Dell EMC OpenManage Plug-in version 3.2.0 for Nagios Core

Security Configuration Guide

June 2022
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

Preface

Dell EMC OpenManage Plug-in version 3.2.0 for Nagios Core provides capabilities for Out-of-Band (Agent-Free) management of iDRAC based PowerEdge Servers, Modular Infrastructure, Hyper-Converged Infrastructure (HCI), Datacenter Scalable Solutions(DSS), Storage and Networking devices. This plug-in provides complete hardware-level visibility including detailed inventory, health status (both overall and component-level health status) and SNMP trap monitoring for supported devices. PowerEdge servers are monitored using the Redfish based REST APIs, WS-Man APIs and SNMP protocol supported by iDRAC with Lifecycle Controller. Modular infrastructure are monitored using the REST APIs, WS-Man and SNMP protocol supported by OpenManage Enterprise-Modular (for MX7000 chassis) and Chassis Management Controller (for M1000e, VRTX and FX2/FX2s). REST APIs and SNMP are supported for monitoring the storage devices whereas networking devices are monitoring using SNMP. One-to-One web console launch of the respective element managers for iDRAC, Modular Infrastructure, Storage and Network devices is also supported by the OpenManage Plug-in to perform further troubleshooting, configuration and management activities.

As part of an effort to improve its product lines, Dell 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 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. For more information on the latest document, see support/dell.com.

Topics:

Scope of the document

This document includes information about the security features and capabilities.

Document references

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

- Dell EMC OpenManage Plug-in for Nagios Installation Guide
- Dell EMC OpenManage Plug-in for Nagios User's Guide.
- Dell EMC OpenManage Plug-in for Nagios Release Notes.

Security Quick Reference

Topics:

Deployment Model

Dell EMC OpenManage Plug-in version 3.2.0 for Nagios Core will have a release in the dell support site which includes new features, updates, and security fixes. For more information on installation procedures, see Installation Guide at support site

Security Profiles

Dell EMC OpenManage Plug-in version 3.2.0 for Nagios Core has a default security profile for secure HTTPS access.

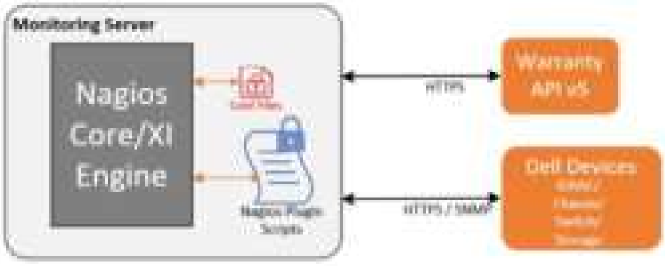
Product and Subsystem Security

Topics:

Security controls map

Dell EMC OpenManage Plug-in version 3.2.0 for Nagios Core uses python scripts to discover and monitor the iDRAC .

The system credentials are saved in object files using AES encryption with a user defined key.



Authentication

Access control settings provide protection of resources against unauthorized access. Dell EMC OpenManage Plug-in version 3.2.0 for Nagios Core does not have any access control system of its own. It is dependent on the Nagios Core and iDRAC.

For more information https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/cgiauth.html

Authentication with external systems

The Dell EMC OpenManage Plug-in version 3.2.0 for Nagios Core modules communicate with iDRAC, Chassis, and Network Switches. Dell EMC OpenManage Plug-in version 3.2.0 for Nagios Core supports session-based authentication for REST calls.

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

- Initiating a login session by accessing a create session URI. The response made to the request includes X-Auth-Token header along with session token. Using the X-Auth-Token header, authentication are made for the subsequent requests.
- Performing a session logout by providing **DELETE** to the session resource which is given by the login operation includes 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.

Dell EMC OpenManage Plug-in version 3.2.0 for Nagios Core communicates with iDRAC using SNMP, WSMan, and REST. Dell EMC OpenManage Plug-in version 3.2.0 for Nagios Core supports session-based authentication for iDRAC REST calls over HTTPS.

Chassis Authentication

Dell EMC OpenManage Plug-in version 3.2.0 for Nagios Core communicates with chassis using WSMan and REST and supports session-based authentication for Chassis REST calls over HTTPS in version 3.2.0. In addition, it supports both session-based and basic authentication for OpenManage Enterprise over HTTPS.

Network Authentication

Dell EMC OpenManage Plug-in version 3.2.0 for Nagios Core communicates with network switches using SNMP.

Data security

Dell EMC OpenManage Plug-in version 3.2.0 for Nagios Core does not store data as per Nagios Core standards, and credentials are stored in AES encrypted format based on the user-defined key. Refer Installation guide on how to configure the key for encryption.

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

Dell EMC OpenManage Plug-in version 3.2.0 for Nagios Core does a security patches as applicable.

Network security

Dell EMC OpenManage Plug-in version 3.2.0 for Nagios Core uses HTTPS with a default security profile to communicate with iDRAC, chassis, and Network Switches. This release does not support SSL certificate validation.

Auditing and logging

Dell EMC OpenManage Plug-in version 3.2.0 for Nagios Core logs the steps in the user provided location and level. No sensitive data is being logged into the log.

4

Miscellaneous configuration and management

Topics:

Protect authenticity and integrity

To ensure the product integrity, the Dell EMC OpenManage Plug-in version 3.2.0 for Nagios installation package is signed and uploaded to https://www.dell.com/support.

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
```