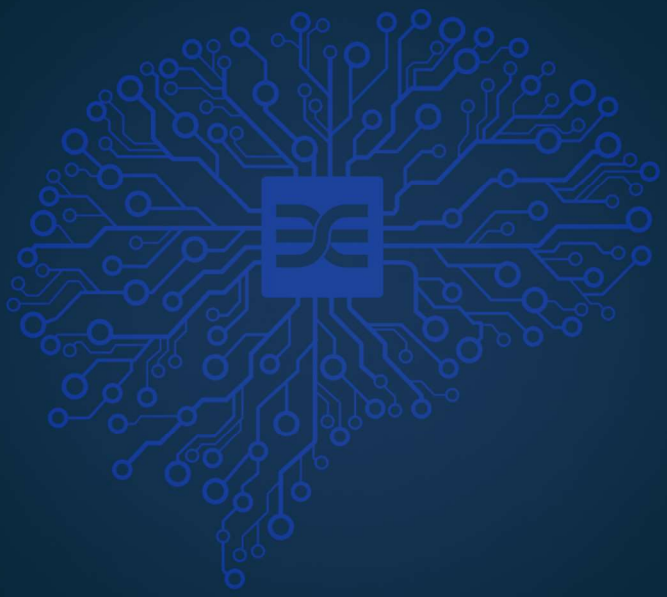
deep instinct
PREDICTIVE PREVENTION

Deep Instinct

DPS for NetApp



ONTAP Performance Analyzer

v 1.0.0

March 2024

Date: March 13, 2024

Author: Kevin Börner, Distinguished Sales Engineer, Deep Instinct
kevinb@deepinstinct.com

Contents

1. Introduction and intended use

Deep Instinct Prevention for Storage (DPS) is designed to safeguard storage repositories against sophisticated cyber threats, including ransomware, zero-day attacks, and both known and unknown malware. Utilizing Deep Instinct's deep learning framework, DPS offers proactive protection for data in Network Attached Storage (NAS) environments, as well as in hybrid and public cloud setups. By seamlessly integrating with existing storage infrastructure, including leading NAS vendors like Dell CAVA and NetApp Vscan, DPS ensures real-time scanning, detection, and prevention of malware, safeguarding the integrity and security of stored data. With its predictive prevention capabilities, DPS delivers unparalleled efficacy and accuracy, along with enterprise-grade scalability, effectively combating the latest cyber threats and maintaining the integrity of organizational data.

The assessment of performance and throughput when utilizing the DPS Scanner presents certain challenges. This document is designed to offer instructions on configuring ONTAP to generate detailed log output during file scanning via the DPS scanner. Additionally, it introduces a Python script designed for analysing the log file, thereby providing insights into throughput and performance metrics.

2. Instructions

2.1 Prerequisites

For the ONTAP Performance Analyser Script to analyse the performance of ONTAP logs we need to make sure that certain prerequisites are met before using it.

NetApp (VScan) integration requirements

If you have an existing NetApp (VScan) environment, make sure you meet the following requirements:

- VScan Server(s) (Windows Scanning Servers) should comply with Deep Instinct system requirements.
- Supported NetApp Data ONTAP operating system versions: v9.8 to v9.13
- ONTAP AV connector (avshim) installed and configured on the VScan Server — required for integrating with third-party antivirus software
- .NET (Microsoft's .NET Framework) and SMB (Server Message Block) v2.0 (and higher) must be installed
- Deep Instinct DPS Agent installed, and flow tested with EICAR file (see below for further steps) **OR any third-party AV agent where the performance needs to be evaluated**
  For further information on how to install the DPS Agent, please refer to the Deep Instinct Prevention for Storage Deployment Guide
- Latest python release installed (https://www.python.org/downloads/) for the script to run

Further information on how to configure the NetApp ONTAP connector can be found in the NetApp Knowledgebase: https://docs.netapp.com/us-en/ontap/antivirus/index.html

For ease of use, we perform all the provided instructions on the AV scanning server.

2.1.1 EICAR test for validating the Storage Agent operation

After installing the DPS agent on Windows (or any other third-party AV for storage), it is recommended to test that the software was correctly installed. A safe way to test the Storage Agent is by simulating a virus on the device. To simulate a virus, use the test file from the European Institute for Computer Antivirus Research (EICAR).
This file is **not** malicious but should be detected as malware when the Storage Agent has been installed successfully.

To acquire a test file

You can acquire an anti-malware test file by doing one of the following:

- ▪ Download a test file from the EICAR website

▪ Create a test file on the protected storage(NAS Storage), as follows:

1. Using a simple text editor, open a new file, and type or copy the following: *X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H**
2. Save the file (with any name). The file name is not relevant.

After downloading/creating the file, Deep Instinct will identify the test file as malicious, creating an event in the Management Console. This confirms that Storage Agent has been installed and is communicating with the Management Server.

2.2 Configuring ONTAP connector logs for performance testing

By default, the ONTAP AV connector does not provide any output when files are being send to the third-party AV scanner. For measuring the performance, we need to enable the trace output logs to gather further information.

To verify the operational flow via the ONTAP trace output (on VScan Server)

1. Access the Windows Registry editor:

    a. Press **Win + R** on our keyboard to open the Run dialog box.

    b. Type regedit and press Enter to open the Registry Editor.

