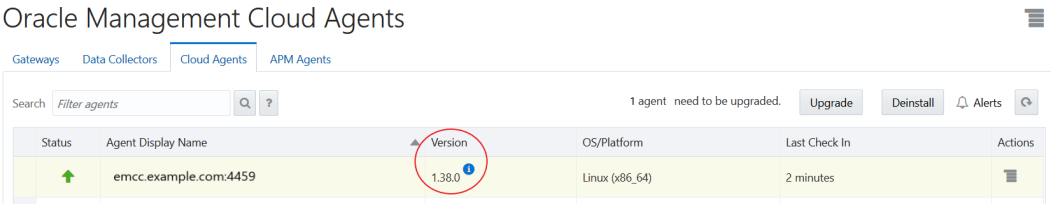
It is recommended that you check the Oracle Management Cloud Agents page and verify that you have deployed the latest version of the agent software. To check if there is a newer version available for a specific agent, perform the following steps:

1. On the Oracle Management Cloud Agents page, you will see a list of gateways, data collectors and cloud agents that you deployed under their corresponding tabs. Click the specific agent tab.

   The Oracle Management Cloud agent tab is displayed

2. Click the specific agent that you deployed and check **Version**.

   If you see a blue information icon next to the current version listed then an upgrade is available to that specific agent.



3. You can decide to upgrade the agent now or later.

When you upgrade the agents, ensure that you upgrade the gateway (if applicable) before you upgrade the associated data collector (if applicable) or cloud agents that are communicating through it.

> **Note:**
>
> Wait for the gateway upgrade process to be completed before proceeding with upgrade of the associated agents.

Before Upgrading Data Collectors

The default roles and privileges given to a data collector user during the installation may be altered or revoked due to in-house security policies. If this is the case, then run the following script at regular intervals to confirm that all necessary and sufficient roles and privileges are still intact:

1. You can click this link to download the script, or go to the data collector agent base directory: `<AGENT_BASE_DIRECTORY>/sysman/admin/scripts/emaas/harvester/script/check_privs.sql` and download the script. The script must be downloaded to a host from which you can connect to the Oracle Management Repository database.
2. Connect to the Oracle Management Repository database as the Data Collector installation user as follows:

   `./sqlplus DATA_COLLECTOR_USERNAME@<OMR_CONNECT_STRING>`
3. Run the script.

Log files

You can find the agent upgrade logs under the following location:

`<AGENT_BASE_DIRECTORY>/agent_inst/sysman/log/upgrade`

Topics:

Upgrade Agents Using User Interface

This section describes how to upgrade gateways, data collectors and cloud agents using user interface.

Topics:

Upgrade Multiple Oracle Management Cloud Agents

You can select multiple agents and upgrade them together.

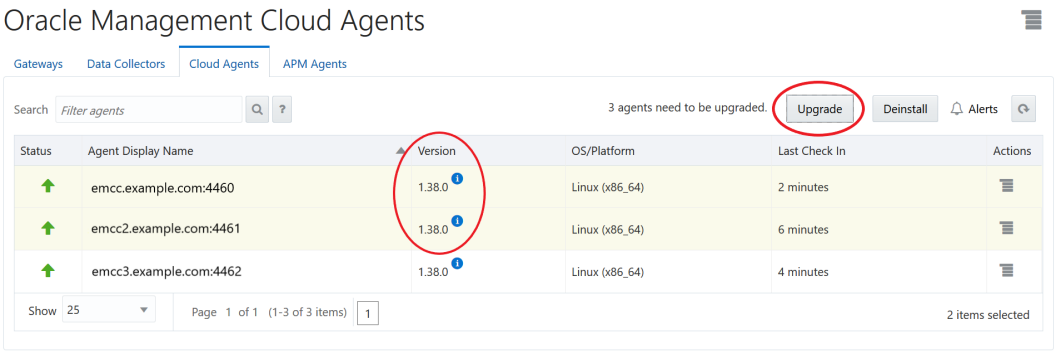
To upgrade multiple Oracle Management Cloud agents using user interface, perform the following steps:

1. On the Oracle Management Cloud page, click the **OMC Navigation** icon on the top-left corner to view the Management Cloud navigation pane, if it isn't already displayed.
2. Select **Agents** under **Administration**.
3. On the Oracle Management Cloud Agents page, click the specific agent tab that needs to be upgraded: **Gateways**, **Data Collectors**, or **Cloud Agents**.

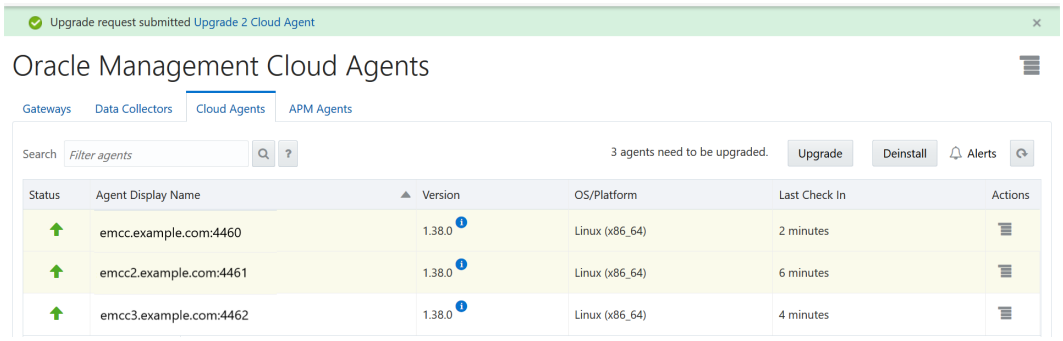
   The Oracle Management Cloud agent tab is displayed.
4. Identify the multiple agents and check if the blue information icon  is displayed next to the agent version to confirm that the agents need to be upgraded.

   You can also use the **Search** feature to find the specific agents.

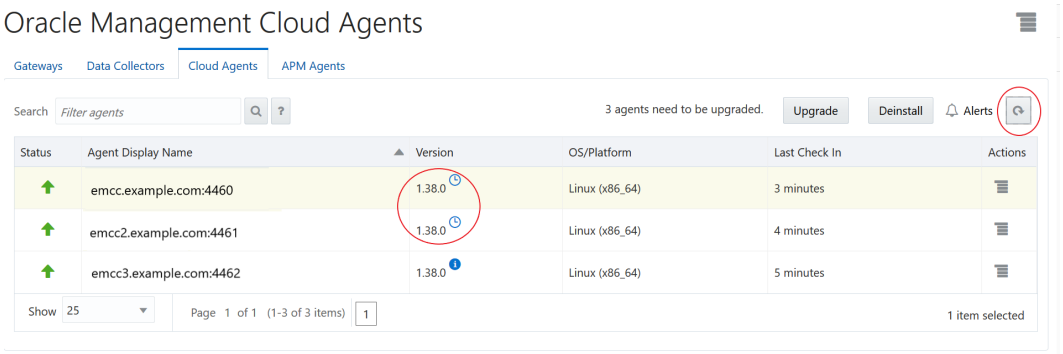
5. Select the multiple agents: Click the first agent, press and hold the CTRL key and then start clicking the additional agents that you want to upgrade.
6. Click **Upgrade**.



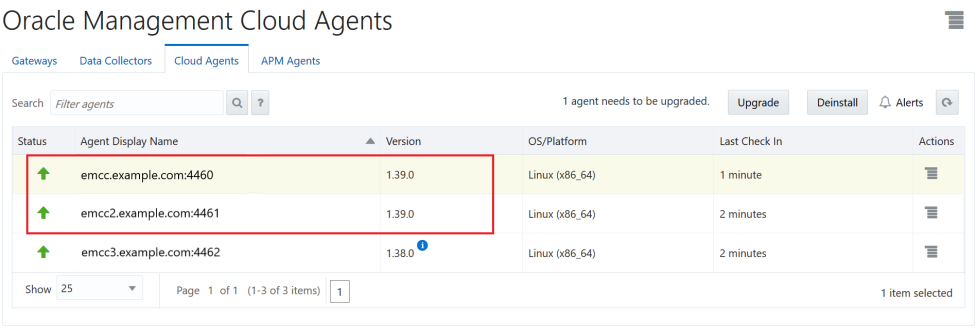
7. A window pops up. It verifies the request and confirms if the agents are eligible to be upgraded. Click **Yes** to proceed.
8. You will see a green message at the top of the page: **Upgrade request submitted** along with a link to track the upgrade progress. If you click on the link then the Lifecycle Tasks page will open and you will be able to monitor details of the upgrade task. See Monitor Upgrade Agents Task.



9. Click **Refresh** located at the top right to refresh the page. You will see a blue clock icon next to the version indicating that upgrade is in progress.



