

Telemetry Streaming with iDRAC9 – Metric Reports Using Rsyslog

Abstract

Dell EMC PowerEdge Servers with iDRAC9 4.x Datacenter streams data to help IT administrators better understand the inner workings of their server environment. This white paper explains the process of configuring iDRAC9 to stream telemetry reports using Rsyslog. This paper also covers configurations that are required at server side to receive and process the reports.

April 2020

Revisions

Date	Description
April 2020	Initial release

Acknowledgments

Authors: Sankunny Jayaprasad, Aaron Colichia, Sankara Gara, Cyril Jose, Sailaja Mahendrakar

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2020 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [6/9/2020] [White Paper] [Document ID: 362]

Table of contents

1	Telemetry Overview	5
2	Streaming reports over RSyslogs.....	6
3	Streaming reports over RSyslog with TLS	8
4	Generating metric reports from rsyslog files	10
A	Technical support and resources	11

Executive summary

Beginning with iDRAC9 v4.00.00.00 firmware and a Datacenter license, IT managers can integrate advanced server hardware operation telemetry into their existing analytics solutions. Telemetry is provided as granular, timeseries data that is streamed, or pushed, compared to inefficient, legacy polling, or pulled, methods. The advanced agent-free architecture in iDRAC9 provides over 180 data metrics that are related to server and peripherals operations. Metrics are precisely timestamped and internally buffered to allow highly efficient data stream collection and processing with minimal network loading. This comprehensive telemetry can be fed into analytics tools to predict failure events, optimize server operation, and enhance cyber resiliency.

Customers can configure the integrated Dell Remote Access Controller (iDRAC) to be streamed using Redfish event listener, SSE Server-Sent Events (SSE) or using Remote Syslog (Rsyslog.) Most applications and analytic engines support the syslog protocol. Sending the Telemetry reports using syslog protocol allows a wide range of existing applications and analytical engines to consume and process these reports. This white paper provides information about configuring iDRAC to stream iDRAC Telemetry reports for Dell EMC PowerEdge Servers over Rsyslog.

