Diode Collector Installation Guide

FortiSIEM 6.7.1

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

02/13/2023
FortiSIEM 6.7.1 Diode Collector Installation Guide

TABLE OF CONTENTS

Change Log 4
Diode Collector **5**
Feature 5
Standard Configuration 5
Additional Configurations 7
Example diode_collector.json File 7

Change Log

Date	Change Description
02/13/2023	Initial version of Diode Collector Installation Guide

Diode Collector

- Feature
- Standard Configuration
- Additional Configurations
- Example diode_collector.json File

Feature

The diode collector has the following functionalities:

1. Ability to install without Internet connectivity
2. Ability to work without registering with Supervisor node
3. Ability to collect syslog, SNMP trap and Windows log via WMI/OMI protocol using local configuration
4. Ability to send events to another Collector or Worker via UDP/514 using syslog protocol

A diode collector only requires a strictly one-way communication from itself to another Collector or Worker. There are two deployment modes:

1. Diode Collector -> Worker
2. Diode Collector -> Regular Collector -> Worker

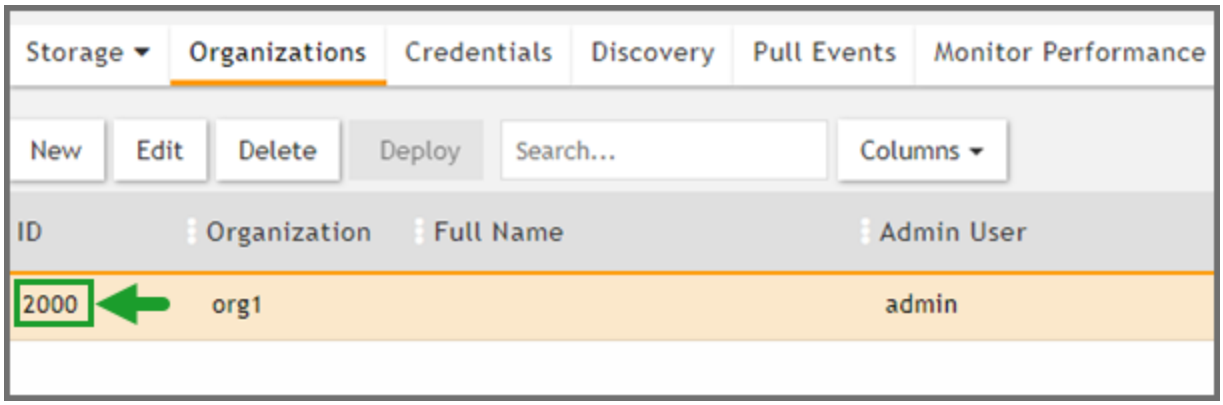
The regular Collector can send events to Worker via HTTPS.

Standard Configuration

To configure a diode collector, there are two general steps. Note that there is a Service Provide case (1) , and an Enterprise case (2), in Step 1.

Step 1: Collect Collector Information from Supervisor Node

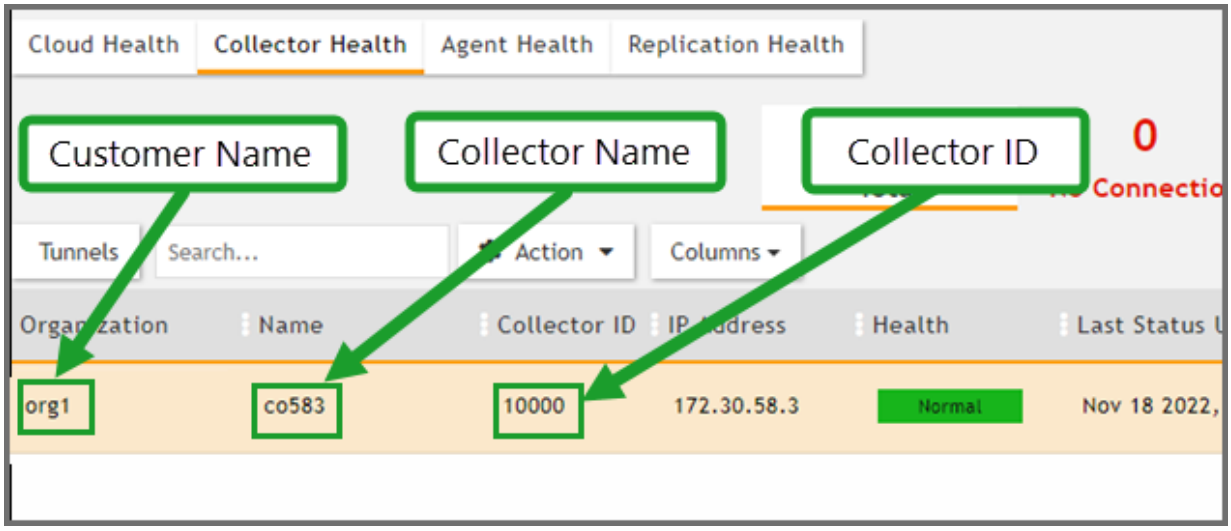
1. For Service Provider case, a Collector is associated with a customer.
   a. Navigate to **Admin > Setup > Organizations**.
   b. Click **New**, and create an Organization with the Collector.
   c. Get the **Customer Id**, which appears in the **ID** column. This should appear after the Organization is created.



