TENABLE.AD

INSTALLATION 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>19/12/2019</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>30/07/2021</td>
<td>TENABLE</td>
<td>Update for 3.1.0</td>
</tr>
</tbody>
</table>
# Table of Contents

- **Introduction**
  - Document objectives
  - Abbreviations
- **Infrastructure presentation**
  - Network Overview
  - Preferred architectures
  - Meta-Kapteyn architecture (optional)
  - Installation log file
- **Required resources**
  - Sizing for Directory Listeners
  - Security Engine Node sizing
- **Storage Manager sizing**
  - Minimal and Recommended Computing Power
  - Supported and Recommended Disk Layout
  - Minimal and Recommended Disk Sizing
  - Minimal and Recommended Disk Performance
  - Additional Notes
  - Example
- **Additional support information**
- **Install Binaries**
  - Deployment on Windows Server (Full-Desktop Experience)
  - Deployment on Windows Server Core
- **Installation procedure**
  - Install Storage Manager
  - Install Security Engine Node
    - One machine
    - Four machines
      - Virtual machine #1: RabbitMQ component
      - Virtual machine #2: Cephei/Ceti Bridge components
      - Virtual machine #3: Cancri and Caroli components
      - Virtual machine #4: Cygni components
  - Install the Directory Listener
    - Install the Directory Listener using DL package
- **Active Directory configuration**
  - General considerations
Domain controller to monitor
User account
Access to specific Active Directory objects or containers
Configure the monitored infrastructure to support Tenable’s Indicator-of-Attack

Tenable deployment script
  Launch the Tenable deployment script
  Configuration adjustments
  Synthesis of the technical changes made by Tenable’s deployment script
  Limitation and potential impacts

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

Problem with Advanced Audit Policy Configuration GPO precedence
  How to check?
  How to fix it?

Annexes

How to change IIS certificate for Tenable.ad Web Application

To install the IIS Certificate:

Meta-Kapteyn configuration file

How to back up Storage Manager

InfluxDB

MSSQL

Expert Mode for Directory Listener

Additional subnets for Ceti

5. What is a complex password?

6. Horizontally scale up/down services to improve data processing performance?

Scale Up

  Scaling Cancri

  Scaling Caroli

  Scaling Eridanis

7. Optional Sysmon configuration file
INTRODUCTION

1. Document objectives

This document aims to help you perform a clean installation of Tenable’s on-premises solution. Each component is made of 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:

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:
The following network matrix describes each required protocol and port used by Tenable’s platform.

<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>Tenable’s Directory Listen</td>
<td>Directory, Rep</td>
<td>LDAP/LDAPS</td>
<td>TCP/389 and TCP/636, ICMP/echo-request</td>
</tr>
<tr>
<td>ers -&gt; Domain controllers</td>
<td>lication, User</td>
<td></td>
<td>ICMP/echo-response</td>
</tr>
<tr>
<td></td>
<td>and Computer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authentication, User and Computer Authentication, Group Policy, Trusts</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Group Policy,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trusts</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Replication, User</td>
<td>SMB, CIFS, SMB2,</td>
<td>TCP/445</td>
</tr>
<tr>
<td></td>
<td>and Computer Authentication, Group Policy, Trusts</td>
<td>DFSN, LSARPC, NbtSS, NetLogonR, SamR, SrvSvc</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<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>
| **Tenable’s Directory Listeners** | User and Computer Authentication, Name Resolution, Trusts | DNS | UDP/53 and TCP/53
| **Tenable’s Security engine nodes** | User and Computer Authentication, Group Policy, Trusts | RPC, DCOM, EPM, DRSUAPI, NetLogonR, SamR, FRS | TCP Dynamic (> 1024)
| **Directory, Replication, User and Computer Authentication, Group Policy, Trusts** | Replication | Global Catalog | TCP/3268 and TCP/3269
| **Tenable’s internal API flows (Optional)** | Replication | RPC Endpoint Mapper | TCP/135
| **Tenable’s communication bus** | Advanced Message Queuing Protocol | TCP/5671 and TCP/5672
| **Tenable’s end-user services (Web portal, REST API, etc.)** | Tenable’s Directory Listeners -> Tenable’s Security engine nodes | Time synchronization | NTP | UDP/123
| **End-users** | Update infrastructure (e.g., WSUS or SCCM) | HTTP/HTTPS | TCP/80 or TCP/443
| **Tenable’s Security engine nodes** | PKI infrastructure | HTTP/HTTPS | TCP/80 or TCP/443
| **Identity provider SAML server** | Identity provider OAuth | TLS/HTTP | TCP/443
| **Identity provider LDAP** | Support services | LDAP/LDAPS | TCP/389 and TCP/636
| **Identity provider OAuth** | | TLS/HTTP | TCP/443