10. After upgrade is completed, check the **Version** to confirm that Oracle Management Cloud agents are up to date.



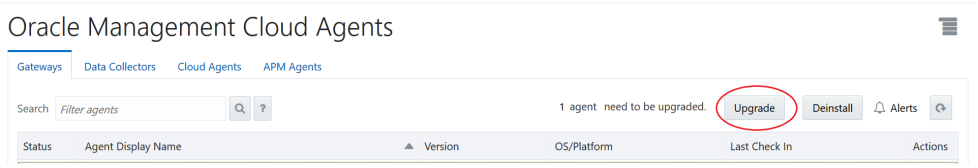
Upgrade a Single Oracle Management Cloud Agent

To upgrade a single Oracle Management Cloud agent using user interface, perform the following steps:

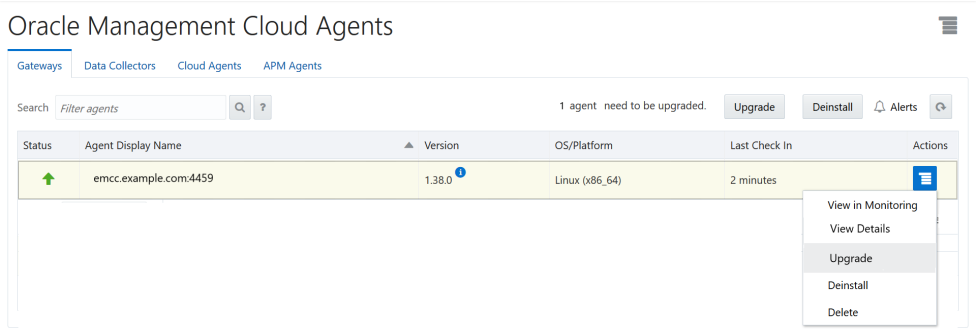
1. On the Oracle Management Cloud page, click the **OMC Navigation** icon on the top-left corner to view the Management Cloud navigation pane, if it isn't already displayed.
2. Select **Agents** under **Administration**.
3. On the Oracle Management Cloud Agents page, click the specific agent tab that needs to be upgraded: **Gateways**, **Data Collectors**, or **Cloud Agents**.

   The Oracle Management Cloud agent tab is displayed.
4. Identify the agent and check if the blue information icon is displayed next to the agent version to confirm that the agent needs to be upgraded.

   You can also use the **Search** feature to find the specific agent.
5. Select the agent and click **Upgrade**.

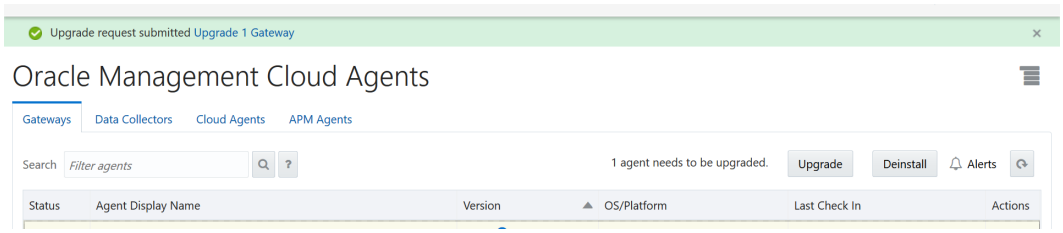


Alternatively, click Actions menu button and select **Upgrade**. If an upgrade is not available, the **Upgrade** option will be disabled.

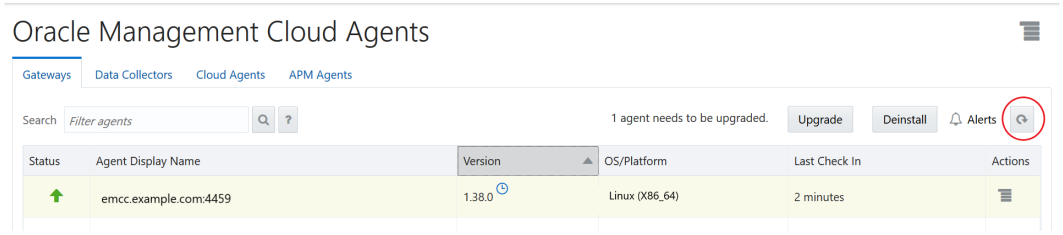


6. A window pops up. It verifies the request and confirms if the agent is eligible to be upgraded. Click **Yes** to proceed.

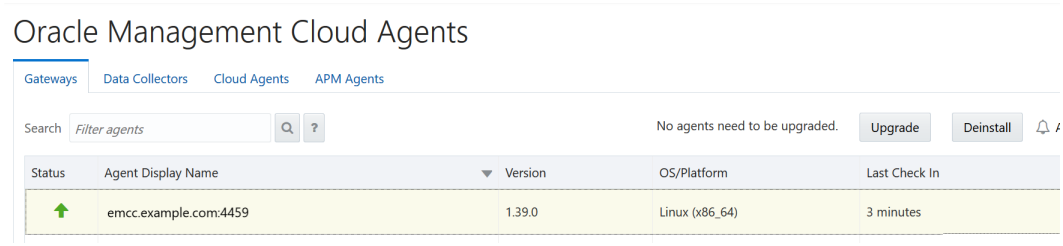
7. You will see a green message at the top of the page: **Upgrade request submitted** along with a link to track the upgrade progress. If you click on the link then the Lifecycle Tasks page will open and you will be able to monitor details of the upgrade task. See Monitor Upgrade Agents Task.



8. Click **Refresh** located at the top right to refresh the page. You will see a blue clock icon next to the version indicating that upgrade is in progress.



9. After upgrade is completed, check the **Version** column to confirm that agent is up to date.



Monitor Upgrade Task Using Lifecycle Tasks

To monitor the Oracle Management Cloud Agents upgrade tasks, use Lifecycle Tasks page. See Agent Lifecycle Tasks for more details.

Upgrade Agents Using Command Line Interface

This section describes how to upgrade gateways, data collectors and cloud agents using command line interface.

Upgrade Using Command Line Interface

To upgrade a single agent from the host it is running on, you can use the `omcli` command line utility.

```
<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli upgrade agent
Oracle Management Cloud Gateway
Copyright (c) 1996, 2018 Oracle Corporation.  All rights reserved.
Upgrade Request was accepted and will be processed as soon as possible.
```

8

Remove Oracle Management Cloud Agents

This section describes how to remove gateways, data collectors and cloud agents.

About Removing Oracle Management Cloud Agents

When you uninstall an Oracle Management Cloud agent associated with a target host, the Oracle Management Cloud agent is unregistered from Oracle Management Cloud and then it's removed.

You remove an agent from your target host if:

- An agent deployed on the target host is no longer necessary.
- You no longer need to collect performance metrics, resource data, or logs for a specific target host.
- You modified your deployment topology.

> **Note:**
>
> If you are removing a gateway, ensure that all data collectors and cloud agents associated with the gateway have also been removed.

Topics:

Remove Agents Using User Interface

This section describes how to remove gateways, data collectors and cloud agents using user interface.

The following remove actions are available:

- **Deinstall**: The selected agent is removed from Oracle Management Cloud and local target host.
- **Delete**: The selected agent is removed only from Oracle Management Cloud. On the local target host, the agent directory is not removed and the agent process is not stopped.

  For example, you can use this action if for some reason your agent target host is no longer available, but you still have the entry on the Oracle Management Cloud User Interface. The delete action will remove and clean up all details from the Oracle Management Cloud User Interface.

Topics:

- Remove a Single Oracle Management Cloud Agent
- Monitor Remove Task using Lifecycle Tasks

Remove Multiple Oracle Management Cloud Agents

To remove multiple Oracle Management Cloud agents using user interface, perform the following steps:

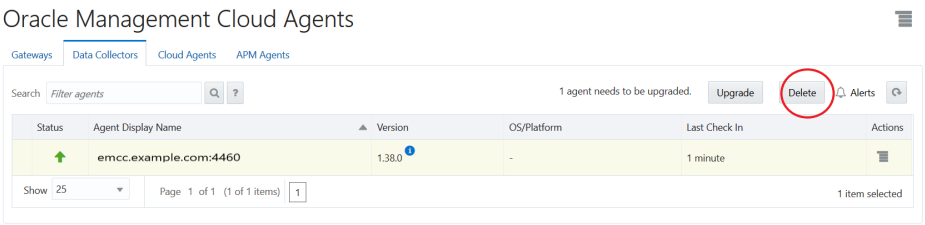
1. On the Oracle Management Cloud page, click the **OMC Navigation** icon on the top-left corner to view the Oracle Management Cloud navigation pane, if it isn't already displayed.
2. Select **Agents** under **Administration**.
3. On the Oracle Management Cloud Agents page, click the specific agent tab that needs to be removed: **Gateways**, **Data Collectors**, or **Cloud Agents**.

   The Oracle Management Cloud agent tab is displayed.
4. Identify the multiple agents that you need to remove.

   You can also use the **Search** feature to find the specific agents.
5. Select the multiple agents: Click the first agent, press and hold the CTRL key and then start clicking the additional agents that you want to remove.
6. Go to the top right corner and click one of the following:
   - **Deinstall** to remove the selected agents from Oracle Management Cloud and local target hosts. Action available if your agent type is gateway or cloud agent.

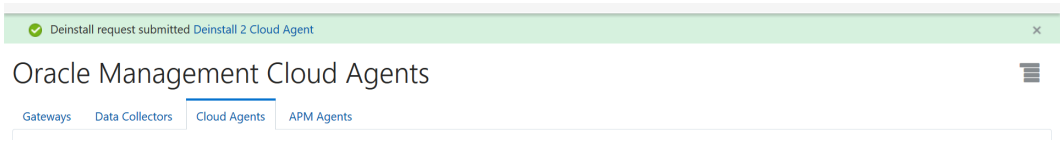
     

   - **Delete** to remove the selected agents only from Oracle Management Cloud. Action available if your agent type is data collector.

