Dell EMC OpenManage Ansible Modules 4.0.0

Security Configuration Guide

August 2021
Rev. A00

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

Preface

Dell EMC OpenManage Ansible Modules(OMAM) allows data center and IT administrators to use RedHat Ansible to automate and orchestrate the configuration, deployment, and update of Dell EMC PowerEdge Servers and modular infrastructure by leveraging the management automation capabilities in-built into the Integrated Dell Remote Access Controller (iDRAC), OpenManage Enterprise, and OpenManage Enterprise Modular.

OpenManage Ansible Modules simplifies and automates provisioning, deployment, and updates of PowerEdge servers and modular infrastructure. It allows system administrators and software developers to introduce the physical infrastructure provisioning into their software provisioning stack, integrate with existing DevOps pipelines and manage their infrastructure using version-controlled playbooks, server configuration profiles, and templates in line with the Infrastructure-as-Code (IaC) principles.

As part of an effort to improve its product lines, Dell EMC periodically releases revisions of its software and hardware. Some functions that are described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information about product features. Contact your Dell EMC technical support professional if a product does not function properly or does not function as described in this document. This document was accurate at publication time. To ensure that you are using the latest version of this document, go to https://github.com/dell/dellemc-openmanage-ansible-modules.

Topics:

Scope of the document

This document includes information about the security features and capabilities of OpenManage Ansible Modules (OMAM).

Document references

In addition to this guide, you can access the associated OMAM guides available at https://www.dell.com/support:

- OpenManage Ansible Modules Installation Guide
- OpenManage Ansible Modules User's Guide.
- OpenManage Ansible Modules Release Notes.

2

Security Quick Reference

Topics:

Deployment Model

OpenManage Ansible Modules release follows a monthly release cycle. Minor versions are released on the last week of each month and are posted to GitHub as well as to the Ansible-Galaxy (as collections). Once there are enough features, updates, and security fixes released over a series of minor releases and patches, a major version containing all these changes is eventually released to GitHub and Ansible Galaxy (as collections). To install the OMAM from Github or Ansible galaxy refer https://github.com/dell/dellemc-openmanage-ansible-modules.

Security Profiles

OMAM has a default security profile for secure HTTP access.

3

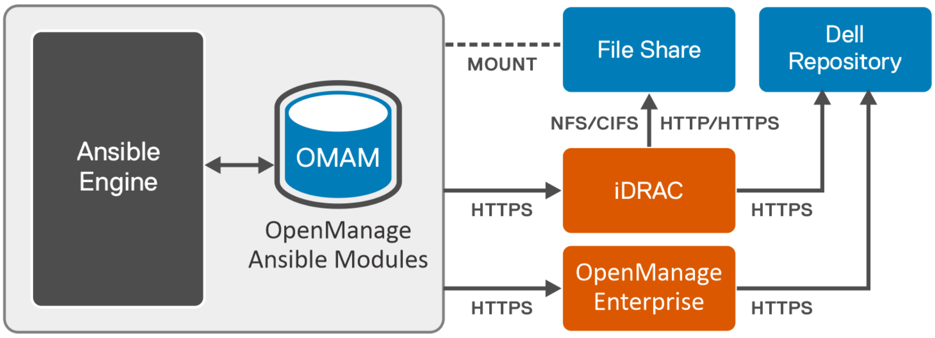
Product and Subsystem Security

Topics:

Security controls map

OpenManage Ansible Modules use Ansible Playbooks to run commands for interacting with iDRAC and Open Manage Enterprise. The system credentials are not stored by default. Some iDRAC modules use a file system to temporarily read and write files to a local Ansible control machine or a file server. The file server path is mounted on the Ansible control machine, and you must securely configure the file servers.

iDRAC and OpenManage Enterprise communicate with Dell server for firmware updates over a HTTPS channel, facilitated by the Ansible control machine through modules and playbooks. The following figure displays the OMAM security controls map:



Authentication

Access control settings provide protection of resources against unauthorized access. OMAM does not have any access control system of its own. It is dependent on the access control settings which are provided by Ansible, File Server, iDRAC, OpenManage Enterprise, and Redfish endpoints.

For more information about the connection methods see the Ansible documentation.

Authentication with external systems

The OMAM modules communicate with iDRAC and OpenManage Enterprise over a secure HTTPS channel. OMAM supports session-based authentication for REST calls.

Session-based authentication is used when issuing multiple Representational State Transfer (REST) requests.

- Session login is initiated by accessing the Create session URI. The response to this request includes an X-Auth-Token header with a session token. Authentication for subsequent requests is made using the X-Auth-Token header.

- Session logout is performed by issuing a DELETE of the Session resource provided by the Login operation including the X-Auth-Token header.

iDRAC authentication

The Integrated Dell Remote Access Controller (iDRAC) is designed to make you more productive as a system administrator and improves the overall availability of Dell EMC servers. iDRAC alerts you on system issues, remotely manage your systems, and reduces the need for physical access to the system. See the latest iDRAC User Guide for more details on available methods of authentication.