2. Navigate to the following Registry Key path:

    64Bit OS: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0

    32Bit OS (less common): HKEY_LOCAL_MACHINE\SOFTWARE\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0

3. Right-click on the "v1.0" key in the left pane to add/modify parameters.

4. Add (if not existing) a TracePath string value where the trace output will be saved:

    a. Right click -> Select New -> String Value.

    b. Name the new string value 'TracePath'.

    c. Double-click on TracePath and set its value to the local log path where you want to save

the trace output. For example: C:\Logs\ontapavc_trace.log

5. Add/Modify the TraceLevel DWORD value:

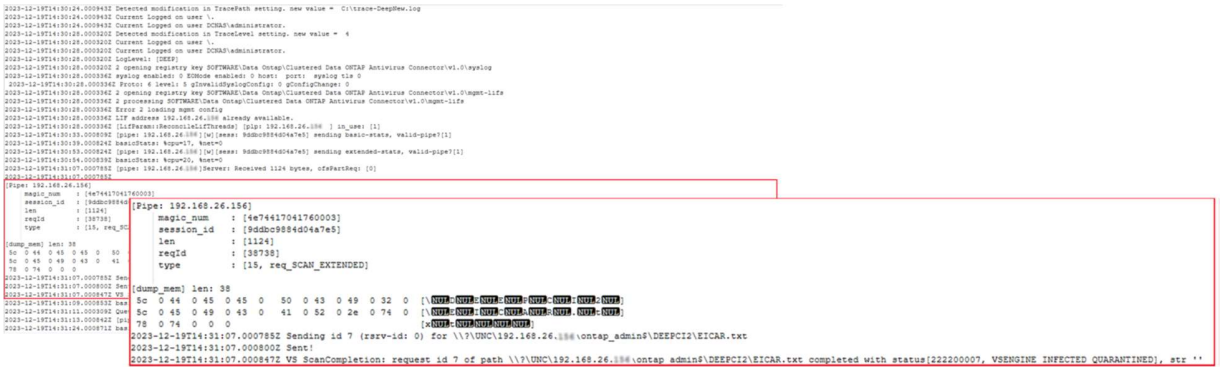
   a. Right click -> New -> DWORD (32-bit) Value.

   b. Name the DWORD value as 'TraceLevel'

   c. Double-click on TraceLevel and set its value data to '4' (DEEP). Level 4 (DEEP) is a debugging trace level that generates highly detailed and extensive log messages including scan requests and responses.

6. Upon closing the Registry Editor, the changes take effect immediately (no need for restart).

7. Verify the trace output is generated in the configured log path and includes information on the scan requests and responses.



ONTAP Log Example — Scan Request for EICAR File

IMPORTANT
The log file does not roll and will continue to grow, so once the trace output is verified, the NetApp suggestion is to set the TraceLevel value to '0' [QUIET] so no trace or log information is recorded.

2.3 Gather dataset and prepare for performance testing

For performance testing, it is important to use meaningful and realistic datasets. These datasets should reflect the common data types used within your NAS environment, such as Office files, PE files, and more. Generally, we recommend using a dataset ranging from 500 MB to 1.5 GB to obtain meaningful output and impose a certain load on the scanning servers. If circumstances allow, real malware can also be incorporated into these datasets.

Please note that real malware poses a severe risk within your environment. It should only be used when you can ensure the use of a controlled and isolated network and lab environment for the tests. If you cannot ensure the above, please use benign data instead.

A typical dataset for testing could consist of the following, as an example:

- 500 Office files with an average size of 5 MB
- 100 PE files with an average size of 10 MB
- 50 ZIP archives with an average size of 10 MB
- You may set up a dataset of your own liking as well of course

When you have found a fitting dataset please make note of the overall size of the dataset (for example 1479.3 MB).

Double check if the ONTAP trace logs are enabled (see 2.2 Configuring ONTAP connector logs)

2.4 Copy dataset to storage

After ensuring that all prerequisites are met and the dataset is ready, copy the dataset to the configured protected storage. Allow the VScan Server to complete the scans and the ONTAP connector to write the output into the configured trace logs. Depending on the size of the dataset, this process could take from several seconds to several minutes to complete.

2.5 ONTAP performance analyser script

Now that the copy and scan process is complete, the ONTAP performance analyser script can be used to calculate the scan time per file, the average scan time for all files, the time it took to complete the scan of the dataset as well as the throughput. All information can additionally be written into an output log to save and compare several logs for several AV scanners for example.

2.5.1 How to use the script

The helper script can be downloaded within this GitHub:
https://github.com/Boerner1337/DI-helper-scripts
See DI_ONTAP_LOG_ANALYZER.py script.

The script offers several arguments to control its output. Below, the supported arguments along with examples can be found.

The script is executed via Python (for example over PowerShell) using the following parameters:

```
PS C:\ONTAP_logs> python .\DI_ONTAP_LOG_ANALYZER.py -p “logfilename.log”
```

Supported parameters

Parameter	Explanation	Example
-p, --path	Path to log file	-p “C:\Folder\tracelog.log”
-l, --log	Path to output csv	-l “C:\log\putput.csv”
-size, --dataset_size	Dataset in MB for throughput calculation	-size 1348.9 -size 50
-v, --verbose	Increase output verbosity	-v

Example usage:

```
PS C:\Users\Downloads> python .\DI_ONTAP_LOG_ANALYZER.py -p
"C:\Users\Downloads\5MB-Office.log" -size 1479
```

For a log called 5MB-Office.log and a dataset size of 1479 MB.
The output of the script should look like this:

Note the total average scan time, total processing time for all files and throughput numbers calculated.

To compare the performance of several third-party AV storage scanners for ONTAP, repeat for the remaining storage scanners using the same dataset.

3 Closing words

As third-party AV scanners for ONTAP use different measuring metrics, and sometimes these metrics are even built into the products, it becomes challenging to objectively compare their performance to one another. This script, utilizing the ONTAP trace collector logs, should provide the most objective possibility, as the numbers come directly from the ONTAP connector and are not influenced by the third-party AV vendor.

The configurations, the performance test, and the script are part of an evaluation process and are not intended for continuous operation.

The script does not come with official support if it is later used in production.