### TENABLE.AD

#### UPDATE PROCEDURE

1. **Document contributors:**

<table>
<thead>
<tr>
<th>Author</th>
<th>Qualification</th>
<th>Contact address</th>
</tr>
</thead>
<tbody>
<tr>
<td>TENABLE</td>
<td>DevOps team</td>
<td><a href="https://community.tenable.com/s/">https://community.tenable.com/s/</a></td>
</tr>
</tbody>
</table>

2. **Document history:**

<table>
<thead>
<tr>
<th>Version</th>
<th>Date (dd/mm/yyyy)</th>
<th>Author</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4.0</td>
<td>12/07/2019</td>
<td>ALSID</td>
<td>Initial document</td>
</tr>
<tr>
<td>2.5.0</td>
<td>23/10/2019</td>
<td>ALSID</td>
<td>Update for 2.5.0</td>
</tr>
<tr>
<td>2.5.3</td>
<td>16/12/2019</td>
<td>ALSID</td>
<td>Use InitDbSize</td>
</tr>
<tr>
<td>2.6.0</td>
<td>21/02/2020</td>
<td>ALSID</td>
<td>Update for 2.6.0</td>
</tr>
<tr>
<td>2.6.1</td>
<td>05/03/2020</td>
<td>ALSID</td>
<td>Update for 2.6.1</td>
</tr>
<tr>
<td>2.6.3</td>
<td>04/04/2020</td>
<td>ALSID</td>
<td>Update for 2.6.3</td>
</tr>
<tr>
<td>2.7.0</td>
<td>06/06/2020</td>
<td>ALSID</td>
<td>Update for 2.7.0</td>
</tr>
<tr>
<td>3.0.0</td>
<td>01/12/2020</td>
<td>TENABLE</td>
<td>Update for 3.0.0</td>
</tr>
<tr>
<td>3.1.0</td>
<td>02/08/2021</td>
<td>TENABLE</td>
<td>Update for 3.1.0</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

I. **Introduction** 3  
   1. Document objectives 3  
   2. Abbreviations 3  
   3. Infrastructure presentation 3  
   4. Required resources 8  

II. **Update procedure** 14  
   1. Update Directory Listener 14  
   2. Update Security Engine Nodes 16  
   3. Update Storage Manager 19  
   4. Restart machines 21  

III. **Active Directory configuration** 22  
   1. General considerations 22  
   2. Access to specific Active Directory objects or containers 23  
   3. Configuring the monitored infrastructure to support Tenable’s Indicator-of-Attack 23  

IV. **Annexes** 30  
   1. How to change IIS certificate for Tenable.ad Web Application 30  
   2. How to back up Storage Manager 35  
   3. Expert Mode for Directory Listener 36  
   4. Optional Sysmon configuration file 36
Introduction

1. Document objectives

This document is intended to help you perform a clean installation of Tenable’s on-premise solution. Each component comprises one server:

- A Directory Listener that targets audited domains
- A Security Engine Node that performs security analysis and serves the Web interface
- A Storage Manager that hosts all data based on MSSQL and InfluxDB.

Note: For many examples, we use the “E” partition letter by default for data partition.

2. Abbreviations

The following table lists the abbreviations used in this documentation:

<table>
<thead>
<tr>
<th>Abbr.</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DL / DLxx</td>
<td>Directory Listener</td>
</tr>
<tr>
<td>SEN / SENxx</td>
<td>Security Engine Node</td>
</tr>
<tr>
<td>DB / DBxx</td>
<td>Storage Manager</td>
</tr>
<tr>
<td>WI / WIxx</td>
<td>Web Interface, or any application offering a website</td>
</tr>
<tr>
<td>PC / PCxx</td>
<td>Personal Computer, or devices used as a computer</td>
</tr>
<tr>
<td>IoE / IoExx</td>
<td>Indicator of Exposure</td>
</tr>
<tr>
<td>DC / DCxx</td>
<td>Domain Controller</td>
</tr>
</tbody>
</table>

3. Infrastructure presentation

The following information is provided as a referral for this document. The infrastructure presented here must be considered as a supported architecture.

3.1. Network Overview

The network is spliced across three areas. The following schema shows an overview of the network communication:

![Figure 1: Network overview](image)
To go further, please read the following schema and its associated network matrix. They describe each required protocol and port used by Tenable’s platform:

Network flow matrix

The following network matrix describes each required protocol and port that the Tenable platform uses.

<table>
<thead>
<tr>
<th>Network flows (From -&gt; To)</th>
<th>Tenable’s usage</th>
<th>Type of traffic</th>
<th>Protocol and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>User and Computer Authentication, Forest Level Trusts</td>
<td>Kerberos</td>
<td>TCP/88, TCP/464 and UDP/464</td>
</tr>
</tbody>
</table>
In addition to the Active Directory protocols, some additional flows may be required depending on the configuration of the Tenable platform. These protocols and ports must be open between the Tenable platform and the targeted service.

<table>
<thead>
<tr>
<th>Network flows (From &lt;-&gt; To)</th>
<th>Tenable’s usage (optional)</th>
<th>Type of traffic</th>
<th>Protocol and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable Security engine nodes &lt;-&gt; Cybersecurity services</td>
<td>Tenable Web Application</td>
<td>HTTP/TLS</td>
<td>TCP/443</td>
</tr>
<tr>
<td></td>
<td>Email notifications</td>
<td>SMTP</td>
<td>TCP/25, TCP/587, TCP/465, TCP/2525, TCP/25025 (depending on the SMTP server’s configuration)</td>
</tr>
<tr>
<td></td>
<td>Syslog notifications</td>
<td>Syslog</td>
<td>TCP/601, TCP/6515, UDP/514 (depending on the event log server’s configuration)</td>
</tr>
<tr>
<td></td>
<td>Tenable REST API</td>
<td>HTTP/TLS</td>
<td>TCP/443</td>
</tr>
</tbody>
</table>
3.2. Preferred architectures

The application runs through many engines that are divided across multiple machines.

The power we need depends on the AD activity/traffic, which is hard to estimate before deployment. Most of the time, it can be correlated with the number of active users in the AD.