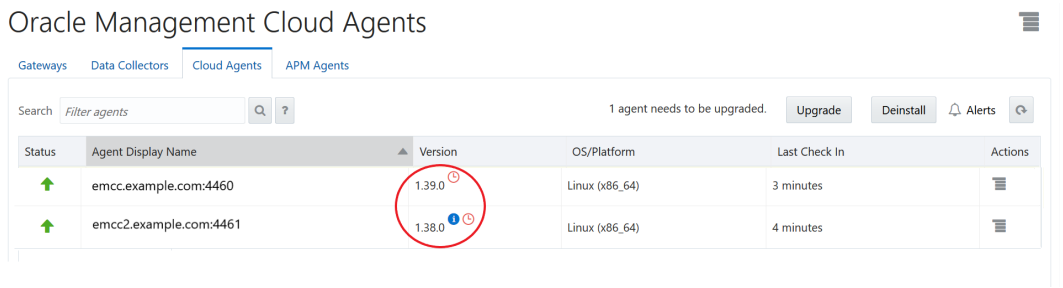
     

7. A window pops up. It verifies the request and confirms if the selected agents are eligible to deinstall or delete. Click **Yes** to proceed.
8. You will see a green message at the top of the page: **Deinstall request submitted** or **Delete request submitted**, depending on your request, along with a link to track the task progress. If you click on the link then the Lifecycle Tasks page will open and you will be able to monitor details of the task. See Monitor Remove Agents Task.

The following image shows the message for a request to deinstall 2 cloud agents:



9. Click **Refresh** located at the top right to refresh the page. You will see a red clock icon next to the agent version indicating that the agent deinstall or delete is in progress.



10. After the task is completed, confirm that the Oracle Management Cloud agent page is up to date and the selected agents are removed and no longer listed.

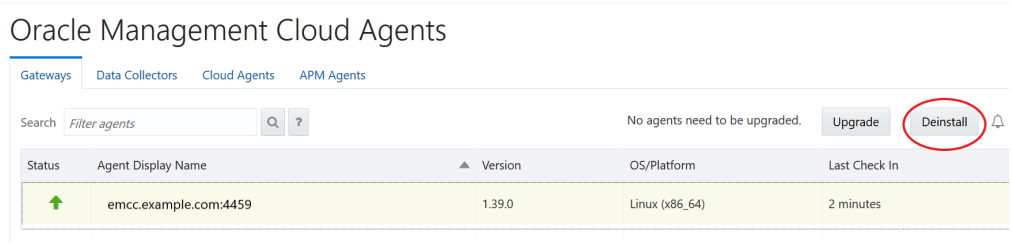
Remove a Single Oracle Management Cloud Agent

To remove an agent using user interface, perform the following steps:

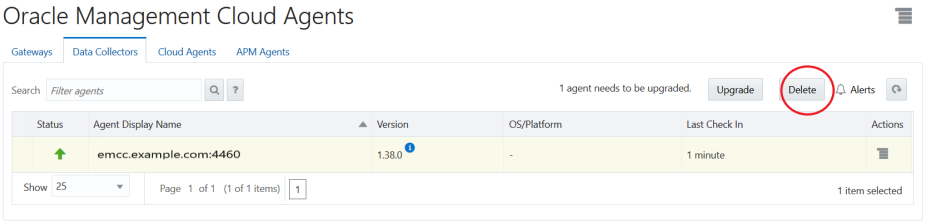
1. On the Oracle Management Cloud page, click the **OMC Navigation** icon on the top-left corner to view the Oracle Management Cloud navigation pane, if it isn't already displayed.
2. Select **Agents** under **Administration**.
3. On the Oracle Management Cloud Agents page, click the specific agent tab that needs to be removed: **Gateways**, **Data Collectors**, or **Cloud Agents**.

   The Oracle Management Cloud agent tab is displayed.
4. Identify the agent that you need to remove.

   You can also use the **Search** feature to find the specific agent.
5. Select the agent. Go to the top right corner and click one of the following:
   - **Deinstall** to remove the selected agent from Oracle Management Cloud and local target host. Action available if your agent type is gateway or cloud agent.

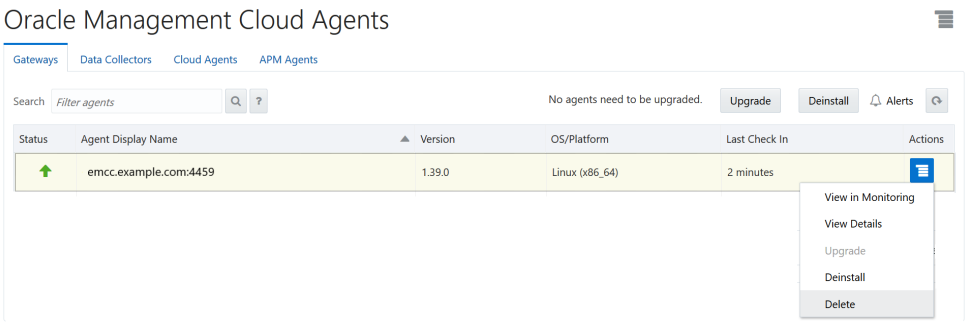


   - **Delete** to remove the selected agent only from Oracle Management Cloud. Action available if your agent type is data collector.



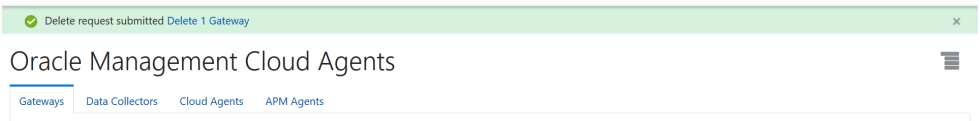
Alternatively, select the specific agent, click Actions menu button and choose the appropriate action:

- **Deinstall**: The selected agent is removed from Oracle Management Cloud and local target host. Action available for gateways and cloud agents.
- **Delete**: The selected agent is removed only from Oracle Management Cloud. On the local target host, the agent directory is not removed and the agent process is not stopped. Action available for gateways, data collectors and cloud agents.



6. A window pops up. It verifies the request and confirms if the agent is eligible to: deinstall or delete. Click **Yes** to proceed.
7. You will see a green message at the top of the page: **Deinstall request submitted** or **Delete request submitted** along with a link to track the task progress. If you click on the link then the Lifecycle Tasks page will open and you will be able to monitor details of the task. See Monitor Remove Agents Task.

   The following image shows the message for a request to delete a gateway:



8. Click **Refresh** located at the top right to refresh the page. You will see a red clock icon next to the agent version indicating that the agent deinstall or delete is in progress.
9. After the task is completed, confirm that the Oracle Management Cloud agent page is up to date and the selected agent is removed and no longer listed.

Monitor Remove Task Using Lifecycle Tasks

To monitor the Oracle Management Cloud Agents remove tasks, use Lifecycle Tasks page. See Agent Lifecycle Tasks for more details.

Remove Agents Using Command Line Interface

This section describes how to remove gateways, data collectors and cloud agents using command line interface.

Remove Agents Using Command Line Interface

To remove an agent using command line interface, you need to use the `AgentInstall` script.

- For Linux/UNIX Systems, you can use `AgentInstall.sh` script to remove agents.

  Run the following:

  – If your agent was installed and it was never upgraded, run the following:

  ```
  <AGENT_BASE_DIRECTORY>/core/<AGENT_VERSION>/sysman/install/
  AgentInstall.sh –deinstall
  ```

  – If your agent was upgraded at least once since the initial installation, run the following:

  ```
  <AGENT_BASE_DIRECTORY>/<latest upgraded version>/core/<AGENT_VERSION>/
  sysman/install/AgentInstall.sh –deinstall
  ```

  The < latest upgraded version> has the following format:

  * Cloud agent: `LAMA_<platform>_<date stamp>`
  * Gateway: `GATEWAY_<platform>_<date stamp>`

- For Windows Systems, you can use `AgentInstall.pl` script to remove agents.

  – If your agent was installed and it was never upgraded, run the following:

  ```
  <AGENT_BASE_DIRECTORY>\core\<AGENT_VERSION>\perl\bin\perl
  <AGENT_BASE_DIRECTORY>\core\<AGENT_VERSION>\sysman\install\AgentInstall.p
  l –deinstall
  ```

  – If your agent was upgraded at least once since the initial installation, run the following:

  ```
  <AGENT_BASE_DIRECTORY>\<date stamp>\core\<AGENT_VERSION>\perl\bin\perl
  <AGENT_BASE_DIRECTORY>\<date
  stamp>\core\<AGENT_VERSION>\sysman\install\AgentInstall.pl –deinstall
  ```

To remove data collectors using command line interface, use the below command:

- For Linux Systems, you can use `AgentInstall.sh` script and run the following:

  ```
  <AGENT_BASE_DIRECTORY>/core/<AGENT_VERSION>/sysman/install/AgentInstall.sh –
  deinstall OMR_USERNAME=omr_privileged_user
  OMR_USER_PASSWORD=omr_user_password OMR_USER_ROLE=omr_user_role
  ```

- For Windows Systems, you can use `AgentInstall.pl` script and run the following:

  ```
  <AGENT_BASE_DIRECTORY>\core\<AGENT_VERSION>\perl\bin\perl
  <AGENT_BASE_DIRECTORY>\core\<AGENT_VERSION>\sysman\install\AgentInstall.pl –
  deinstall OMR_USERNAME=omr_privileged_user
  OMR_USER_PASSWORD=omr_user_password OMR_USER_ROLE=omr_user_role
  ```

Please refer to log file located under /tmp for Linux Systems or `<AGENT_BASE_DIRECTORY>/logs` for Windows Systems for more details.