Tenable's communication bus Advanced Message Queuing Protocol TCP/5671 and TCP/5672
Tenable's end-user services (Web portal, REST API, etc.)
Time synchronization NTP UDP/123
Update infrastructure (e.g., WSUS or SCCM) HTTP/HTTPS TCP/80 or TCP/443
PKI infrastructure HTTP/HTTPS TCP/80 or TCP/443
Identity provider SAML server TLS/HTTP TCP/443
Identity provider LDAP LDAP/LDAPS TCP/389 and TCP/636
Identity provider OAuth TLS/HTTP TCP/443
In addition to the Active Directory protocols, some additional flows may be required depending on Tenable’s platform configuration. These protocols and ports need to be opened between Tenable’s 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’s 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>Tenable’s Security engine nodes &lt;-&gt; Tenable’s Storage Manager</td>
<td>Tenable REST API</td>
<td>HTTP/TLS</td>
<td>TCP/443</td>
</tr>
<tr>
<td></td>
<td>MSSQL Server database access</td>
<td>MSSQL queries</td>
<td>TCP/1433</td>
</tr>
<tr>
<td></td>
<td>InfluxDB Server access</td>
<td>InfluxDB queries over HTTP</td>
<td>TCP/8086</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.

For more information, please refer to [Meta-Kapteyn configuration file](#) and contact [our Support](#).

3.4. 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 Tenable's 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. Security Engine Node sizing

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>
</tbody>
</table>
4.3. Storage Manager sizing

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 performances 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

<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 – 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>32 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>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>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>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>
</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).

### Storage managers – Disk Performance Matrix

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Minimal Disk Performance</th>
<th>Recommended Disk Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – 25 000</td>
<td>150/2 500</td>
<td>300/5 000</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
<td>200/5 000</td>
<td>400/10 000</td>
</tr>
<tr>
<td>50 001 - 75 000</td>
<td>200/5 000</td>
<td>400/10 000</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
<td>200/5 000</td>
<td>400/10 000</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
<td>250/7 500</td>
<td>500/15 000</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
<td>250/7 500</td>
<td>500/15 000</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
<td>500/16 000</td>
<td>1 000/32 000</td>
</tr>
</tbody>
</table>

### 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 are the following:

<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>

1.1. 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. Do not run Tenable.ad 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-tiers model. It does not support one or two VMs. It supports at least three VMs and eventually more than one DL. 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 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’ or ‘Tenable’ on the data partition.
- Erlang known issues: Do not modify the HOMEDRIVE environment variable. The PATHEXT environment variable must contain the .EXE and .BAT file extensions.

1.2. Install Binaries

Tenable.ad installer binary is available on Tenable’s Downloads Portal (https://www.tenable.com/downloads/tenablead).

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

Tenable recommends rebooting all machines before starting a new installation.
Deployment on Windows Server (Full-Desktop Experience)

1. Place the installer binary 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>C:\Users\Administrator\Desktop\</td>
<td><img src="image" alt="Desktop location" /></td>
</tr>
</tbody>
</table>

2. Activate Extended debug logging with the following command (replace the first path by your executable file location, and the second by 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

You can display the installer GUI on a Server Core.