- Under 300,000 active users, we recommend using a three-servers architecture. Each server has one or more services, and each server must be considered as an independent entity.

- If there are more than 300,000 active users, they will overload these three servers and degrade performance. Hence, the Security Engine Node is split into four machines.
3.3. Meta-Kapteyn architecture (optional)

For example, consider a group which is in Europe and has a subsidiary in North America. They are not directly connected and there is no trust relationship between their Active Directory domains. You can use Meta-Kapteyn as a consolidation platform to display both dashboards of Europe and North America instances on a single page.

This feature is optional and is not required for the analysis.

Installation log file

If the installer cannot install Tenable.ad on a machine, you can forward the log file to our support.

This file is in your %tmp% folder, and its name always starts with "MSI" followed by random numbers, such as MSI65931.LOG.

4. Required resources

Tenable.ad is built upon three main categories of services:

- The directory listeners: receive real-time Active Directory flows.
- The security engine nodes: support the Tenable security engine, API services, and end-users.
- The storage managers: provide hot and cold storage support for the directory listeners and the security nodes services.

To ensure correct behavior, these components require a certain amount of memory and computing power.

These required resources scale depending on the size of the Active Directory infrastructures to monitor.

As a metric, Tenable uses the number of active users to compute the required sizing. It includes the regular user accounts and the service accounts used by applications.

You can compute the volume using the following command line, which you must run on every Active Directory domain to monitor.

PowerShell command line
Import-Module ActiveDirectory
(Get-ADUser -Server "dc.domain.com" -Filter 'enabled -eq $true').Count

- In this command, the parameter "-Server" must specify the Active Directory Domain Services instance to connect to.
- Replace the value "dc.domain.com" by the fully qualified domain name (FQDN) of the domain controller to use for counting.

After you collect the number of active users to monitor, the following sections define the appropriate sizing requirements.

4.1. Sizing for Directory Listeners

This table describes the required sizing for the system hosting the "Directory Listener" components.

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Instance required</th>
<th>vCPU (per instance)</th>
<th>Memory (per instance)</th>
<th>Disk space (per instance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – 25 000</td>
<td>1 Virtual Machine</td>
<td>2 cores on 2 sockets</td>
<td>12 GB of RAM</td>
<td>30 GB (silver performance)</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
<td>1 Virtual Machine</td>
<td>4 cores on 2 sockets</td>
<td>16 GB of RAM</td>
<td>30 GB (silver performance)</td>
</tr>
<tr>
<td>50 001 - 75 000</td>
<td>1 Virtual Machine</td>
<td>4 cores on 2 sockets</td>
<td>24 GB of RAM</td>
<td>30 GB (silver performance)</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
<td>1 Virtual Machine</td>
<td>4 cores on 2 sockets</td>
<td>32 GB of RAM</td>
<td>30 GB (silver performance)</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
<td>1 Virtual Machine</td>
<td>8 cores on 2 sockets</td>
<td>32 GB of RAM</td>
<td>30 GB (silver performance)</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
<td>1 Virtual Machine</td>
<td>8 cores on 2 sockets</td>
<td>64 GB of RAM</td>
<td>30 GB (silver performance)</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
<td>1 Virtual Machine</td>
<td>8 cores on 2 sockets</td>
<td>64 GB of RAM</td>
<td>30 GB (silver performance)</td>
</tr>
</tbody>
</table>

4.2 Sizing for the Security Engine Node

This table describes the required sizing for the system hosting the "Security Engine Node" components.

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Instance required</th>
<th>vCPU (per instance)</th>
<th>Memory (per instance)</th>
<th>Disk space (per instance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – 25 000</td>
<td>1 Virtual Machine</td>
<td>8 cores on 2 sockets</td>
<td>16 GB of RAM</td>
<td>200 GB (gold performance)</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
<td>1 Virtual Machine</td>
<td>8 cores on 2 sockets</td>
<td>16 GB of RAM</td>
<td>300 GB (gold performance)</td>
</tr>
<tr>
<td>50 001 - 75 000</td>
<td>1 Virtual Machine</td>
<td>10 cores on 3 sockets</td>
<td>24 GB of RAM</td>
<td>300 GB (gold performance)</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
<td>1 Virtual Machine</td>
<td>12 cores on 4 sockets</td>
<td>32 GB of RAM</td>
<td>400GB (gold performance)</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
<td>1 Virtual Machine</td>
<td>16 cores on 4 sockets</td>
<td>32 GB of RAM</td>
<td>400GB (gold performance)</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
<td>1 Virtual Machine</td>
<td>16 cores on 4 sockets</td>
<td>64 GB of RAM</td>
<td>500GB (gold performance)</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
<td>4 Virtual Machines</td>
<td>VM1: 8 cores on 2 sockets</td>
<td>VM1: 16 GB of RAM</td>
<td>VM2: 12 cores on 4 sockets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VM2: 12 cores on 4 sockets</td>
<td>VM2: 32 GB of RAM</td>
<td>VM3: 16 cores on 4 sockets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VM3: 16 cores on 4 sockets</td>
<td>VM3: 16 GB of RAM</td>
<td>VM4: 16 cores on 4 sockets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VM1: 1 TB</td>
<td>VM1: 1 TB</td>
<td>VM2: 300 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VM3: 100 GB</td>
<td>VM3: 100 GB</td>
<td>VM4: 100 GB</td>
</tr>
</tbody>
</table>
Sizing for the Storage Manager

As part of its security analysis, Tenable.ad needs to store the differences for each Active Directory change, whether this change comes from the Active Directory database or from the Sysvol network share. The Storage Manager component is in charge of storing these events in two databases: a Microsoft SQL Server instance and an InfluxDB instance.

To predict the number of AD changes (named events in the product) to store in Tenable’s database is a challenge as this number depends on the Active Directory activities, thus depends on the business activities of our customers. To cover both general and edge cases, this guide offers two configuration suggestions:

- a minimal sizing to start and run the platform in most infrastructures
- a recommended configuration that covers the needs of most of the event-intensive Active Directory infrastructures. Most platforms will not need that much disk space, so use the recommended values if you do not plan to monitor the platform closely and do not want to potentially grow disks in the future.

