Dell EMC OEM Identity Module

Installation Guide using RACADM Command Line Interface

A document to describe the process of installing an Identity Module on a Dell EMC server using RACADM.
June 2018

Revisions

Date	Description
June 2018	Initial release

Table of contents

1 Introduction

The Dell EMC OEM Identity Module enables OEMs to rebrand and customize their products. The Identity module centralizes the control points of multiple features, enabling OEM customers to save time and resources when deploying their systems.

You can install the OEM Identity Module using the following:

- Dell Remote Access Controller Admin utility
- RACADM — Remote RACADM or Local RACADM
- iDRAC web interface

This document describes the process of installing an OEM Identity Module on a Dell EMC enterprise system using RACADM.

RACADM is a command-line interface for iDRAC, which allows for remote and local management of Dell EMC servers. For more details on RACADM, see RACADM Command Line Interface for DRAC.

The target audience for this document is OEM customers and partners of Dell EMC who are looking for a command line method of installing an Identity Module.

For installing the module using the iDRAC web interface, see *Dell EMC OEM Identity Module Installation Guide using iDRAC Web Interface.*

Note: The Dell EMC OEM Identity Module is also referred to as Personality Module in some earlier documentation.

2 Prerequisites

- iDRAC version 1.30.30 or later.
- A system with a supported Windows or Linux OS to execute RACADM commands.
- CSIOR must be enabled. For more information, see *Lifecycle Controller User's Guide*.
- RACADM utilities must be installed. For more information about installing remote and local RACADM utilities, see RACADM Command Line Interface for DRAC.
  - Remote RACADM: If you are using a management station for installing the Identity Module on the target server, download and install the Remote RACADM utility on the management station.
  - Local RACADM: If you are using RACADM on the same server where the Identity Module is being installed, install the Local RACADM utility on the target system.
- `CustBSU.pm` file – Use this file while performing the steps mentioned in this document. In some cases, you may have a `[PartNumber]_CustBSU_ver.exe` file. To access the `CustBSU.pm` file located in this self-extracting package, extract the contents of this file and locate the `CustBSU.pm` file.

Note: Do not use the `[PartNumber]_Cust_ver.exe` file for initial installation.

3 Installing Identity Module

The procedure to install the Identity Module is as follows:

1. Upload the Identity Module file
2. Check the job status in the iDRAC job queue
3. Reset the iDRAC
4. Configure BIOS to load defaults at reboot
5. Reboot the host system

3.1 Uploading Identity Module file

You can upload the Identity Module file from a local or network path using the `update` subcommand.

3.1.1 Uploading Identity Module file using Remote RACADM

3.1.1.1 Local path

Command

```
racadm <ip address or hostname> -u <username> -p <password> update –f
<path to .pm file>
```

Example:

```
racadm 1.2.3.4 –u admin –p mypass update –f /root/IdentityModuleFile.pm
```

3.1.1.2 Remote share

Command:

```
racadm <iDRAC ip address or hostname> -u <iDRAC username> -p <iDRAC
password> update -f <.pm file name> -u <share user name> -p <share
password> -l <path to share>
```

Example for CIFS:

```
racadm 1.2.3.4 -u dracadmin -p dracpass update -f IdentityModuleFile.pm
-u admin -p mypass -l //1.2.3.4/folder
```

Example for NFS:

```
racadm 1.2.3.4 -u dracadmin -p dracpass update -f IdentityModuleFile.pm
-u admin -p mypass -l 1.2.3.4:/folder
```

3.1.2 Uploading Identity Module file using Local RACADM

3.1.2.1 Local path

Command: `racadm update -f <path to .pm file>`

Example: `racadm update -f /root/IdentityModuleFile.pm`

3.1.2.2 Remote share

Command: `racadm update -f <.pm file name> -u <user name> -p <password> -l <path to share>`

Example for CIFS: `racadm update –f IdentityModuleFile.pm -u admin -p mypass -l //1.2.3.4/folder`

Example for NFS: `racadm update -f IdentityModuleFile.pm -u admin -p mypass -l 1.2.3.4:/folder`

3.2 Checking the Job Queue status

After you execute the `update` command, the file is placed in the job queue of iDRAC. Check the status of the job queue by using the following commands:

Local RACADM: `racadm jobqueue view`

Remote RACADM: `racadm -r <ip address or hostname> -u <username> -p <password> jobqueue view`

When the Identity Module file is processed through the queue, the status displays **Completed**.

```
------------------------JOB QUEUE-----------------------
[Job ID=JID_832353087747]
Job Name=Firmware Update: OEM ID Module Status=Completed
Start Time=[Not Applicable] Expiration Time=[Not Applicable]
Message=[RED001: Job completed successfully.]
--------------------------------------------------------
```

The process from uploading the Identity Module file to the job being complete generally takes less than 30 seconds.

3.3 Resetting iDRAC

After the job is complete, reset the iDRAC using the following commands:

Local RACADM: `racadm racreset`

Remote RACADM: `racadm -r <ip address or hostname> -u <username> -p <password> racreset`

The iDRAC reset process takes approximately 2-3 minutes. To confirm that the iDRAC is reset and is functioning, use a test command.

Example:

Local RADADM: `racadm getsysinfo`

Remote RACADM:
```
racadm -r <ip address or hostname> -u <username> -p <password>
getsysinfo
```

If the command returns the requested information, iDRAC the reset process is complete and iDRAC is functioning normally.

If the command times-out, the reset process is not yet complete. Wait for a minute and try the command again.

3.4 Setting BIOS to load defaults at reboot

The server must be rebooted in a subsequent step. Upon that reboot the BIOS must be set to load the new defaults provided by the Identity Module. The following command instructs the BIOS to load the defaults at next reboot:

Local RACADM: `racadm Set LifecycleController.LCAttributes.BIOSRTDRequested True`

Remote RACADM:
```
racadm -r <ip address or hostname> -u <username> -p <password> Set
LifecycleController.LCAttributes.BIOSRTDRequested True
```

3.5 Rebooting the Server

Reboot the server using the following command:

Local RACADM: `racadm serveraction hardreset -f`

Remote RACADM:
```
racadm -r <ip address or hostname> -u <username> -p <password>
serveraction hardreset -f
```

During the reboot, the Identity Module performs the rebranding and the host automatically reboots again.

4 Verifying installation of Identity Module

To verify if an Identity Module is successfully installed in a Dell EMC server, use the following commands. These commands list the versions of all the installed firmware and software.

Local RADADM: `racadm swinventory`

Remote RACADM: `racadm -r <ip address or hostname> -u <username> -p <password> swinventory`

Search for the text `IDENTITY MODULE`. If the text is not present, the Identity Module is not installed.

5 Contact information

For questions related to this document, contact the account manager responsible for the customer engagement.