9

Agent Lifecycle Tasks

You can use the Lifecycle Tasks to monitor the status of the different tasks like upgrade, deinstall or delete of Oracle Management Cloud Agents.

Topics

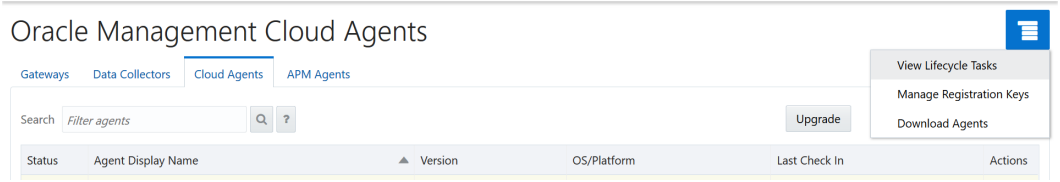
Open Lifecycle Tasks

To open the Lifecycle Tasks page, perform the following steps:

1. On the Oracle Management Cloud page, click the global navigation menu on the top left, then go to **Administration** and click **Agents**.

   The Oracle Management Cloud Agents page is displayed.

2. On the Oracle Management Cloud Agents page, click the Actions Menu on the top right corner of the page and select **View Lifecycle Tasks**.



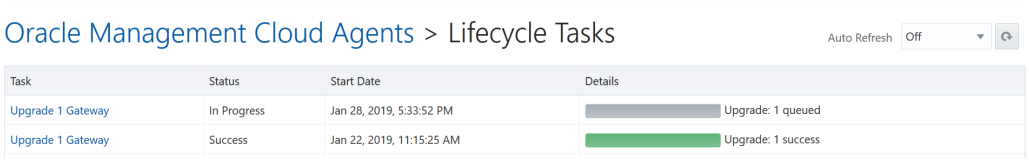
   The Lifecycle Tasks page is displayed.

View Lifecycle Tasks

Lifecycle Tasks shows the status of the upgrade, deinstall and delete tasks. It displays information and other details about the tasks completed or running on the Oracle Management Cloud.

The Lifecycle Tasks page displays the following information:

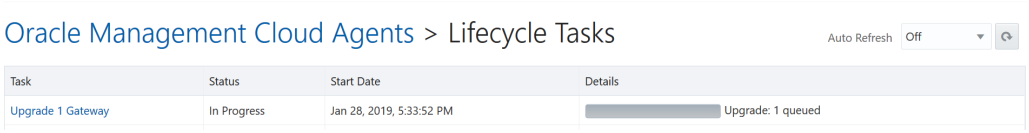
- Task
- Status
- Start Date
- Details



If you click on a task, the task details page will open displaying more details about the specific task.

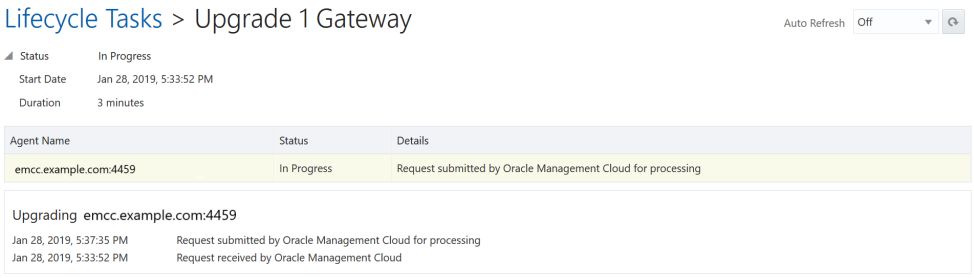
Monitor Upgrade Agents Task

After you request an agent upgrade, you will see a green message at the top the page: **Upgrade request submitted** along with a link to the Lifecycle Tasks page. If you click on the link, Lifecycle Tasks page is displayed.

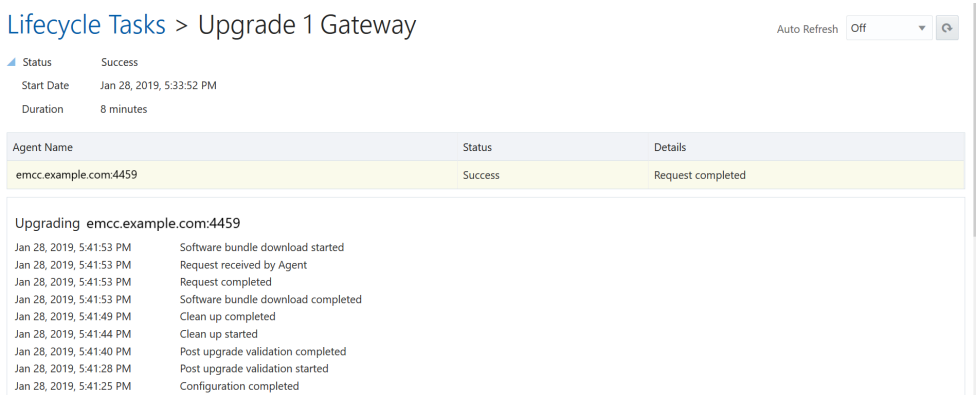


After the Lifecycle Tasks page is displayed, perform the following:

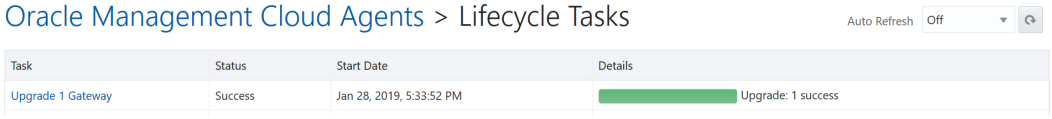
1. Click on the specific task to open the Lifecycle Tasks details page and track the task progress and see more information about it.



2. Click **Refresh** to refresh the page.
3. Once the upgrade task is completed, **Status** will be updated to Success.



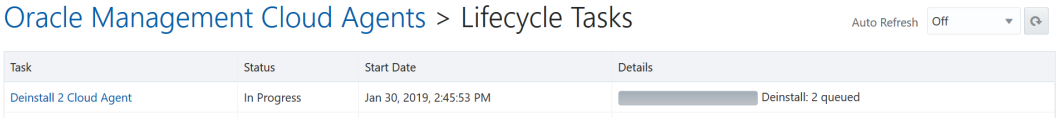
4. Go back to the Lifecycle Tasks main page to see the task summary:



Monitor Remove Agents Task

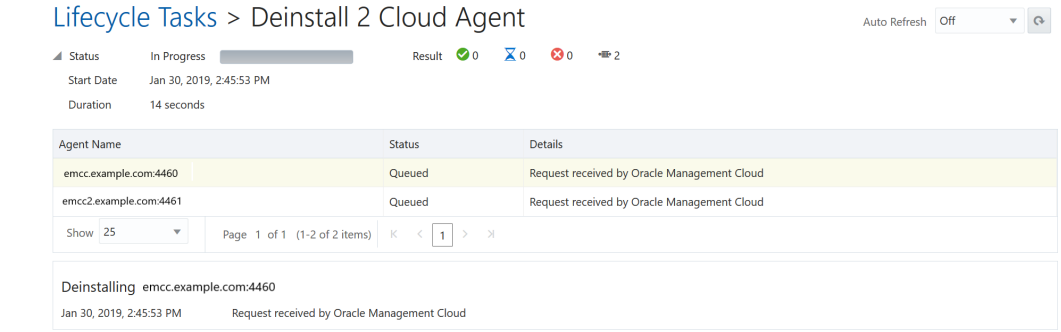
After you request an agent deinstall or delete, you will see a green message at the top the page: **Deinstall request submitted** or **Delete request submitted** along with a link to the Lifecycle Tasks page. If you click on the link, Lifecycle Tasks page is displayed.

- **Deinstall Task:**

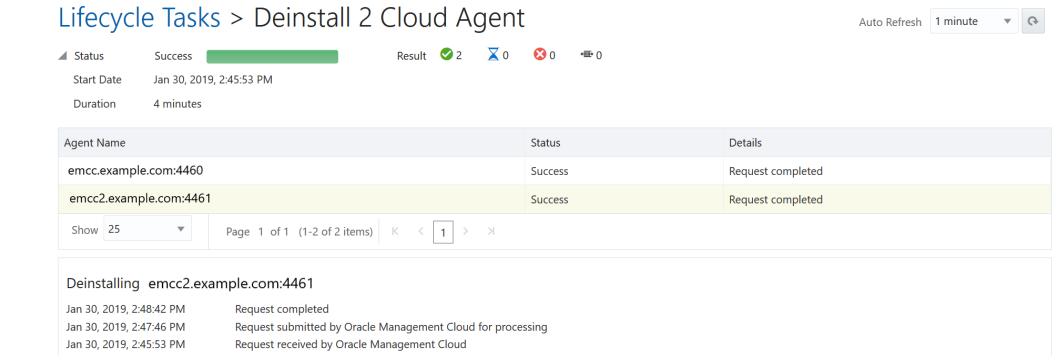


After the Lifecycle Tasks page is displayed, perform the following:

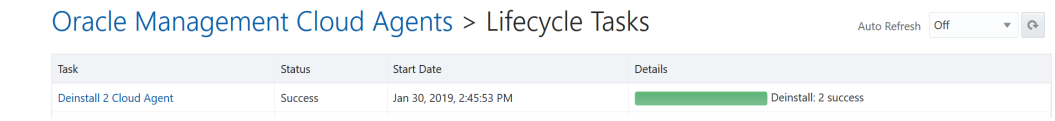
1. Click on the specific task to open the Lifecycle Tasks details page and track the task progress and see more information about it.