Dealing with databases also means implementing a specific disk layout to store the different database files and to ensure that I/O performances are compatible with the product’s activity.

This section also covers the recommended disk layout and storage performances for Tenable.ad. Due to the amount of Active Directory data processed by the product, Tenable.ad is a disk-intensive application. To avoid any bottleneck introduced by the storage (disk or SAN), this presents two disk performance scenarios. Just like the sizing, the minimal disk performance covers the needs of most infrastructures. The recommended infrastructure offers a better experience for large or very active AD infrastructures.
Minimal and Recommended Computing Power

### Storage managers – Minimal Computing Power Matrix

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Instance required</th>
<th>vCPU (per instance)</th>
<th>Memory (per instance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – 25 000</td>
<td>1 Virtual Machine</td>
<td>8 cores on 2 sockets</td>
<td>8 GB of RAM</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
<td>1 Virtual Machine</td>
<td>8 cores on 2 sockets</td>
<td>12 GB of RAM</td>
</tr>
<tr>
<td>50 001 - 75 000</td>
<td>1 Virtual Machine</td>
<td>12 cores on 4 sockets</td>
<td>16 GB of RAM</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
<td>1 Virtual Machine</td>
<td>12 cores on 4 sockets</td>
<td>16 GB of RAM</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
<td>1 Virtual Machine</td>
<td>12 cores on 4 sockets</td>
<td>32 GB of RAM</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
<td>1 Virtual Machine</td>
<td>16 cores on 4 sockets</td>
<td>64 GB of RAM</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
<td>1 Virtual Machine</td>
<td>16 cores on 4 sockets</td>
<td>64 GB of RAM</td>
</tr>
</tbody>
</table>

### Storage managers – Recommended Computing Power Matrix

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Instance required</th>
<th>vCPU (per instance)</th>
<th>Memory (per instance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – 25 000</td>
<td>1 Virtual Machine</td>
<td>8 cores on 2 sockets</td>
<td>8 GB of RAM</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
<td>1 Virtual Machine</td>
<td>8 cores on 2 sockets</td>
<td>16 GB of RAM</td>
</tr>
<tr>
<td>50 001 - 75 000</td>
<td>1 Virtual Machine</td>
<td>12 cores on 4 sockets</td>
<td>32 GB of RAM</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
<td>1 Virtual Machine</td>
<td>12 cores on 4 sockets</td>
<td>64 GB of RAM</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
<td>1 Virtual Machine</td>
<td>16 cores on 4 sockets</td>
<td>64 GB of RAM</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
<td>1 Virtual Machine</td>
<td>16 cores on 4 sockets</td>
<td>96 GB of RAM</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
<td>1 Virtual Machine</td>
<td>16 cores on 4 sockets</td>
<td>96 GB of RAM</td>
</tr>
</tbody>
</table>

### Supported and Recommended Disk Layout

Some specific environments require splitting the database files across different disks.

Since this type of configuration does not directly improve performance and requires manual actions during the deployment or upgrade phases, Tenable does not recommend using this configuration, even if it is supported.

- **Recommended Active Directory integration**
  - 1 disk to host Data, TempDB and Log files

- **Supported Active Directory integration**
  - 1 Data file disk
  - 1 TempDB disk
  - 1 Log file disk
  - (optional) 1 Backup disk
Minimal and Recommended Disk Sizing

The following tables describe the minimal and recommended disk sizing to store 6 months of Active Directory events within Tenable.AD.

### Storage managers – Minimal Disk Sizing Matrix

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Total Disk Space</th>
<th>Data File Disk Space</th>
<th>Log File Disk Space</th>
<th>TempDb Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – 25 000</td>
<td>450 GB</td>
<td>340 GB</td>
<td>100 GB</td>
<td>10 GB</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
<td>550 GB</td>
<td>400 GB</td>
<td>125 GB</td>
<td>25 GB</td>
</tr>
<tr>
<td>50 001 – 75 000</td>
<td>800 GB</td>
<td>600 GB</td>
<td>150 GB</td>
<td>50 GB</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
<td>1 TB</td>
<td>725 GB</td>
<td>200 GB</td>
<td>75 GB</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
<td>2 TB</td>
<td>1.6 TB</td>
<td>300 GB</td>
<td>100 GB</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
<td>3 TB</td>
<td>2.45 TB</td>
<td>400 GB</td>
<td>150 GB</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
<td>4 TB</td>
<td>3.3 TB</td>
<td>500 GB</td>
<td>200 GB</td>
</tr>
</tbody>
</table>

### Storage managers – Recommended Disk Sizing Matrix

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Total Disk Space</th>
<th>Data File Disk Space</th>
<th>Log File Disk Space</th>
<th>TempDb Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – 25 000</td>
<td>600 GB</td>
<td>375 GB</td>
<td>200 GB</td>
<td>25 GB</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
<td>800 GB</td>
<td>500 GB</td>
<td>250 GB</td>
<td>50 GB</td>
</tr>
<tr>
<td>50 001 – 75 000</td>
<td>1.2 TB</td>
<td>775 GB</td>
<td>350 GB</td>
<td>75 GB</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
<td>2 TB</td>
<td>1.3 TB</td>
<td>600 GB</td>
<td>100 GB</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
<td>4 TB</td>
<td>3 TB</td>
<td>800 GB</td>
<td>200 GB</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
<td>6 TB</td>
<td>4.7 TB</td>
<td>1 TB</td>
<td>300 GB</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
<td>8 TB</td>
<td>6.4 TB</td>
<td>1.2 TB</td>
<td>400 GB</td>
</tr>
</tbody>
</table>

Minimal and Recommended Disk Performance

The limiting factor of our database is usually the underlying disk performances. The better disk throughput/IOPS, the better overall performances of Tenable.ad will be. A low latency is also required (<5 ms).