OMAM communicates with iDRAC using WSMan and REST. OMAM supports both session-based and basic authentication for iDRAC REST calls over HTTPS.

OMAM supports standard Redfish endpoints as well. Both session-based and basic authentication are supported.

OpenManage Enterprise Authentication

OpenManage Enterprise is a simple-to-use, one-to-many systems management console. It is cost effective and facilitates comprehensive lifecycle management for Dell EMC PowerEdge servers through one console. OpenManage Enterprise supports basic authentication and X-Auth-Token Authentication for the REST calls. For more information, see the latest OpenManage Enterprise API guide.

OMAM supports both session-based and basic authentication for OpenManage Enterprise over HTTPS.

File server authentication

Some of the OMAM modules take the artifacts from CIFS or NFS shares as module parameters. These shares are accessed by iDRAC services to perform operations such as firmware update, system configuration exports or imports. It is recommended to configure the share folders securely with the required user access controls.

Data security

OMAM does not store data. See Ansible Vault for details on securing credentials passed to external systems.

Serviceability

The support website https://www.dell.com/support provides access to product documentation, advisories, downloads, and troubleshooting information. This information helps you to resolve a product issue before you contact the support team.

Security patches

OMAM follows a monthly release cycle. On the last week of every month, the updated modules are posted on GitHub. The monthly OMAM releases include feature updates, defect fixes, and security only updates. Every major release is uploaded on the Dell support site. For a critical security issue, a security patch is released as soon as possible.

Network security

OMAM uses HTTPS with a default security profile to communicate with OpenManage Enterprise and iDRAC. This release does not support SSL certificate validation.

Auditing and logging

OMAM does not have its own logging mechanism, and it depends on the default Ansible logging capability. By default, Ansible sends output about plays, tasks, and module arguments to your screen (STDOUT) on the control node see Logging Ansible Output for more details. Encryption with Ansible Vault only protects data at rest. Once the content is decrypted (data in use), play and plugin authors are responsible for avoiding any secret disclosure. For details on hiding output, see no_log. For security considerations on editors that you use with Ansible Vault, see Steps to secure your editor.

Protecting sensitive data with 'no log'

If you save Ansible output to a log, you expose any secret data in your Ansible output, such as passwords and usernames. To keep sensitive values out of your logs, mark tasks that expose them with the `no_log: True` attribute. However, the no_log attribute does not affect debugging output.

4

Miscellaneous configuration and management

Topics:

- OpenManage Ansible modules licensing
- Protect authenticity and integrity
- Signature file verification
- Ansible module security

OpenManage Ansible modules licensing

OMAM is open source and licensed under the **GNU General Public License v3.0+.** For more details see COPYING.md. iDRAC and OpenManage Enterprise may require its own licenses for some functions in OMAM to work. Refer the User Guide for more details.

Protect authenticity and integrity

To ensure the product integrity, the OMAM installation package is signed and uploaded to https://www.dell.com/support. The collection bundle uploaded to ansible-galaxy is also signed.

Signature file verification

About this task

To verify the signature file, perform the following steps:

Steps

1. Download GPG3 public key from https://linux.dell.com/files/pgp_pubkeys/0x1285491434D8786F.asc.
2. Import the public key in the system using GPG. `gpg --import 0x1285491434D8786F.asc`
3. Upon running `gpg --list-key`, it lists the key ID 34D8786F.
4. Validate signature file using `gpg --verify <FileName>.tar.gz.sign <FileName>.tar.gz or gpg -v --verify <FileName>.tar.gz.sign <FileName>.tar.gz`

   Verification is successful if you see the following output:

```
gpg: Signature made Fri 17 Nov 2017 03:40:10 PM IST using RSA key ID 34D8786F
gpg: using PGP trust model
gpg: Good signature from "Dell Inc., PGRE 2012 (PG Release Engineering Build Group
2012) <PG_Release_Engineering@Dell.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4255 0ABD 1E80 D7C1 BC0B  AD85 1285 4914 34D8 786F
gpg: binary signature, digest algorithm SHA512
```

Ansible module security

For security guidelines for Ansible modules, see Module Best Practices. Any developer who wants to contribute to OMAM adhere to these guidelines, along with the UT and sanity requirements.

Certain settings in Ansible are adjustable through a configuration file (`ansible.cfg`). The stock configuration should be sufficient for most users, but there may be reasons you would want to change them. Paths where the configuration file is searched are listed in the reference documentation.

Ansible vault

Ansible Vault is a feature that allows users to encrypt values and data structures within the Ansible projects. This provides the ability to secure any sensitive data that is necessary to successfully run Ansible plays but should not be publicly visible, such as passwords or private keys. Ansible automatically decrypts vault-encrypted content at runtime when the key is provided. See Vault documentation for more details.