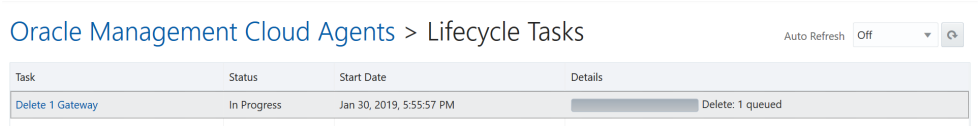
2. Once the task is completed, **Status** will be updated to Success.



3. Go back to the Lifecycle Tasks main page to see the task summary:

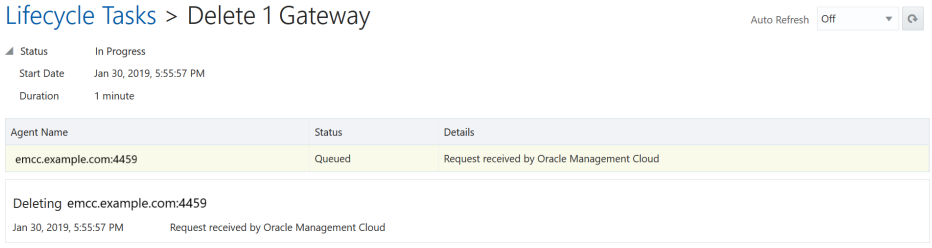


- **Delete Task:**

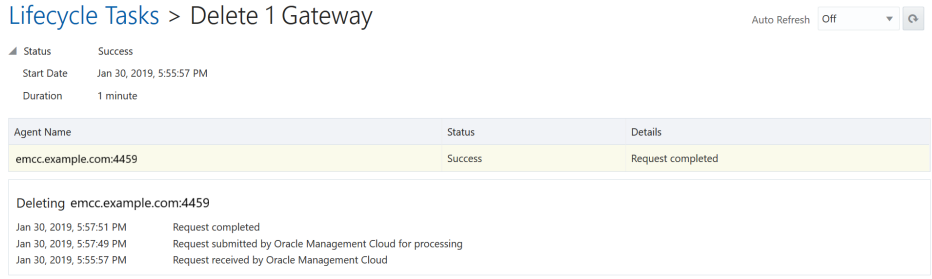


After the Lifecycle Tasks page is displayed, perform the following:

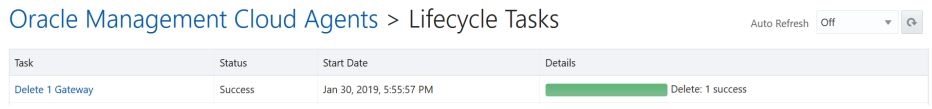
1. Click on the specific task to open the Lifecycle Tasks details page and track the task progress and see more information about it.



2. Once the task is completed, **Status** will be updated to Success.



3. Go back to the Lifecycle Tasks main page to see the task summary:



10

Troubleshoot Oracle Management Cloud Agents

This topic covers the typical issues and their resolutions related to installing and working with Oracle Management Cloud agents.

The topic covers the following:

Oracle Management Cloud Agent Connectivity Issues

If you're encountering any connectivity issues between the Oracle Management Cloud agents and Oracle Management Cloud, then you can run the following command to check the connectivity issues after installation:

```
<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli status agent connectivity
```

The command displays the list of connectivity issues, if any, at the agent.

Running connectivity command without –verbose flag

If you run this command without the `-verbose` flag, then the first line of output identifies the type of agent and whether or not it's running. It also reports if there is any connectivity issues. If that's the case, the subsequent lines list all known communication issues identified for this type of agent given its current availability status. The issues output is organized in three columns: Symptom, Cause and Observed.

Symptom	Cause	Observed
This is the symptom of the issue. For example, one symptom is "The agent is unable to start."	This is the most likely cause of the issue. For example, one cause is "The agent is not registered."	This is the earliest time the agent made the observation.

Example 1: Cloud Agent communicates to Oracle Management Cloud successfully. Cloud Agent has no connectivity issues.

```
$ ./omcli status agent connectivity
Oracle Management Cloud Agent
Copyright (c) 1996, 2019 Oracle Corporation.  All rights reserved.
------------------------------------------------------------
Cloud Agent is Running

No identifiable connectivity issues found between Cloud Agent and
Management Cloud at
https://d123.us2.oraclecloud.com/.
---[OMC Ping Hop]--------------------[Time]-
[Details]--------------------------
OMC d123.us2.oraclecloud.com   71ms   HTTP 200 OK
------------------------------------------------------------------------
--------
```

Example 2: Gateway communicates to Oracle Management Cloud successfully. Gateway has no connectivity issues.

```
$ ./omcli status agent connectivity
Oracle Management Cloud Gateway
Copyright (c) 1996, 2019 Oracle Corporation.  All rights reserved.
------------------------------------------------------------
Gateway is Running

No identifiable connectivity issues found between Gateway and
Management Cloud at
https://d123.us2.oraclecloud.com/.
---[OMC Ping Hop]--------------------[Time]-
[Details]--------------------------
OMC d123.us2.oraclecloud.com   66ms   HTTP 200 OK
------------------------------------------------------------------------
--------
```

Example 3: Cloud Agent communicates to Oracle Management Cloud through a Gateway. Cloud Agent has no connectivity issues.

```
$ ./omcli status agent connectivity
Oracle Management Cloud Agent
Copyright (c) 1996, 2019 Oracle Corporation.  All rights reserved.
------------------------------------------------------------
Cloud Agent is Running

No identifiable connectivity issues found between Cloud Agent and
Gateway.

---[OMC Ping Hop]-----------------------[Time]-
[Details]----------------------
Gateway emcc.example.com:4459   13ms   HTTP 200 OK
OMC d123.us2.oraclecloud.com   90ms   HTTP 200 OK
```

```
--------------------------------------------------------------------------------
---
Check the connectivity status of the Gateway: emcc.example.com
```

Example 4: Cloud Agent communicates to Oracle Management Cloud through a Gateway. Cloud Agent has connectivity issues: It is up and running, but it can't connect to the Gateway.

```
$ ./omcli status agent connectivity
Oracle Management Cloud Agent
Copyright (c) 1996, 2019 Oracle Corporation.  All rights reserved.
----------------------------------------------------------------
Cloud Agent is Running

Connectivity Issues:
Symptom                     Cause
Observed
--------------------------- --------------------------------
-------------------
Agent unable to communicate Agent unable to connect to server 2019-01-29
04:33:25
---[OMC Ping Hop]--------------------[Time]-
[Details]------------------------
Gateway emcc.example.com:4459         1ms
java.net.ConnectException:Connection refused
(Connection refused)
--------------------------------------------------------------------------------
---
The Gateway is unavailable: emcc.example.com
```

Example 5: Cloud Agent communicates to Oracle Management Cloud through a Proxy Server. Cloud Agent has connectivity issues: It is up and running, but it can't connect to the Proxy Server.

```
$ ./omcli status agent connectivity
Oracle Management Cloud Agent
Copyright (c) 1996, 2018 Oracle Corporation.  All rights reserved.
----------------------------------------------------------------
Cloud Agent is Running

Connectivity Issues:
Symptom                     Cause                          Observed
--------------------------- ------------------------------
-------------------
Agent unable to communicate The proxy host is not reachable 2019-01-29
16:09:39
---[OMC Ping Hop]------------------------------[Time]-[Details]-----
OMC 6e8c5404a19b42cd82d.us2.oraclecloud.com:-1  1ms
java.net.UnknownHostException:
NOproxy.example.com
--------------------------------------------------------------------------------
---
```

Running connectivity command with –verbose flag

If you want to see more information, then you can execute a more verbose flavor by adding the `-verbose` flag to the command. This adds the following columns:

Category	Confidence	Detail
The type of issue.	An internal measure of confidence. This can be thought of as a percentage, where 100.0 is certainty and 0.0 is no idea. The confidence measure is based on empirical data and code knowledge.	A message that can give more insight into the occurrence. This may be an exception message or something else.