Additional Notes

- The requirements described in the preceding tables are for the well-being of Tenable's platform, they do not take into consideration the operating system requirements in case of an application package-based deployment.
- CPU Speed should be at least 2.6 GHz.
- The "+" sign means that Tenable needs to assess the requirements on a case-by-case basis if the number of active users exceeds this metric.
- Tenable’s platform supports the x86-64 processor architecture, being at least Sandy Bridge or Piledriver architecture, with Intel Turbo Boost Technology 2.0.
- One network interface is required. Other network interfaces can be added as per client’s requests for administration, monitoring, or any other reason.
Example
An Information System made of three Active Directory domains has the following sizing:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Number of Active AD users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain A</td>
<td>45 000</td>
</tr>
<tr>
<td>Domain B</td>
<td>15 000</td>
</tr>
<tr>
<td>Domain C</td>
<td>150</td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td><strong>60 150</strong></td>
</tr>
</tbody>
</table>

Following the sizing matrix, the required resources will be as follows:

<table>
<thead>
<tr>
<th>Tenable services</th>
<th>Instance required</th>
<th>vCPU (per instance)</th>
<th>Memory (per instance)</th>
<th>Disk space (per instance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory listeners</td>
<td>1</td>
<td>4 cores, at least 2.6 GHz</td>
<td>12 GB of RAM</td>
<td>30 GB</td>
</tr>
<tr>
<td>Security Engine nodes</td>
<td>1</td>
<td>10 cores, at least 2.6 GHz</td>
<td>24 GB of RAM</td>
<td>300 GB</td>
</tr>
<tr>
<td>Storage managers</td>
<td>1</td>
<td>12 cores, at least 2.6 GHz</td>
<td>16 GB of RAM</td>
<td>1.2 TB with 10 000 IOPs</td>
</tr>
</tbody>
</table>

4.4. Additional support information

- Tenable.ad works with Windows Server 2016 with the latest available update.
- Tenable.ad installer requires Local Administrator rights on Windows Server 2016. If the account used for the installation is not the built-in one, make sure that this account can run programs without restrictions.
- Tenable.ad services require Local Administrator rights to run local services on the machine.
- Tenable.ad requires a dedicated data partition. Tenable.ad must not be run on the OS partition to prevent system freeze if the partition is full.
- Tenable.ad SQL instance requires the virtual accounts usage feature.
- Tenable.ad works on a three-tier model. One or two VMs are not supported. At least three VMs and eventually more than one DL are supported. **Exception:** Ceti-TLS mode requires only one VM from a customer point-of-view.
- Tenable.ad must be considered as a black-box: Each machine must be considered as dedicated to the product and must not be shared for another purpose.
- Tenable.ad can create any folder starting with ‘Alsid’ or ‘Tenable’ prefix on the data partition. Therefore, do not create folders starting with ‘Alsid’ nor ‘Tenable’ on the data partition.
- Erlang known issues: the HOMEDRIVE environment variable must not be modified. The PATHEXT environment variable must contain the .EXE and .BAT file extensions.
4.5. Installation Programs

Tenable.ad installer is available on Tenable’s release portal (https://www.tenable.com/downloads/).

This package contains the files required to perform installation/uninstallation/update and to reconfigure the solution with different IP addresses (if needed).

Deployment on Windows Server (Full-Desktop Experience)

You must place the installation program in a valid location on each server to set up.

In the following example, on the Storage Manager machine, we put it on the Desktop:

<table>
<thead>
<tr>
<th>Binaries location</th>
<th>Binaries content</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>C:\Users\Administrator\Desktop\</code></td>
<td><img src="image" alt="Desktop" /></td>
</tr>
</tbody>
</table>

- You can activate extended debug logging with the following command (replace the first path with your installation program location, and the second with your log file path):

  `"C:\Users\Administrator\Desktop\Tenable.ad_3.X.X.exe" /AI_DEBUGLOG=1 /L\*V "E:\example.log"`

Deployment on Windows Server Core

The installer GUI can be displayed on a Server Core. Type this command to start the installation:

- Run the following command (replace the path by your exe file location):

  `C:\Users\Administrator\Desktop\Tenable.ad_3.X.X.exe`
5. **UPDATE PROCEDURE**

1. **Backup your system**
   
   *Warning:* Tenable strongly advises you to make a backup of your databases and/or make a snapshot of your environment prior to the update procedure.

2. **Update Directory Listener**
   
   During this step, the process updates the following applications:
   
   - Tenable component
     - Ceti
   
   In a specific context, it can be useful to deploy more than one DL within the same infrastructure. For example, if two forests are registered in the solution but those two are on different networks because of legal restrictions, you can deploy one DL in the first subnet and another DL in the second subnet.

   **Expert Mode:**
   
   This configuration requires to check the “Expert mode” box on the first installer window to display advanced installation options. For more details, please refer to 3 Expert Mode for Directory Listener - page.

   The update mechanism is fully automated.

   1. Execute “tenable.ad_v3.X.X.exe” with full Local Administrator privileges and click on the “Next” button.

   ![Welcome dialog on Directory Listener](image)

   2. In the next dialog box, features and location are automatically preselected based on the previous installation. As mentioned previously, only the DirectoryListener feature must be selected. Click on the “Next” button.
3. The installation program automatically fills in RabbitMQ's IP address based on the previous version. You can check if this is consistent, then click on the "Next" button and update Tenable.AD.

4. At the end of the installation, WAIT until the server asks for a reboot. Do NOT reboot it now! Leave it like this for the moment and go to the next page. We will reboot it later.
3. Update Security Engine Nodes

During this step, the process updates the following applications:

- Tenable nodes
  - Cancri
  - Caroli
  - Cephei
  - Ceti-Bridge
  - Cygni
  - Electra
  - Enif
  - Equuleus
  - Eridanis
  - Kapteyn
  - IIS
  - RabbitMQ

The SEN machine can be split into different machines to improve performance on huge infrastructures.

2.1. One machine

The update mechanism is fully automated through an installer file.

1. To perform the update, execute "tenable.ad_v3.X.X.exe" with full Local Administrator privileges and click on the "Next" button.

2. On the next dialog, features and location are automatically preselected based on the previous installation. As mentioned before, here you can see that only the SecurityEngineNode feature must be selected. Click on the "Next" button.
3. All required fields are automatically filled based on the previous version. You can check if this is consistent, then click on the "Next" button.

4. The same thing applies to the next window. Then, click on the "Next" button and update Tenable.ad.
5. At the end of the installation, **WAIT** until the server asks for a reboot. **Do NOT reboot it now!** Leave it like this for the moment and go to the next page. We will reboot it **later**.

