Deep Discovery Analyzer (DDAN) 1100 & 1000 appliance Sizing Guide with firmware version 5.5 Service Pack 1

Confidential/Internal Only

By: Jowell Lim
August, 2016

Chapter 1: Introduction

This chapter provides an overview of the product functionalities and enhancements introduced in its latest release. The following topics are covered:

- Product Overview
- Key Features
- Supported Sandboxes Operating System

Product Overview

Deep Discovery Analyzer (DDAN) is a scalable custom sandbox analysis server that enhances the targeted attack protection of Trend Micro and third-party security products. Deep Discovery Analyzer supports out-of-the-box integration with Trend Micro email and web security products, and can also be used to augment or centralize the sandbox analysis of other Deep Discovery products. It allows you to define multiple, custom sandboxes—virtual environments that precisely match your desktop software configurations. It also provides a Web Services API to allow integration with any product, and a manual submission feature for threat research. Its custom sandboxing environments precisely match target desktop software configurations—resulting in more accurate detections and fewer false positives.

DDAN 1100 appliance utilizes DDAN 5.5 SP1 firmware version.

Key Features

Here are key features of Deep Discovery Analyzer 5.5 SP1:

- Deep Discovery Director Support
- Simple Network Management Protocol (SNMP) Support
  - Deep Discovery Analyzer sends SNMP trap messages to notify administrators about events that require attention, and listens to SNMP manager requests for system information, status updates, and configuration.
- Smart Protection Server Integration
  - Deep Discovery Analyzer integrates with Smart Protection Server for web reputation data, and can also use the Smart Protection Server to connect to global services.
- Enhanced Syslog Integration
  - Deep Discovery Analyzer now allows the customization of logs by selecting the scope and exclusions, and provides the option of sending logs to the syslog server using the SSL protocol.
- Threat Types Widget
  - The Threat Types widget shows the type, amount, and risk level of threats detected in all submissions.
- Improved Detection
  - Deep Discovery Analyzer provides increased protection by improving its detection capabilities. This release supports the deployment of sandbox images running Windows 10 operating system.
- Network Services Diagnostics
  - Deep Discovery Analyzer provides the option of testing the connectivity of local and global services.
- Inline Migration From Deep Discovery Analyzer 5.1 and 5.5
  - Deep Discovery Analyzer provides users with the option of automatically migrating the settings from 5.1 and 5.5 to 5.5 SP1 using the Firmware screen of the management console.

- Improved Usability
    - Deep Discovery Analyzer provides improved usability by rearranging several configuration screens, including Cluster and High Availability, and by introducing a new Integrated Products and Services section, which contains the Log Settings, Smart Protection, and Deep Discovery Director screens.

Supported Sandboxes Operating System

DDAN allows the user to create customize sandboxes. It is highly recommended to create the virtual machine image that is identical to a typical workstation in your environment. This provides added value since the malware would be executed that matches the customer's real environment.

Below are the supported virtual images operating systems:

- Windows XP (both 32-bit and 64-bit platform)
- Windows 2003 (both 32-bit and 64-bit platform)
- Windows 7 (both 32-bit and 64-bit platform)
- Windows 8 (both 32-bit and 64-bit platform)
- Windows 2008 (both 32-bit and 64-bit platform)
- Windows 10 (both 32-bit and 64-bit platform) – introduced in DDAN 5.5 SP1
    - Windows 10 Redstone 1 (aka Windows 10 Anniversary update) is not yet supported
- Windows 2012 or 2012 R2 (64-bit platform) – a DDAN 5.5 SP1 HF will be released on mid-Sept 2016 to support win2012

NOTE: DDAN allows a maximum of 3 windows virtual images. Each windows virtual image can have several sandbox instances. However, the total number of sandbox instances should not exceed 60 for DDAN 1100 and 33 sandbox instances for DDAN 1000.

Starting with DDAN 5.5, it supports installation of MS Office 2013 in the virtual image.

For MAC Cloud Sandboxing, it utilizes MAC OS 10.9.

Chapter 2: Trend Micro Products Integrated with DDAN

This chapter discusses what Trend Micro products can be integrated with DDAN. The following topics are covered:

- Samples sent to DDAN for analysis
- DDAN supported File Types

Samples Sent to DDAN for Analysis

The table below explains what types of samples are being sent to DDAN for analysis by different Trend Micro products.

Trend Micro Product	What samples are being sent to DDAN
IMSVA 8.2 SP1 - 8.5	Detected by Advance Threat Scan Engine (ATSE) as suspicious. Suspicious detections have a malware prefix of HEUR_ or EXPL_. Other detections won't be submitted to DDAN for analysis.