Understanding the Symptom and the Cause

Cloud Agent Issues

Cause	Symptom
AGENT_UNABLE_TO_START due to AGENT_NOT_REGISTERED	Registration Key and Tenant ID are provided to the agent installer during installation. Oracle Management Cloud identifies an agent using an entity ID/ MEID; this is based on the host and port on which the agent is installed. The agent can’t start without being registered with Oracle Management Cloud. The entity ID given during registration is what identifies this agent to the cloud. That entity ID is missing. The Agent Config phase runs the agent registration. If this fails (which can happen, for example, if there are required proxy settings for the agent that aren’t supplied during the installation), then the agent won’t be registered and won’t be able to start. Review the installation logs and check the proxy settings.
AGENT_UNABLE_TO_COMMUNICATE due to SERVER_UNAVAILABLE	In this case, the agent can’t connect to the server. If the cloud agent is configured for a gateway and it's unable to connect to that gateway, then it could be a network problem, or the gateway isn't running. You can run the connectivity command at the gateway to find out more.
AGENT_UNABLE_TO_COMMUNICATE due to AGENT_CERTIFICATE_MISMATCH	The agent can’t communicate with its gateways or Oracle Management Cloud because of certificate mismatch failures. There might be some third-party certificate at the proxy that got changed, there could have been a failure to download the certificates, or the certificates changed at Oracle Management Cloud.

Gateway Issues

Cause	Symptom
AGENT_UNABLE_TO_START due to AGENT_NOT_REGISTERED	Registration Key and Tenant ID are provided to the agent installer during installation. Oracle Management Cloud identifies an agent using an entity ID/ MEID; this is based on the host and port on which the agent is installed. The agent can't start without being registered with Oracle Management Cloud. The entity ID given during registration is what identifies this agent to the cloud. That entity ID is missing. The Agent Config phase runs the agent registration. If this fails (which can happen, for example, if there are required proxy settings for the agent that aren't supplied during the installation), then the agent won't be registered and won't be able to start. Review the installation logs and check the proxy settings.
AGENT_UNABLE_TO_COMMUNICATE due to AGENT_CERTIFICATE_MISMATCH	The certificate the gateway uses to trust Oracle Management Cloud is no longer correct.
• AGENT_UNABLE_TO_UPLOAD due to DATARECEIVER_SERVICE_MISSING • AGENT_UNABLE_TO_DISPATCH due to DATARECEIVER_SERVICE_MISSING • AGENT_UNABLE_TO_DISPATCH due to WORKDEPOT_SERVICE_MISSING	There is an issue with Oracle Management Cloud. File a service request.

Cloud Agent Installation Fails Due to Insufficient ulimit

Sometimes, cloud agent installation fails with an `OMCAGNT - 2101` error.

This error is caused by an insufficient `ulimit` value. A cloud agent installation requires a minimum of 4000 as the `ulimit` value. However, the recommended value for `ulimit` should be set to 100000 for uninterrupted service of the agent.

To set the `ulimit` value, run the following command:

```
ulimit –u 100000
```

Data Collector Installation Fails Due to Inaccessible Stage Directory

When you install a data collector, if the installation fails with the error "`DataCollector Validation failed with status [1]`". It's difficult to understand the real cause of this failure. In this case, you can set the following parameter in the response file:

```
IGNORE_DATA_COLLECTOR_VALIDATIONS=true
```

This helps you to identify the actual, underlying issues that are causing the installation to fail.

Data Collector Stopped Working After Upgrading to Enterprise Manager 13.x

If you deployed the data collector on Enterprise Manager 12*c* and then upgraded to Enterprise Manager 13.1 or a later release, then the data collector must be updated.

To update the data collector, follow these steps:

1. Click this link to download the `patch_harvester_after_em_upgrade.sql` script, or go to `$ORACLE_HOME/sysman/admin/scripts/emaas/harvester/patch_harvester_after_em_upgrade.sql`
2. Connect to the Oracle Management Repository database as a `SYS` user.
3. Run the downloaded script using `SYS` credentials, and provide the data collector schema name as input.

   You can find the data collector schema name by using the following statement:

   ```
   SELECT owner
   FROM all_objects
   WHERE object_name = 'EMAAS_PERF_LOG'
   and object_type = 'TABLE';
   ```

   > **Note:**
   >
   > If multiple rows are displayed in the output, then contact Oracle Support to find out the correct active schema.

4. After the script is executed, verify that the data collector schema was edition enabled, as follows:

   ```
   SELECT EDITION_ENABLED
   FROM DBA_USERS
   WHERE username = upper('&DATA_COLLECTOR_SCHEMA_NAME')
   ```

   Y indicates that the edition was enabled. If the edition wasn't enabled, then try running the script again. If you still see an issue, then contact Oracle Support.

5. Verify that all the objects are valid in the data collector schema, as follows:

   ```
   SELECT object_name from all_objects where owner =
   upper('&DATA_COLLECTOR_SCHEMA_NAME') and status = 'INVALID';
   ```

   If any invalid objects are found, try recompiling it again. If you still see an issue, then contact Oracle Support.

Host Name Issues

You may see the following error while deploying Oracle Management Cloud agents:

```
"Error: Unable to resolve the ORACLE_HOSTNAME/Computed hostname :
<hostname>."
```

When you install the agent, if the system host name doesn't resolve to a fully qualified domain name (FQDN), because you aren't using a DNS, then add the fully qualified domain name in the `etc/hosts` file, and ensure that it maps to the correct host name and IP address of the host. Ensure that the local host is reachable and resolves to 127.0.0.1. The recommended format is as follows:

```
<ip> <fully_qualified_host_name> <short_host_name>
```

For example:

If your host name is `myhost` and your domain is `example.com` (IPv4):

```
172.16.0.0 myhost.example.com myhost
```

If your host name is `myhost` and your domain is `example.com` (IPv6):

```
aaaa::111:2222:3333:4444 myhost.example.com myhost
```

You can run the following commands to verify this. You should see the same host name and IP address displayed.

```
$getent hosts `hostname`
$host `hostname -f`
```

In the output, the fully qualified domain name must appear in the second field as specified in the `/etc/hosts` file.

If you can ensure that short host names don't have the same value on different hosts in your environment, then you can ignore the FQDN requirement by passing the following argument to the `AgentInstall` script: `IGNORE_VALIDATIONS=true` along with `ORACLE_HOSTNAME=<host_name>`

```
$./AgentInstall.sh IGNORE_VALIDATIONS=true ORACLE_HOSTNAME=<host_name>
```

Frequent Password Changes Affect Data Collection

If the Cloud Control Management Repository passwords are changed frequently, then this may affect the data collector collection. Due to the security policies at your data center, if the operating system password for the user that was used to install the Cloud Control Management Repository is changed, then the data collector stops collecting performance and event data.

To update the data collector with the new password, follow these steps:

1. Stop the data collector agent.

   `<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli stop agent`

2. Run the following command on the host that's running the data collector:

   `<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli change_datacollector_host_pwd agent <new password>`

3. Restart the data collector agent.

   `<AGENT_BASE_DIRECTORY>/agent_inst/bin/omcli start agent`

Debugging a Cloud Agent Installed Through a Gateway

When you install the cloud agent through a gateway, ensure that the gateway host name you provide is the same as the host name you specified when the gateway was installed. Any mismatch will result in a failure, prompting the user with connectivity error.

For example: If you specified the host name as `ORACLE_HOSTANME=abc.xyz.com` when you deployed the gateway, but when you install the cloud agent, you specify `GATEWAY_HOST=abc`, then this will cause the cloud agent registration to fail.

Error Example:

```
2017-02-10 11:29:39,308 [1:EE2D8594] DEBUG - Establishing connection to agent at
https://abc.xyz.com:1846/emd/lifecycle/main/... 2017-02-10 11:29:39,321 [1:EE2D8594]
DEBUG - setting user-interaction allowed to false 2017-02-10 11:29:39,329 [1:EE2D8594]
INFO - Unable to connect to the agent at https://abc.xyz.com:1846/emd/lifecycle/main/
[Connection refused] 2017-02-10 11:29:39,694 [1:EE2D8594] DEBUG - Establishing
connection to agent at https://abc.xyz.com:1846/emd/lifecycle/main/... 2017-02-10
11:29:39,694 [1:EE2D8594] DEBUG - setting user-interaction allowed to false 2017-02-10
```

```
11:29:39,696 [1:EE2D8594] INFO - Disconnecting: client terminus 2017-02-10
11:29:39,696 [1:EE2D8594] INFO - stderr: Status agent Failure:Unable to connect
to the agent at https://abc.xyz.com :1846/emd/lifecycle/main/ [Connection
refused] 2017-02-10 11:29:39,696 [1:EE2D8594] INFO - Exit Code: 1
```

Remove an Incompletely Installed Data Collector

You may need to remove the data collector if the installation is incomplete, or you may need to delete the data collector schema if the data collector home was manually deleted or if the host was decommissioned. In these cases, you must remove the data collector and clean up the left over schema in the Enterprise Manager repository. Follow these steps to remove the data collector and the schema:

1. On the Oracle Management Cloud home page, click the **OMC Navigation** icon on the top-left corner to view the Management Cloud navigation pane, if it isn't already displayed.
2. Select **Agents** under **Administration**.
3. Click the **Data Collectors** menu option to go to the Data Collectors page. If the data collector to be removed still appears on this page, then select the data collector, right click the **Actions** menu, and then click **Remove** to remove the data collector.

   > **Note:**
   >
   > It's recommended that you save a copy of the data collector schema before you delete the data collector.