### 2.2. Multiple machines

Follow the instructions above, but in the following order on the machines which are running those services:

1. Cygni
2. Cancri
3. Caroli
4. Others (Eridanis, Kapteyn, etc.)
5. RabbitMQ

### 2.3. Meta-Kapteyn (optional)

To update Meta-Kapteyn, as it is just a component without data, please refer to appropriate Uninstall and Install guides.

1. Uninstall Meta-Kapteyn using the uninstall script for Security Engine Nodes (follow the uninstall procedure).
2. As asked by the script, reboot.
3. Install Meta-Kapteyn using the dedicated install script (follow the installation procedure).
4. **Update Storage Manager**

4.1. **Backup your system**

**Warning**: We strongly recommend that you **back up the Storage Manager and/or make a snapshot of your environment** prior to running the update procedure.

For a procedure to **back up the databases before running the update**, please refer to the section *How to back up Storage Manager*.

4.2. **Run the update procedure**

During this step, the process will update the following applications:

- InfluxDB (Tenable database)
- MSSQL (Tenable database)

The update mechanism is fully automated through an installer file. The update mechanism is fully automated.

1. Execute "tenable.ad_v3.X.X.exe" with full Local Administrator privileges and click on the "Next" button.

   ![Welcome dialog on Storage Manager](image)

   *Welcome dialog on Storage Manager*

2. In the next dialog box, features and location are automatically preselected based on the previous installation. As mentioned previously, here you can see that only the **StorageManager** feature must be selected. Click on the "Next" button.
3. All required fields are automatically filled based on the previous version. You can check if this is consistent, then click on the “Next” button and update Tenable.ad.

4. Wait for the end of the installation and click on YES to reboot the server.
5. **Restart machines**

5.1. **Start Security Engine Nodes services**

Databases must be running before starting SEN services. You can now restart the SEN machine by clicking on the "Yes" button.

![Reboot message after update message box on SEN](image)

If you have more than one SEN machine, please follow this reboot order:

1. RabbitMQ
2. Others (Eridanis, Kapteyn, etc.)
3. Cancri
4. Caroli
5. Cygni

5. **Start Directory Listeners services**

Databases and SEN must be running before starting DL services. So now the DL machine can be restarted by clicking on the "Yes" button.

![Reboot message after update message box on DL](image)
6. **Active Directory Configuration**

1. **General considerations**

Tenable.ad has been designed as a non-intrusive solution able to monitor a directory infrastructure without requiring the deployment of agents, and as little as possible configuration change in the customer’s environment.

Tenable uses a regular user account with no administrative right to connect to standard APIs for its security monitoring feature (also named Indicator-of-Exposure), which by nature prevents any side effect for the monitored infrastructure. This feature leverages the Active Directory replication mechanisms to retrieve the relevant information which incurs limited bandwidth costs only between each domain’s PDC and Tenable’s DirectoryListener, but no additional cost within the infrastructure.

To efficiently **detect security incidents through its Indicator-of-Attack feature**, Tenable additionally leverages the ETW information (often used by Windows event logs) and the replication mechanisms available on each Domain Controller. To collect this set of information, a dedicated Group Policy object will need to be deployed using a dedicated deployment tool available in Tenable’s console. This GPO will activate, on all domain controllers, a WMI filter which will write to the SYSVOL to profit from the AD replication engine and the ability of Tenable to listen to SYSVOL events. Files written by the WMI filter are removed as they are written as a rolling mechanism is in place, using another WMI filter, to avoid filling the SYSVOL.

To initiate security monitoring, Tenable.ad requires to contact standard directory APIs specified by Microsoft and documented in the MS-DRSR open specifications¹.

---

2. Access to specific Active Directory objects or containers

Tenable’s platform achieves its security monitoring without the need of administrative privileges. Despite its many advantages (operation safety, limited attack surface, etc.), this approach relies on the ability of the user account used by the platform to read all the Active Directory objects stored in a domain (including user accounts, organizational units, groups, etc.). This section only applies for the platform benefiting from the Indicator-of-Exposure module and only need to be applied if it has not been achieved during a previous product install.

By default, most of the objects natively benefit from a default read access for the group Domain Users used by Tenable’s service account. However, some containers need to be manually configured to allow read access to Tenable’s user account:

<table>
<thead>
<tr>
<th>Location of the container</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN=Deleted Objects,DC=&lt;DOMAIN&gt;,DC=&lt;TLD&gt;</td>
<td>Container hosting deleted objects</td>
</tr>
<tr>
<td>CN=Password Settings Container,CN=System, DC=&lt;DOMAIN&gt;,DC=&lt;TLD&gt;</td>
<td>[Optional] Container hosting Password Strategy Objects</td>
</tr>
</tbody>
</table>

For each of the above containers, Tenable requires to grant access to the service account used by the platform via the following command line:

<table>
<thead>
<tr>
<th>Command line</th>
</tr>
</thead>
<tbody>
<tr>
<td>dsacls &quot;&lt;<strong>CONTAINER</strong>&gt;&quot; /takeownership</td>
</tr>
<tr>
<td>dsacls &quot;&lt;<strong>CONTAINER</strong>&gt;&quot; /g &lt;<strong>SERVICE_ACCOUNT</strong>&gt;:LCRP /I:T</td>
</tr>
</tbody>
</table>

In the previous table, <__CONTAINER__> refers to the container to grant access to. <__SERVICE_ACCOUNT__> refers to the service account used by Tenable’s platform.

This command needs to be run on every domain monitored by Tenable’s platform.

3. Configuring the monitored infrastructure to support Tenable’s Indicator-of-Attack

This section only applies for the platform benefiting from the Indicator-of-attack module and needs to be applied after each platform upgrade.

Tenable’s platform provides real-time security incident detection thanks to correlating ETW information (generated by each domain controller) with LDAP and SYSVOL events. This section is focused on how to configure the monitored Domain Controllers to retrieve the required ETW information and to forward them to the Tenable.ad platform.