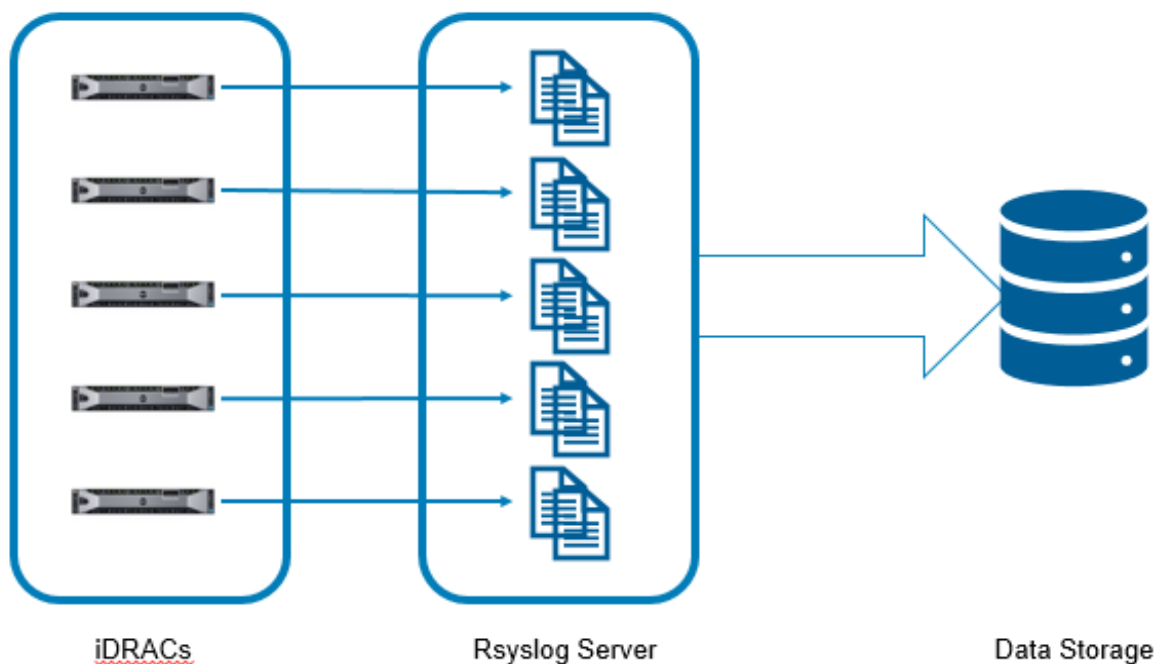


Figure 1 – Overview of infrastructure setup to stream iDRAC Telemetry streaming over Rsyslog

1 Telemetry Overview

Telemetry enables users to collect metric and data logs from various devices on PowerEdge server. Also, it provides streaming the data to the subscribed external client or server application. Using telemetry, it is possible to set types of reports and the frequency of reports that must be generated.

1.1 Prerequisites

- The Telemetry feature is available on iDRAC9 firmware version 4.00.00.00 or above and requires a Datacenter license.
- Rsyslog server for receiving reports available-

2 Streaming reports over Rsyslog

iDRAC can stream telemetry reports to Rsyslog servers that require an SSL certificate, and ones that do not require an SSL certificate. The streaming is either event or schedule based. On-demand streaming over Rsyslog is not supported.

2.1 iDRAC Configurations

There are few configuration changes that must be applied at iDRAC side to enable the telemetry streaming over Rsyslog.

2.1.1 Enable and set configurations

There are a few different ways to set the following parameters. One is the Dell EMC Command Line Interface (CLI) known as RACADM. Another tool is the RESTful API Redfish. A powerful and flexible tool is the Server Configuration Profile (SCP) which can be used to set any and every configuration option for a server. An SCP can include (but not limited to) BIOS, iDRAC, NIC, PERC, alerts, users, and all the Telemetry Streaming settings.

Ensure that below steps are completed using RACADM/Redfish/SCP.

1. Enable 'Telemetry Data Stream'
2. Set Rsyslog Server IPs and port

Sample RACADM commands to Enable and set Rsyslog configurations.

```
racadm>>set idrac.telemetry.EnableTelemetry Enabled
[Key=idrac.Embedded.1#Telemetry.1]
Object value modified successfully
```

Setting rsyslog Server1 IP

```
set idrac.telemetry.RSyslogServer1 10.100.100.11
[Key=idrac.Embedded.1#Telemetry.1]
Object value modified successfully
```

Setting rsyslog Server1 Port

```
racadm>>set idrac.telemetry.RSyslogServer1Port 514
[Key=idrac.Embedded.1#Telemetry.1]
Object value modified successfully
```

Sample SCP snippet

```
<SystemConfiguration>
<Component FQDD="iDRAC.Embedded.1">
  <Attribute Name="Telemetry.1#EnableTelemetry">Enabled</Attribute>
  <Attribute Name="Telemetry.1#RSyslogServer1">10.100.100.11</Attribute>
  <Attribute Name="Telemetry.1#RSyslogServer1Port">514</Attribute>
  <Attribute Name="Telemetry.1#RSyslogServer2">100.65.84.123</Attribute>
  <Attribute Name="Telemetry.1#RSyslogServer2Port">514</Attribute>
</Component>
```

```
</SystemConfiguration>
```

2.1.2 Viewing Rsyslog related configurations

To view and verify that the settings applied using above commands, use RACADM 'get' command.

```
racadm>>get idrac.telemetry
[Key=idrac.Embedded.1#Telemetry.1]
EnableTelemetry=Enabled
RSyslogServer1=10.100.100.11
RSyslogServer1Port=514
RSyslogServer2=100.65.84.123
RSyslogServer2Port=514
```

2.2 Rsyslog server-side Configurations

Instructions for installation and configuration of Rsyslog server are not in the scope of this document. For more information, see the documentation for the system operating system

The syslog protocol has a message size limitation for the efficient queuing and delivery of the messages. Telemetry reports can be larger than 100 K based on the report interval configuration. Hence the MaxMessageSize at server side must be raised to a value greater than or equal to 32 K.