4. Log in as SYS user to the Oracle Management Repository host, and then run the script to drop collector schema.

   ```
   @<script_path>
   ```

   You are prompted for the data collector schema name. To find the data collector schema name, enter the following command:

   ```
   SELECT owner
         FROM  all_tables
         WHERE table_name='EMAAS_PERF_HV_PROPS'
   ```

   If multiple rows are displayed, then this indicates that there is more than one `data_collector_schema`. You can either drop all the schemas, one after the other, or contact Oracle Support.

   This script checks whether the schema being dropped is a data collector schema. If this validation fails, then the schema won't be dropped.

   In this case, using SYS user credentials, pass the `data_collector_schema_name` as input, and run the following command to drop the data collector schema: `@DROP user <data_collector_schema_name> CASCADE;`

   Don't use this script if your data collector home is intact, and it can communicate with Oracle Management Cloud. In this case, follow the steps in Uninstalling Oracle Management Cloud Agents to remove the data collector.

Agent or Gateway Installation Fails Due to Connectivity Issues from OCI-C to a tenant in OCI

If the installation of Oracle Management Cloud Agent or Gateway is failing, you may have connectivity issues to the Oracle Management Cloud backend services.

You may see the following error message:

```
[OMCAGNT-3018]: Can not connect to Oracle Identity Cloud Service. Please ensure
that the URL [ https://idcs-xxxxx.oraclecloud.com:443/.well-known/idcs-
configuration ] is accessible from the installation host and retry.
```

Root Cause:

The actual root cause is a wrong setting of the MTU size on the network interface which reaches out to the internet. By default, all VMs in OCI have a MTU size of 9000 bytes where a value of 1500 is required for communicating with OMC and IDCS endpoints. The following OCI document describes the general issue in full detail: https://docs.cloud.oracle.com/iaas/Content/Network/Troubleshoot/connectionhang.htm.

Solution:

Customers have to set the MTU size of the outgoing network interface on the gateway (or on the proxy if used) to 1500.

If Customers want to stay with the default value, they can create static host routes to use the smaller MTU value only for certain IPs. For example:

```
[root@proxy] # ip route add 10.10.10.10/32 via 10.0.0.1 mtu 1500
```

Due to load balancers in front of the OMC or IDCS endpoint, you have to perform this for multiple IP addresses usually. Use `getent hosts <OMC-Endpoint | IDCS-Endpoint>` to get all required IP-Addresses.

Update Authenticated Proxy Server Parameters

If you are using an authenticated proxy server, you can edit the `emd.properties` file to update the following proxy parameters: `OMC_PROXYUSER`, `OMC_PROXYPWD` and `OMC_PROXYREALM`.

You can specify the proxy parameters values by using the prefix `CLEAR:` before the parameter value. `CLEAR:` indicates that the value provided is in clear text. For example:

```
OMC_PROXYUSER=CLEAR:johndoe

OMC_PROXYPWD=CLEAR:password

OMC_PROXYREALM=CLEAR:McAfee Web Gateway
```

The value of the `OMC_PROXYREALM` parameter is specific to the authenticated proxy server in use. In the above example, the realm value for McAfee Web Gateway is `McAfee Web Gateway`. Contact your proxy vendor for instructions about how to get the realm value from the proxy settings.

After updating the `emd.properties` file, stop and restart the agent.

The above proxy parameters will be encrypted by the agent and stored in the `emd.properties` file.

Do not use `omcli setproperty` command to set any of the above proxy parameters.

A

Log Files and Debug Logs

This topic covers using log files to check the agent installation, and setting up and collecting debug logs in case you run into problems and need to troubleshoot them.

Using Log Files for Debugging

The agent installation and upgrade logs can be used to troubleshoot issues during installation. Check the following log files for the gateway, data collector, and cloud agents:

- For agent installation failures, check the log file under:

  `<AGENT_BASE_DIRECTORY>/logs/AgentInstall_logs/AgentInstall_<time stamp>`

- After the installation, check the log files at the following path:

  `<AGENT_BASE_DIRECTORY>/agent_inst/sysman/log/*.*`

- If your cloud agent and data collector are using a gateway, then check the gateway log file under:

  `<AGENT_BASE_DIRECTORY>/agent_inst/sysman/log/*.*`

- For all agents (gateway, data collector, and cloud agent), check the update log files under:

  `<AGENT_BASE_DIRECTORY>/logs/AgentUpdate_<time stamp>.log`

Setting up Debug Logs

You can setup debug logs for Oracle Management Cloud agents if you are facing problems after running them for a while.

1. Go to `<AGENT_HOME>/bin` directory on the host that is running the agent.
2. Run the following command to set up the debug logs:

   ```
   $ omcli setproperty agent –name Logger.log.level –value DEBUG
   Oracle Management Cloud Agent
   Copyright (c) 1996, 2018 Oracle Corporation. All rights reserved.
   EMD setproperty succeeded
   ```

3. Verify if the debug log property has been set.

   ```
   $ omcli getproperty agent –name Logger.log.level
   Oracle Management Cloud Agent
   Copyright (c) 1996, 2018 Oracle Corporation. All rights reserved.
   Logger.log.level=DEBUG
   ```

   If the debug property is not set, the output of the above command will display `Logger.log.level=INFO`

```
$ omcli getproperty agent –name Logger.log.level
Oracle Management Cloud Agent
Copyright (c) 1996, 2018 Oracle Corporation. All rights reserved.
Logger.log.level=INFO
```

Collecting Debug Logs

You can collect debug logs by generating a bundle that contains all the logs needed for troubleshooting. Once bundle is generated, you can review the logs within it or you can pass it to Oracle Support for further assistance.

Run the following command to collect debug logs:

```
$ omcli generate_support_bundle agent <directory_where_bundle_will_be_created>
```

B
omcli Command Options

`omcli` commands let you work with Oracle Management Cloud agents and entities.

Accessing omcli

`omcli` comes bundled with a deployment of Oracle Management Cloud. You can access `omcli` from the <*AGENT_BASE_DIR*>/agent_inst/bin folder.

omcli Commands

Command	Usage
`start`	`omcli start agent` Starts the Oracle Management Cloud agents on the host.
`stop`	`omcli stop agent` Stops the Oracle Management Cloud agents running on the host.
`status`	`omcli status agent` Retrieves the status of the Oracle Management Cloud agents running on the host.
`setproperty`	`omcli setproperty agent [-allow_new] -name` *PROPERTY_NAME* `-value` *PROPERTY_VALUE* Sets the specified property name and value in the agent configuration file. `-allow_new` is an optional parameter that inserts a new property in the agent configuration file if the property doesn't exist. `-allow_new` must be the first option to be provided to the command.
`getproperty`	`omcli getproperty agent -name` *NAME_1* `[...` *NAME_N*`] | -category` *NAME_1* Gets the specified properties or a category of properties from the agent configuration files. `-name` accepts a list of property names separated by spaces. However, you can't have spaces in the property names.
`dumpstate`	`omcli dumpstate agent [-dump_full_state] [`*COMPONENTNAME ...*`]` Dumps the internal state of the specified list of components.
`clear_property`	`omcli clear_property agent -name` *PROPERTY_NAME* Clears the value for the specified property in the agent configuration file.
`status`	`omcli status agent [`*TIMEOUT*`]` Returns the status of the agent. *TIMEOUT* is the timeout value in seconds.
`reload`	`omcli reload agent` Reloads the configuration properties of the agent.

Command	Usage
`upgrade`	`omcli upgrade agent` Requests an upgrade of the agent to the latest available version. The request will be accepted only if the agent is eligible for an upgrade. Once the request is accepted, the agent will be upgraded as soon as possible.
`getversion`	`omcli getversion agent` Prints the version of the agent.
`status agent scheduler`	`omcli status agent scheduler [-summary]` Displays the status of the agent scheduler. The `status agent scheduler` command lists the tasks that are periodically scheduled by the agent. It includes collection items and internal tasks.
`status agent connectivity`	`omcli status agent connectivity [-verbose]` Displays current connectivity issues the agent is suffering. Also, it indicates whether the agent is running or not. If the agent is not running, it displays connectivity issues experienced at the time of the shutdown.
`config agent getTZ`	`omcli config agent getTZ` Gets the system time zone from the environment.
`config agent listtargets`	`omcli config agent listtargets` Lists the entities that were registered with the agent.

Command	Usage

`add_entity`	`omcli add_entity agent FILENAME [-credential_file CREDENTIAL_FILE [-encryption_method_gpg]] [-tag_all] [-no_check] [-force]`
	Adds the defined entity to Oracle Management Cloud.
	• *FILENAME* is the name of the file that contains the entity definition to be added. This file cannot contain any credentials.
	• *CREDENTIAL_FILE* is an optional parameter and is required only if you need to add entities with credentials.
	A credential file follows this format:
	`{"credentials": [ {"id":"id1", "name":"credName1", "credType":"type1", "properties":[{"name":"prop1", "value":"CLEAR[value1]"}, {"name":"prop2", "value":"FILE[/tmp/filename]"}] } ] }`
	This sample format includes:
	– A credential with an ID (`id1`). This credential must match the credential reference in the entity definition and must be unique.
	– A name (`CredName1`) that you specify to distinguish your credentials.
	– A credential type, from a predefined set of known types (for example, `DBCreds` for databases).
	– A property name (`prop1`) whose value (`value1`) is specified in clear text.
	– A property (`prop2`) whose value is the contents of the file `/tmp/filename`.
	• `-encryption_method_gpg` is an optional parameter. If specified, this option indicates that the file is encrypted using `gpg` symmetric encryption.
	• `-tag_all` is an optional parameter. If specified, the tags in the definition are applied to all the sub-entities as well. The default behavior is that the tags only apply to the entity.
	• `-no_check` is an optional parameter. If specified, the credential password is *not* checked before updating. The default behavior is that the credential password is checked.
	• `-force` is an optional parameter. If specified, all validation errors are ignored.