d. Navigate to **ADMIN > Health > Collector Health**.

e. From the Collector Health page, get the following information:

- Customer Name (From the **Organization** column)
- Collector Name (From the **Name** column)
- Collector Id (From the **Collector ID** column)



2. For Enterprise case (1 Organization)

a. Navigate to **ADMIN > Setup > Collector**.

b. Click **New**, and create a Collector.

c. Navigate to **ADMIN > Health > Collector Health**.

d. From the Collector Health page, get the following information:

- Collector Id
- Collector Name

Step 2: Configure Collector Using the Information in Step 1

1. Download the collector binary from the Fortinet Support Site.
2. Run `configFSM.sh` on the VM (Internet connectivity not needed). Installation steps are provided here.
3. Modify the file `/opt/phoenix/config/diode_collector.json`. See Example diode_collector.json File for an example file.

a. Set **custId** to Customer Id from Step 1 (for Enterprise case, set to 1).
b. Set **collectorId** to Collector Id from Step 1.
c. Set **orgName** to Customer Name from Step 1 (for Enterprise case, set to super).
d. Set **collectorName** to Collector Name from Step 1.
e. Set **eventUploadServers** to the Worker in UDP:<IP1>:514,UDP<IP2:514> format where IP1 and IP2 are Worker IP addresses.
f. Set Windows Server credentials in the Credentials section.

4. Run the following command.

```
phProvisionDiodeCollector
```

Setup is now complete, and events should appear in the FortiSIEM GUI. There are no differences between events from a diode collector and a regular collector.

Additional Configurations

The following additional configurations are available.

- Adding Windows Servers or Changing WMI/OMI Credentials
- Change Parsers

Adding Windows Servers or Changing WMI/OMI Credentials

To add more Windows servers or change WMI/OMI credentials, take the following step.

1. Modify `/opt/phoenix/config/diode_collector.json`
   There is no need to restart any process.

Change Parsers

To Change Parsers, take the following steps.

1. Modify or create parser files under `/opt/phoenix/config/xml/`
2. Edit `/opt/phoenix/config/xml/parserOrder.csv`
3. Restart phParser by running the following command.

```
killall -9 phParser
```

Example diode_collector.json File

This JSON has 1 WMI example and 1 OMI example.

```
{
  "custId": 2000,
  "orgName": "org1",
  "collectorId": 10000,
  "collectorName": "CO1",
  "eventUploadServers": "UDP:192.168.1.100:514,UDP:192.168.1.101:514",
```

```
"eventUploadEpsLimit": 1000,
"creds": [
  {
    "custId": "2000",
    "accessIp": "1.2.3.4",
    "deviceType": {
      "vendor": "Microsoft",
      "model": "Windows",
      "version": "ANY"
    },
    "accessMethod": {
      "accessProtocol": "MS_WMI",
      "pullInterval": 1,
      "credential": {
        "username": "Administrator",
        "password": "12345678"
      },
      "template": {
        "name": "Get All Logs",
        "logTypes": [
          {
            "type": "SECURITY",
            "include": "", //blank means ALL
            "exclude": "" //blank means ALL
          },
          {
            "type": "APPLICATION",
            "include": "", //blank means ALL
            "exclude": "" //blank means ALL
          },
          {
            "type": "SYSTEM",
            "include": "", //blank means ALL
            "exclude": "" //blank means ALL
          }
        ]
      }
    }
  } ,
  {
    "custId": "2000",
    "accessIp": "1.2.3.4",
    "deviceType": {
      "vendor": "Microsoft",
      "model": "Windows",
      "version": "ANY"
    },
    "accessMethod": {
      "accessProtocol": "MS_OMI",
      "pullInterval": 1,
      "credential": {
        "username": "Administrator",
        "password": "12345678",
        "omiAuth": "ntlm or kerberos",
        "kerberosADServer": "1.2.3.4",
        "kerberosDomain": "abc"
```

```
          },
          "template": {
            "name": "Get All Logs",
            "logTypes": [
              {
                "type": "SECURITY",
                "include": "",
                "exclude": ""
              },
              {
                "type": "APPLICATION",
                "include": "",
                "exclude": ""
              },
              {
                "type": "SYSTEM",
                "include": "",
                "exclude": ""
              }
            ]
          }
        }
      }
    ]
  }
```

www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.