This section only applies for the platform benefiting from the Indicator-of-Attack module (IOA). It will first discuss Tenable’s deployment script, a PowerShell script used to deploy Windows-component requirements on the Domain Controllers. Secondly, this section will detail how to install Microsoft Sysmon, a Windows system tool needed by some of the Tenable’s IOA to get relevant system data. Finally, this section will cover how to uninstall or update Tenable’s deployment script. In the third section, the document describes potential issues with the audit policy.

3.1. Tenable’s deployment script

To retrieve the required ETW information within Tenable’s platform, a unique system based on an agentless solution has been designed. This solution extracts ETW insertion strings² data and forwards them, using a simple PowerShell script, to SYSVOL files. This approach only necessitates a one-time initialization step to:

- Setup the PowerShell script to be executed.

² ETW insertion strings are the same information used by Windows to build its Event Logs
- Configure the necessary audit policies.

This initialization step is performed on each domain controller thanks to a Tenable deployment script downloadable in Tenable.ad, in **System > Configuration > Indicator of Attack**. This page lists the commands to be executed (one for each domain registered in Tenable.ad). To activate the monitoring process, the Tenable deployment script will create a GPO embedding an immediate task configuring the PowerShell ETW script, which runs on each DC to extract ETW information. This immediate task will also install a WMI filter to restart the PowerShell script at boot.

**Manually deploying a GPO from one domain to another is NOT supported. Please use Tenable deployment script for each domain you want to monitor.**

The Tenable deployment script is to be launched from a machine member of the domain to monitor (some customers run the script directly from one of the Domain Controllers, which is supported too), with an account having enough administrative privileges to create a GPO and to link it to the organizational unit hosting the Domain Controllers of the domain to monitor, and to have various PowerShell modules installed and available: ActiveDirectory, GroupPolicy. Note that the ActiveDirectory PowerShell module must also be available on each DC of the domain. When installing the GPO, the deployment script will check for the replication status (a GPO cannot be installed while the DC is replicating), therefore the RSAT-DFS-Mgmt-Con feature is also needed on the machine that runs this script.

**Tenable.ad – Indicator-of-Attack setup view**

**Configuration adaptations**

For each targeted domain, executing this script will apply configuration changes, listed below. Some parameters (e.g. the GPO name), can be modified using command-line arguments passed when executing the script.

Use the following PowerShell command to have the complete list of available arguments and examples:

```
Get-Help Register-TenableIOA.ps1
```

**Synthesis of the technical changes made by Tenable’s deployment script**
The following table describes the major configuration changes applied to the Domain Controllers to monitor. These changes are transparently applied by the GPO created by Tenable’s deployment script.

**Configuration changes**

- Add a GPO, named “Tenable.ad” by default, linked to the Domain Controllers OU by default. This GPO contains an immediate task configuring the PowerShell script running on each DC and installing a WMI filter that will start the PowerShell ETW script at boot, and the Advanced logging policy (see below).
- Activate the Microsoft Advanced logging policy, by modifying a registry key\(^3\) (using the GPO).
- Apply a new Event Log policy to force Domain Controllers to generate the ETW information required by Tenable’s IOAs.
  - Install a WMI event consumer that will execute a VBS script (using the `ActiveScriptEventConsumer` class). This VBS script is run at boot and looks for a running PowerShell ETW script, which it will run if not found.

The new event log policy is dynamically generated within the Tenable deployment script and activated by the GPO. Applying this policy is mandatory to have the ETW engine to generate the Insertion Strings required by Tenable. This policy does not disable any existing logging policy but enriches them if need be. If a conflict is detected, the Tenable deployment script will stop with a message stating that the audit policy policy_name is needed, but that the current AD configuration prevents its configuration.

More technical information describing step-by-step changes operated by Tenable deployment script is available on Tenable’s [online documentation](https://docs.microsoft.com/en-us/windows/win32/etw/about-event-tracing#missing-events).

### Limitation and potential impacts

Despite being the less intrusive way to capture Domain Controllers’ ETW information, some limitations and limited impact could exist in Tenable’s approach. These drawbacks need to be reviewed before starting the deployment of the Indicator-of-Attack module.

Tenable’s incident detection module is based on the ETW data, thus bound by their limitations as defined by Microsoft\(^4\).

The installed GPO needs to be replicated over the entire domain, and the GPO refresh interval must be over for the install process to be complete. During the replication period, false positives and false negatives can happen even though Tenable minimizes this effect by not starting the checks in the IOA engine immediately.

Tenable is using the SYSVOL file share to retrieve ETW information coming from the Domain Controllers. As the SYSVOL replicates to every Domain Controller of the domain, a significant increase of the replication activity will appear during a high peak of AD activity.

Replicating files between the Domain Controllers and Tenable’s platform will also consume some network bandwidth. These impacts are controlled by the auto-removal of the files collected by Tenable and the limited size of these files (500 MB maximum by default, see the `MaxBufferSizeBytes` script variable for the exact default value).

### 3.2. Microsoft Sysmon

The additional Microsoft Sysmon\(^5\) service is required to activate a subset of Tenable’s Indicators-of-Attack. Supported by Microsoft, this software registers a new Windows Service to provide more security-oriented information in the ETW infrastructure.

---

\(^3\) Specifically, the registry key is `MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy`, Set to 1

\(^4\) Microsoft documentation: [https://docs.microsoft.com/en-us/windows/win32/etw/about-event-tracing#missing-events](https://docs.microsoft.com/en-us/windows/win32/etw/about-event-tracing#missing-events)

The list of Indicators-of-Attack requiring Microsoft Sysmon to operate are listed in the following table. If the IOA is not mentioned, it will work even if Microsoft Sysmon has not been deployed.

<table>
<thead>
<tr>
<th>Name of the indicator</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Credential Dumping: LSASS Memory</td>
<td>Detecting Process Injection</td>
</tr>
</tbody>
</table>

Tenable understands that installing an additional Windows Service can affect performances of the Domain Controllers hosting the AD infrastructure. Therefore, Tenable chooses not to automatically deploy Microsoft Sysmon. It must be installed manually or by a dedicated GPO.

Manual deployment of Microsoft Sysmon on the domain controllers (optional)

Sysmon deployment and management is at the customer's discretion. In particular, incompatibilities need to be tested before a full-blown deployment.