Here is sample Rsyslog.conf file snippet from 'Ubuntu-18.04'.

```
# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
$MaxMessageSize 32k
$template remote-incoming-logs, "/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
```

2.3 Testing Rsyslog configuration

```
# racadm -r 192.168.1.2 -u root -p calvin --nocertwarn testrsyslogconnection
```

```
TELEMETRY0100: A test message was sent to the configured rsyslog server(s).
To check, perform a manual verification of the message on the required server(s)
```

On the server, verify that the test message is received, here is a sample message.

```
number cat 100.65.99.127.log

2019-12-19T13:18:50.058962-06:00 192.168.1.1 idrac-SVCTAG: Testing Rsyslog
Connection...
```

If there are multiple rsyslog servers that are configured to receive the reports from iDRAC, all the servers are expected to receive the message.

3.1.2 Viewing rsyslog CA certificate using RACADM

```
# racadm -r 192.168.1.2 -u root -p calvin --nocertwarn sslcertview -t 8 -i 1

Serial Number           : 5D83A7A11856C555
Subject Information:
Common Name (CN)       : example.delllabs.net
Issuer Information:
Common Name (CN)       : example.delllabs.net
Valid From              : Sep 19 16:06:59 2019 GMT
Valid To                : Sep 16 16:07:02 2029 GMT
```

3.1.3 Deleting rsyslog CA certificate using RACADM

Use the following sample command to delete the CA certificate if any reason for deletion arises.

```
# racadm -r 192.168.1.2 -u root -p calvin --nocertwarn sslcertdelete -t 8 -i 1

RSYSLOG303: The telemetry Rsyslog Server CA certificate is successfully deleted.
```

3.2 Example rsyslog server configuration for TLS

```
/etc/rsyslog.d/tls.conf:
$ModLoad imtcp
# make gtls driver the default
$DefaultNetstreamDriver gtls

# certificate files
$DefaultNetstreamDriverCAFile /etc/rsyslog-keys/ca.pem
$DefaultNetstreamDriverCertFile /etc/rsyslog-keys/telemetry3-cert.pem
$DefaultNetstreamDriverKeyFile /etc/rsyslog-keys/telemetry3-key.pem
$ModLoad imtcp # TCP listener
$InputTCPStreamDriverMode 1 # run driver in TLS-only mode
$InputTCPStreamDriverAuthMode anon
$InputTCPStreamRun 6514 # start up listener at port 10514
$template DynamicFile, "/var/log/loghost/%HOSTNAME%.log"
*. * -?DynamicFile
```

4 Generating metric reports from Rsyslog files

iDRAC telemetry reports are streamed as message chunks in order to overcome the syslog message size limitation. The chunks include metadata at the beginning so that the messages can be reassembled to form the complete message. The message can be assembled based on metadata consisting of *Message SeqNo*, *Total chunks*, and *Chunk Number*. A sample aggregation python script is available in the GitHub. www.github.com/dell

A Technical support and resources

iDRAC Telemetry Workflow examples

<https://github.com/dell/iDRAC-Telemetry-Scripting/>

Open-source iDRAC REST API with Redfish Python and PowerShell examples.

<https://github.com/dell/iDRAC-Redfish-Scripting>

The iDRAC support home page provides access to product documents, technical white papers, how-to videos, and more.

www.dell.com/support/idrac

iDRAC User Guide and other manuals

www.dell.com/idracmanuals

Dell Technical Support

www.Dell.com/support