IMSVA 8.2 SP2 or later	Detected by ATSE as suspicious. Suspicious detections have a malware prefix of HEUR_ or EXPL_. Administrator have an option to submit files by true file type (i.e. Executable, Document, Image, Media, Compressed Files)
IMSS 7.5 or later	Detected by ATSE as suspicious. Suspicious detections have a malware prefix of HEUR_ or EXPL_. Other detections won't be submitted to DDAN for analysis.
IWSVA 6.0 or later	Detected by ATSE as suspicious. Suspicious detections have a malware prefix of HEUR_ or EXPL_. Can configure certain file types should always be submitted to DDAN.
IWSS 6.5 or later	Detected by ATSE as suspicious. Suspicious detections have a malware prefix of HEUR_ or EXPL_. Can configure certain file types should always be submitted to DDAN.
SMEX 11 or later	Detected by ATSE as suspicious. Suspicious detections have a malware prefix of HEUR_ or EXPL_. Can configure certain file types should always be submitted to DDAN.
SMID 5.6 or later	Detected by ATSE as suspicious. Suspicious detections have a malware prefix of HEUR_ or EXPL_. Other detections won't be submitted to DDAN for analysis.
DDI 3.7 or later	Configurable based on any of the following criteria: Detection Type, Protocol, File Type, File Extension, File Size, Direction or Source/Destination IP.
TMES 1.6	If the behavior matches the attack discovery rules. Will not submit files to DDAN if any of the following is met: 1. Files larger than 10MB 2. File from good company list 3. Files submitted before

DDAN Supported File Types

DDAN supports the analysis of the following file types:
Cell, Chm, Class, Dll, Doc, Docx, Exe, Gul, Hta, Hwp, Hwpx, Jar, Js, Jse, Jtd, Lnk, Mov, Pdf, Ppt, Ps1, Rtf, Swf, Vbs, Vbe, Xls, Xlsx, Xml, Wsf

Chapter 3: Sizing

This chapter discusses the DDAN 5.5 SP1 performance based on different setup. The following topics are covered:

- Success Criteria
- Factors affecting DDAN Performance
- Breakdown of File Types used in Testing
- Single DDAN 1100 / 1000 appliance file performance test result using DDAN 5.5 / 5.5 SP1
- Windows 10 performance
- DDAN 1100 and windows 10 (1 image only)
- DDAN with 3 images including windows 10

Success Criteria

The following DDAN performance test criteria were used:

- Average CPU usage: below 80%
- Average memory usage: below 80%
- Average Disk I/O usage: below 80%

Factors affecting DDAN Performance

Below are some factors that may affect DDAN performance:

- Number of Trend Micro products that send samples to DDAN
- Number of samples that are manually submitted to DDAN for analysis
- Number of files in an compressed file
- OS of the virtual machine image
- Number of Virtual images
- Number of sandbox instances
- Types of files being analyzed. For example, a PDF file may take longer to analyze because it has to be analyzed by 3 different versions of PDF reader.
- Complexity of the malware behavior. For example, some malware sample may drop more files or do a connection to C&C server. This will take longer time to analyze.
- If high availability is enabled, continuous data syncing between the active primary appliance and the passive primary appliance could impact active primary appliance's system resource usage and sandbox analysis capabilities.

Breakdown of File Types used in Testing

Below is the list of file types used during the test. There are a total of 7,510 samples.

- Compressed Macromedia Flash – 3,317
- MIME - 2,708
- Adobe Portable Document Format (PDF) - 560
- WIN32 EXE - 237
- Android Application Package (APK) - 125
- MS Cabinet - 111
- 7-ZIP - 106
- Macromedia Flash - 104
- MS Excel 95/97 - 43
- GNU ZIP - 37
- PKZIP - 35
- MS Office - 33
- MS Office 2007 Excel - 19
- Win32 DLL - 18
- AMD64 EXE - 13
- MS Office 2007 Word - 8
- MS Installer - 8
- ASCII text - 7
- UUENCODE - 5
- MS Office 2007 PowerPoint - 5
- AMD64 DLL - 4
- UPX EXE - 4

- DOS EXE - 2
- MS PowerPoint – 1

Out of the 7,510 samples used, below is the breakdown of samples categorized as compressed and non-compressed.

Compressed files	2,980
Non-compressed files	4,530

NOTE: These files types are categorized as compressed.