Once downloaded from the Sysinternal website, the following command will install Microsoft Sysmon on the current machine:

```
Command line
.
```

The configuration file is available in the annexes of this document or on Tenable’s documentation portal where the file is entirely commented.

This Sysmon installation is not sufficient by itself and a registry key is needed for the WMI filters to be aware of Sysmon being installed:

```
Command line
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon\Operational"
```

In case the Sysmon tool indeed affects the performances of the AD infrastructure, the following command will uninstall Sysmon from the current machine:

```
Command line
.
```

---


7 Tenable documentation portal: [https://docs.tenable.com/Tenablead.htm](https://docs.tenable.com/Tenablead.htm)
3.3. Problem with Advanced Audit Policy Configuration GPO precedence

The GPO created by Tenable.ad to enable required events logging is linked to the Domain Controllers OU and Enforced mode is enabled. This gives it a very high priority, but an Enforced GPO configured at a higher level (e.g. Domain or Site) will take precedence over it. If this higher priority GPO defines Advanced Audit Policy Configuration settings that conflict with Tenable’s needs, it will win and Tenable.ad will miss required events for attack detection.

Advanced Audit Policy Configuration settings defined by GPOs are merged by Windows, so different GPOs can define different settings. However, at each setting level, only the value defined by the GPO with the higher precedence is used. For example, Tenable.ad needs the "Success and Failure" value for the "Audit Credential Validation" setting. However, if a GPO with more precedence only defines "Success" for "Audit Credential Validation", then Windows will only collect "Success" events and Tenable.ad will miss the required "Failure" too.

How to check?

Run the following command on a Domain Controller. It will output the effective Advanced Audit Policy Configuration after considering all GPOs and precedence.

```
Command line

auditpol.exe /get /category:*
```

Compare the output with the Tenable.ad advanced audit policy requirements. For each setting required by Tenable.ad, ensure that the effective policy covers it, at least. This is also fine if the effective policy is more exhaustive, for example when Tenable.ad needs "Success" or "Failure" and the setting is "Success and Failure".

How to fix it?

If the effective policy is insufficient, it means that a GPO with a higher precedence defines conflicting settings. Look for GPOs linked to higher levels (Domain or Site) in Enforced mode that define Advanced Audit Policy Configuration.

The following command can also be used on a Domain Controller to pinpoint the Winning GPO:

```
Command line

```
When identified, the corresponding Advanced Audit Policy Configuration setting in the GPO must be modified to cover at least what is required by Tenable.ad.

For example, if Tenable.ad requires "Success" and the higher priority GPO defines "Failure", then it should be modified to "Success and Failure".

Another example, if Tenable.ad requires "Success and Failure" and the higher priority GPO defines "Success", then it should be modified to "Success and Failure".

After modification, wait until the updated GPO applies, or force it with the "gpupdate" command.

Then, check the new effective policy as instructed above.

3.4. Update Tenable's module on the Domain Controllers

To update the Tenable's IoA module, you must:

1. Uninstall the script currently in use by running it with the "-Uninstall" parameter
2. Wait a couple of hours so the cleaning GPO is properly replicated and applied by all domain controllers (at the time of writing, the script will enforce a 4-hour delay)
3. Delete manually the cleaning GPO
4. Download the new script version
5. Install it as explained above
7. ANNEXES

1. How to change IIS certificate for Tenable.ad Web Application

When the Tenable.ad SEN module is installed, a self-signed certificate is created and bound to the Tenable.ad web application.

The certificate name is chosen during the installation and is equal to webAppHostName. Let us assume that the chosen name is the IP address of the SEN server where the IIS role is installed, since this is the most common scenario.

If, by assumption, the IP address of the SEN server is **10.0.48.55**, after installation, the web application can be accessed via **https://10.0.48.55**.

There are two important pieces involved here so you can access the web application via HTTPS:

- Self-signed certificate
- Web App binding

During installation, a self-signed certificate is created and placed in the IIS Server Certificate store.

To access this certificate, go to **Windows Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**, and click on the Server Name on the left (Connections) pane followed by a double-click on 'Server Certificates'.
During installation, IIS Site Binding is created by using the HTTPS port (443 by default) and the self-signed certificate.

To explore this binding, go to Windows Start > Windows Administrative Tools > Internet Information Services (IIS) Manager and expand the ‘Sites’ menu on the left pane. Right-click on your site (Default Web Site, in this example) and choose ‘Edit Bindings’. A new window ‘Site Bindings’ will pop up, and from there you can select the ‘https’ binding and click on ‘Edit’.

On the ‘Edit Site Binding’ window that will appear, you can find installed IIS certificates in the drop-down menu at the bottom of the dialog.

To use your certificate for the Tenable.ad web application, you must:
- Install your certificate in IIS.
- Edit site binding to use your installed certificate.

To install the IIS Certificate, go to Windows Start > Windows Administrative Tools > Internet Information Services (IIS) Manager and click on Server Name on the left (Connections) pane followed by a double-click on 'Server Certificates'.

From there, choose 'Import' on the right pane menu and import your certificate.

To edit site binding, navigate to 'Edit Site Binding' as described above, and choose your newly installed certificate from the SSL certificate dropdown menu at the bottom of the dialog:
Select new certificate in IIS Manager

Right-click on the website on the left pane and restart to take effect.

Restart IIS Manager service
2. How to back up Storage Manager

2.1. InfluxDB

Backup procedure

To perform a **remote** backup, please follow those steps:

- Open a PowerShell (x64) window as an administrator
- Move to D:\Tenable\Tenable.ad\AfadInfluxDB\influxdb
- Run the following command (replace the yellow part by the real expected value):

  ```bash
  influxd backup -portable -host <host:port> <path-to-backup>
  ```

To perform a **local** backup, please follow those steps:

- Open a PowerShell (x64) window as an administrator
- Move to D:\Tenable\Tenable.ad\AfadInfluxDB\influxdb
- Run the following command (replace the yellow part by the real expected value):

  ```bash
  influxd backup -portable <path-to-backup>
  ```

Restore procedure

To perform a **remote** restoration, please follow those steps:

- Open a PowerShell (x64) window as an administrator
- Move to D:\Tenable\Tenable.ad\AfadInfluxDB\influxdb
- Run the following command (replace the yellow part by the real expected value):

  ```bash
  influxd restore -portable -host <host:port> <path-to-backup-files>
  ```

To perform a **local** restoration, please follow those steps:

- Open a PowerShell (x64) window as an administrator
- Move to D:\Tenable\Tenable.ad\AfadInfluxDB\influxdb
- Run the following command (replace the yellow part by the real expected value):

  ```bash
  influxd restore -portable <path-to-backup-files>
  ```

⚠️ The backup is a folder, not a file.