Command	Usage

`update_entity`	`omcli update_entity agent FILENAME [-credential_file CREDENTIAL_FILE [-encryption_method_gpg]] [-tag_all] [-no_check] [-force]`
	Updates an existing entity.
	• *FILENAME* is the name of the file that contains the entity definition to be updated. This file cannot contain any credentials.
	• *CREDENTIAL_FILE* is an optional parameter and is required only if you need to add entities with credentials.
	A credentials file follows this format:
	`{"credentials": [ {"id":"id1", "name":"credName1", "credType":"type1", "properties": [{"name":"prop1", "value":"CLEAR[value1]"}, {"name":"prop2", "value":"FILE[/tmp/filename]"}] } ] }`
	This sample format includes:
	– A credential with an ID (`id1`). This credential must match the credential reference in the entity definition and must be unique.
	– A name (`CredName1`) that you specify to distinguish your credentials.
	– A credential type, from a predefined set of known types (for example, `DBCreds` for databases).
	– A property, (`prop1`), whose value, (`value1`), is specified in clear text.
	– A property, (`prop2`), whose value is the contents of the file `/tmp/filename`.
	• `-encryption_method_gpg` is an optional parameter. If specified, this option indicates that the file is encrypted using `gpg` symmetric encryption.
	• `-tag_all` is an optional parameter. If specified, the tags in the definition are applied to all the sub-entities as well. The default behavior is that the tags only apply to the entity.
	• `-no_check` is an optional parameter. If specified, the credential password is *not* checked before updating. The default behavior is that the credential password is checked.
	• `-force` is an optional parameter. If specified, all validation errors are ignored.

`delete_entity`	`omcli delete_entity agent FILENAME` Deletes an existing entity. *FILENAME* is the name of the file that contains the entity definition to be deleted.

Command	Usage
`refresh_entity`	`omcli refresh_entity agent FILENAME [-preserve]` Refreshes an existing entity, such as a WebLogic Domain, to ensure that Oracle Management Cloud is synchronized with the changes made to the entity. For example, if WebLogic Servers are added to or removed from the WebLogic Domain, then this command ensures that the changes reflect in Oracle Management Cloud as well. • *FILENAME* is the name of the file that contains the entity definition to be refreshed. • `[-preserve]` is an optional parameter. If specified, deleted entities are preserved and continue to exist in Oracle Management Cloud.
`status_entity`	`omcli status_entity agent FILENAME [-long] [-verbose]` Verifies and displays the status of the entity. • *FILENAME* is the name of the file that contains the entity definition whose status must be verified. The format of this file is the same as in the file used for the add or update entity operation. • `-long` is an optional parameter. If specified, the status of the entity is extracted from Oracle Management Cloud as well. • `-verbose` is an optional parameter. If specified, detailed messages for entity operations are extracted.
`add_credential_store`	`omcli add_credential_store agent [ wallet-file ] [ -no_password ]` Configures the agent to use a wallet-based credential store. The wallet can be pre-existing. The wallet can be found in the location identified by `wallet-file`; if no `wallet-file` is specified, then the wallet is created in `$EMSTATE/sysman/config/creds/`. If `-no_password` is specified, then an SSO wallet (protected only by file permissions) will be created and used. If the `-no_password` token is omitted, then you are prompted for a password to use in the wallet. **Note:** To add a credential store to an agent, stop the agent, add the credential store, then restart the agent.

Command	Usage
add_credentials	omcli add_credentials agent -credential_file CREDENTIALS_FILE [-encryption_method_gpg] [-allow_entityless] Adds a file full of credentials to the agent. Credentials listed in CREDENTIALS_FILE are of the following form: { "entity":"lama.abc.example.com:1899", "name":"lama.abc.example.com:1899-HostSSHPwdCreds", "type":"HostSSHPwdCreds", "globalName":"AgentUserCredential", "description":"SSH Credential for the agent user", "properties":[{ "name":"USERNAME", "value":"CLEAR[aime]" }, { "name":"PASSWORD", "value":"CLEAR[2cool]" }] } If -encryption_method_gpg is specified, then the credentials file is encrypted using symmetric gpg, and a passphrase may be needed. If -allow_entityless is specified, then the agent will not produce an error about credentials that are missing the entity field. However, a global name should be supplied if an entity isn't.
list_credentials	omcli list_credentials agent [TARGETNAME:TARGETTYPE | -global] [-usage USAGE] Lists the non-sensitive credential attributes for specified credentials. If an entity is specified, then only the credential definitions relative to the entity are listed. If -global is specified, then only the credential definitions with global names are listed. If neither is specified, then all credentials are listed. If -usage is specified, then only the credentials that may be used for that usage are listed. When supplied, USAGE can have one of the following values: • ORCHESTRATION • MONITORING • INTERNAL
disable_credential	omcli disable_credential agent CREDENTIAL_NAME [TARGETNAME:TARGETTYPE | -global] Disables the specified credential. If -global is provided, then only the credentials with the CREDENTIAL_NAME global name are disabled. If CREDENTIAL_NAME TARGETNAME:TARGETTYPE is specified, then only the credentials with the CREDENTIALS_NAME local name are disabled within the entity's scope.
enable_credential	omcli enable_credential agent CREDENTIAL_NAME [TARGETNAME:TARGETTYPE | -global] Enables the specified credential. If -global is provided, then only the credentials with the CREDENTIAL_NAME global name are enabled. If CREDENTIAL_NAME TARGETNAME:TARGETTYPE is specified, then only the credentials with the CREDENTIAL_NAME local name are enabled within the entity's scope.

Command	Usage
remove_credential	omcli remove_credential agent CREDENTIAL_NAME [TARGETNAME:TARGETTYPE | -global] Removes the specified credential. If -global is provided, then only the credential with the CREDENTIAL_NAME global name is removed. If CREDENTIAL_NAME TARGETNAME:TARGETTYPE is specified, then the credential with name CREDENTIAL_NAME on the specified TARGETNAME (entity name) is removed.
set_credential_alias	omcli set_credential_alias agent ALIAS_NAME TARGETNAME:TARGETTYPE CREDENTIAL_NAME [TARGETNAME:TARGETTYPE | -global] Sets the credential alias ALIAS_NAME to refer to credential CREDENTIAL_NAME within the entity. If -global is provided, then the ALIAS_NAME credential alias will be created referring to the credential with global name CREDENTIAL_NAME.
remove_credential_alias	omcli remove_credential_alias agent ALIAS_NAME TARGETNAME:TARGETTYPE Removes the specified credential alias within the scope of the entity.
generate_support_bundle	omcli generate_support_bundle agent DIRECTORY Generates a specific set of logs and configuration information that can be used to diagnose problems with the agent. DIRECTORY specifies the directory in which the archive bundle will be generated.
secure	omcli secure agent Secures communication for the agent.
secure add_trust_cert_to_jks	omcli secure add_trust_cert_to_jks [-password <password> -trust_certs_loc <loc> -alias <alias>] Allows to add/import additional certificates to the agent's monitoring truststore for secure communication between the agent and its monitored entities. The location of the agent's monitoring truststore is: <AGENT_BASE_DIR>/agent_inst/sysman/config/montrust/AgentTrust.jks • If -password is specified, <password> is the password to AgentTrust.jks agent truststore. • If -trust_certs_loc is specified, <loc> is the location of the trust certificate file to import into the agent truststore. • If -alias is specified, <alias> is the alias for the certificate to import.

C

Sample Response Files

This topic provides a set of sample response files that are required to install Oracle Management Cloud agents.

Topics:

Sample Response File for Installing a Gateway Over a Proxy Server

Click to download the sample response file.

Sample Response File for Installing a Data Collector Over a Gateway

Click to download the sample response file.

Sample Response File for Installing a Cloud Agent with Additional Gateways

Click to download the sample response file.

D

Custom Certificates

This topic covers working with custom certificates and exporting them to a file. We recommend to work with the IT Security team within your organization to obtain the correct custom certificate.

Work with Custom Certificates

If your environment uses custom certificates, it's important that you work with the IT Security team within your organization to obtain the correct custom certificate to be able to perform a successful gateway or cloud agent installation. They should provide a custom root certificate of the used proxy server in a DER format file.

Export Custom Certificates

If you can't obtain the certificate from your IT Security team, one way to get it is by exporting the certificate to a file using a browser.

Before attempting to export a custom certificate, be sure that the browser is connecting to the internet via the same proxy like the system where the gateway or cloud agent needs to get installed.

To export a custom certificate, do the following:

- Using your browser security options, select **View Certificate** and go to the **Certificate Hierarchy** tab or menu depending on your browser options. Be sure to review the **Certificate Hierarchy** which lists all the certificates available.
- Export the certificate to a file: It's important to export the top-most certificate from the list. The top-most certificate usually has the suffix `Root CA` within its name. Once you identify the correct certificate, select it and then export it to a file with DER format.