- 7-ZIP
- GNU ZIP
- MS Cabinet
- MIME
- Outlook Item (MSG)
- PKZIP
- UUENCODE

Single DDAN 1100 / 1000 Appliance File Performance Test Result using DDAN 5.5/5.5 SP1

Below is the test result using DDAN 1000 / 1100 with firmware version 5.5 vs 5.5 SP1. In summary, utilizing firmware DDAN 5.5 SP1, there's a 5% throughput drop on DDAN 1100 and 7% throughput drop on DDAN 1000.

DDAN 1100	DDAN 1100 using DDAN 5.5 33 Sandbox instances (XP, Win7, Win8)	DDAN 1100 using DDAN 5.5 SP1 33 Sandbox instances (XP, Win7, Win8)
Total processing time	11h 24m 33s	12h 2m 35s
Total number of samples	7510	7510
Throughput (samples/min)	10.98	10.40
Throughput (samples/hour)	658.8	624
Throughput (samples/day)	15811	14976
Average Processing time per sample per sandbox	2m 50s	2m 59s

DDAN 1000	DDAN 1000 using DDAN 5.5 33 Sandbox instances (XP, Win7, Win8)	DDAN 1000 using DDAN 5.5 SP1 33 Sandbox instances (XP, Win7, Win8)
Total processing time	22h 39m 36s	24h 27m 38s
Total number of samples	7510	7510
Throughput (samples/min)	5.53	5.12
Throughput (samples/hour)	331.8	307.2
Throughput (samples/day)	7963	7372
Average Processing time per sample per sandbox	3m 12s	3m 27s

Windows 10 Performance

In general, Windows 10 is significantly slower than previous OS. Here's a link from TechSpot (http://www.techspot.com/review/1042-windows-10-vs-windows-8-vs-windows-7/page3.html). In summary, here's what Trend recommends:

- For DDAN 1000 customers, it is highly recommended not to utilize windows 10 virtual image due to the fact that there will be ~40% performance degradation
- Windows 10 32 bit is slightly faster than windows 10 64 bit
- If windows 10 will be used, Trend recommends allocating at least an additional 30% sandbox instance for this OS. For example, if customer will utilize windows XP, 7 and 10. Here's the breakdown on the number of sandbox instance per platform.
    - Windows XP: 18
    - Windows 7: 18
    - Windows 10: 24

  Using the above as preliminary values, Trend recommends adjusting the instance number allocation according to the instance utilization percentage on Virtual Analyzer Status widget (under the dashboard page).
- If both Windows 10 32-bit and 64-bit are needed, Trend recommends allocating at least an additional of 30% sandbox instance for windows 10 32-bit and at least an additional 40% sandbox instance for windows 10 64-bit. Below is an example breakdown.
    - Windows 7: 16
    - Windows 10 32-bit: 21
    - Windows 10 64-bit: 23

  Using the above as preliminary values, Trend recommends adjusting the instance number allocation according to the instance utilization percentage on Virtual Analyzer Status widget (under the dashboard page).

DDAN 1100 and Windows 10 (1 image only)

With DDAN 1100 and DDAN 5.5 SP1, there is a throughput drop of 26% compared with windows 8 and 32% throughput drop compared with windows 7.

DDAN 1100	Windows 7	Windows 8	Win10 (32-bit)	Win10 (64-bit)
Total processing time	3h 54m 34s	4h 16m 28s	5h 23m 31s	5h 44m 4s
Total number of samples	7510	7510	7510	7510
Throughput (samples/min)	32.09	29.34	23.25	21.83
Throughput (samples/hour)	1925.4	1760.4	1395	1309.8
Throughput (samples/day)	46209	42249	33480	31435
Average Processing time per sample per sandbox	2m 41s	2m 57s	3m 46s	4m 2s

DDAN with 3 images including Windows 10

Comparing Windows XP+7+8 and Windows XP+7+10, there's a significant throughput drop of 40% on DDAN 1000 and 25% drop on DDAN 1100.

DDAN 1100	DDAN 5.5 SP1 (Win 7 32bit, Win8 32bit, Win10 64bit)
Total processing time	15h 58m 47s
Total number of samples	7510
Throughput (samples/min)	7.84
Throughput (samples/hour)	470.4
Throughput (samples/day)	11289

Average Processing time per sample per sandbox	4m

DDAN 1000	DDAN 5.5 SP1 (Win 7 32bit, Win8 32bit, Win10 64bit)
Total processing time	1d 16h 47m 08s
Total number of samples	7510
Throughput (samples/min)	3.07
Throughput (samples/hour)	184.2
Throughput (samples/day)	4421
Average Processing time per sample per sandbox	5m 48s