Source: [https://docs.influxdata.com/influxdb/v1.7/administration/backup_and_restore/](https://docs.influxdata.com/influxdb/v1.7/administration/backup_and_restore/)

2.2. MSSQL

Please follow the official documentation to perform MSSQL backup or restoration:

The database name is “dsc” prior to version 2.6.0, and “alsidforad” for ulterior versions.
3. Expert Mode for Directory Listener

Expert Mode: The following options are only available when this mode is switched on.

3.1. Additional subnets for Ceti

You can specify the subnet(s) you want to use for Ceti. If you want to add more than one subnet, use a comma as a separator between the CIDR subnets you will use. For example, 10.0.0.1/32, 192.168.0.0/24.

In the following screenshots, we are only using one subnet. Then, click on the "Next" button and install Tenable.ad.

![Directory Listener settings dialog with Expert Mode]

Wait for the end of the installation and click on YES to reboot the server.

4. Optional Sysmon configuration file

```xml
<Sysmon schemaversion="4.40">
  <EventFiltering>
    <!-- SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate] -->
    <RuleGroup name="" groupRelation="or">
      <ProcessCreate onmatch="exclude">
        <!-- NOTE: Using "exclude" with no rules means everything in this section will be logged -->
      </ProcessCreate>
    </RuleGroup>
    <!-- SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHANGED IN THE FILESYSTEM [FileCreateTime] -->
    <RuleGroup name="" groupRelation="or">
      <FileCreateTime onmatch="include">
        <!-- NOTE: Using "include" with no rules means nothing in this section will be logged -->
      </FileCreateTime>
    </RuleGroup>
    <!-- SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect] -->
    <RuleGroup name="" groupRelation="or">
      <NetworkConnect onmatch="include">
        <!-- NOTE: Using "include" with no rules means nothing in this section will be logged -->
      </NetworkConnect>
    </RuleGroup>
  </EventFiltering>
</Sysmon>
```
<RuleGroup name="" groupRelation="or">
  <ProcessTerminate onmatch="exclude">
    <!--NOTE: Using "exclude" with no rules means everything in this section will be logged-->
  </ProcessTerminate>
</RuleGroup>

<!--SYSMON EVENT ID 5 : DRIVER LOADED INTO KERNEL [DriverLoad]-->
<RuleGroup name="" groupRelation="or">
  <DriverLoad onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </DriverLoad>
</RuleGroup>

<!--SYSMON EVENT ID 6 : DLL (IMAGE) LOADED BY PROCESS [ImageLoad]-->
<RuleGroup name="" groupRelation="or">
  <ImageLoad onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </ImageLoad>
</RuleGroup>

<!--SYSMON EVENT ID 7 : REMOTE THREAD CREATED [CreateRemoteThread]-->
<RuleGroup name="" groupRelation="or">
  <CreateRemoteThread onmatch="include">
    <TargetImage name="lsass" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    <!-- Detect Access to LSASS-->
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x1FFFFF</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x1F1FFF</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x1010</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x143A</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x0800</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x800</GrantedAccess>
    </Rule>
  </CreateRemoteThread>
</RuleGroup>

<!--SYSMON EVENT ID 9 : RAW DISK ACCESS [RawAccessRead]-->
<RuleGroup name="" groupRelation="or">
  <RawAccessRead onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </RawAccessRead>
</RuleGroup>

<!--SYSMON EVENT ID 10 : INTER-PROCESS ACCESS [ProcessAccess]-->
<RuleGroup name="" groupRelation="or">
  <ProcessAccess onmatch="include">
    <!-- Detect Access to LSASS-->
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x1FFFFF</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x1F1FFF</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x1010</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x143A</GrantedAccess>
    </Rule>
    <Rule groupRelation="and">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x0800</GrantedAccess>
    </Rule>
  </ProcessAccess>
</RuleGroup>

<!--SYSMON EVENT ID 11 : FILE CREATED [FileCreate]-->
<RuleGroup name="" groupRelation="or">
  <FileCreate onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </FileCreate>
</RuleGroup>

<!--SYSMON EVENT ID 12 & 13 & 14 : REGISTRY MODIFICATION [RegistryEvent]-->
<RuleGroup name="" groupRelation="or">
  <RegistryEvent onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </RegistryEvent>
</RuleGroup>

<!--SYSMON EVENT ID 15 : ALTERNATE DATA STREAM CREATED [FileCreateStreamHash]-->
<RuleGroup name="" groupRelation="or">
  <FileCreateStreamHash onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </FileCreateStreamHash>
</RuleGroup>
<EventFiltering>

<!--SYSMON EVENT ID 16 : SYSMON CONFIGURATION CHANGE-->
<!--Cannot be filtered.-->

<!--SYSMON EVENT ID 17 & 18 : PIPE CREATED / PIPE CONNECTED [PipeEvent]-->
<RuleGroup name="" groupRelation="or">
  <PipeEvent onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </PipeEvent>
</RuleGroup>

<!--SYSMON EVENT ID 19 & 20 & 21 : WMI EVENT MONITORING [WmiEvent]-->
<RuleGroup name="" groupRelation="or">
  <WmiEvent onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </WmiEvent>
</RuleGroup>

<!--SYSMON EVENT ID 22 : DNS QUERY [DnsQuery]-->
<RuleGroup name="" groupRelation="or">
  <DnsQuery onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </DnsQuery>
</RuleGroup>

<!--SYSMON EVENT ID 23 : FILE DELETED [FileDelete]-->
<RuleGroup name="" groupRelation="or">
  <FileDelete onmatch="include">
    <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
  </FileDelete>
</RuleGroup>

</EventFiltering>