3. Run the following command to start the installation (replace the path with your executable file location):

```
C:\Users\Administrator\Desktop\Tenable.ad_3.X.X.exe
```
I. INSTALLATION PROCEDURE

As mentioned previously, we are using three machines: the **Storage Manager**, the **Security Engine Node** and the **Directory Listener**.

- Tenable provides an installer for these components but does not configure the host beyond what is necessary for the product to run.
- In particular, all three machines and installed binaries support the application of any security update for the underlying OS, either through WSUS or SCCM. Patch management is left at the customer’s discretion.

1. **Install Storage Manager**

   During this step, the process delivers the following applications:

   - InfluxDB
   - MSSQL

   The installation is fully automated using an executable file. To run the installation:

   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)

   2. In the next window, you can choose the features you want to deploy. By default, everything is selected. You must specify what you do not want to install. To deploy only the Storage Manager feature, you must select only this feature.
   3. Change the Location if needed by editing ONLY the drive letter. You can do this by clicking on the "Browse" button.
   4. Click on the "Next" button.
5. Enter a complex password (if you need more details, please refer to [What is a complex password?](#)) for the SQL database. The instance name is **TENABLE** by default. Change it only if necessary. Otherwise, keep **TENABLE** default instance name and click on the “Next” button. You are now ready to install Tenable.ad.

We strongly recommend you keep the default instance name ("TENABLE"). If you change it, please refer to the following documentation to use a valid name: [https://docs.microsoft.com/mt-mt/sql/sql-server/install/instance-configuration?view=sql-server-2017](https://docs.microsoft.com/mt-mt/sql/sql-server/install/instance-configuration?view=sql-server-2017)

6. Wait for the end of the installation and click on **YES** to reboot the server.
If virtual account usage is prohibited on the SQL machine, this step will fail. The MSSQL service can run as NT AUTHORITY\SYSTEM account instead of a virtual account after the installation.

If you are looking for a procedure to back up the Influx and MSSQL databases, please refer to [How to back up Storage Manager](#).

2. Install Security Engine Node

During this step, the process delivers the following applications:

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

You can split the SEN machine into different machines to improve performance on huge infrastructures.

1.1. One machine

The installation is fully automated using an executable file. To perform the installation:

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

2. In the next window, you can choose the features you want to deploy. By default, everything is selected. You must specify what you do not want to install. To only deploy the SecurityEngineNode feature, you must select only this feature.
3. Change the Location if needed by editing ONLY the drive letter. You can do this by clicking on the “Browse” button.

4. Click on the “Next” button.

5. Indicate the Storage Manager’s IP address in the two dedicated fields and enter the password of the SQL database that you previously chose and click “Next”.

6. To make the Tenable Web application and services (SAML, SMTP, etc.) available for end users, enter the DNS name (preferred) or the IP address that the end users use to access Tenable’s platform.

   By default, the installation process creates a self-signed certificate with the DNS name or the IP you entered. If you want to change this certificate, refer to How to change IIS certificate for Tenable.ad Web Application.
7. Click “Install”.

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

1.2. Four machines

The standard architecture for the Tenable.ad on-premises solution comprises three VMs by default. However, if the environment that you want to monitor is greater than 300K users, consider splitting the SEN into four different machines.

As mentioned in 4 Required resources page, we recommend using the following architecture for SEN components when three VMs are not enough:

<table>
<thead>
<tr>
<th>VM name</th>
<th>vCPU (per instance)</th>
<th>Memory (per instance)</th>
<th>Disk space (per instance)</th>
<th>Recommended services</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM1:</td>
<td>8 cores, at least 2.6 GHz</td>
<td>16 GB of RAM</td>
<td>1 TB</td>
<td>RabbitMQ</td>
</tr>
</tbody>
</table>
Virtual machine #1: RabbitMQ component

The installation is fully automated using an executable file. To perform the installation:

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

   ![Welcome dialog on Security Engine Node (1)](image)

2. In the next window, you can choose the features you want to deploy. By default, everything is selected. You must specify what you do not want to install. To only deploy the RabbitMQ feature, you must select only this feature.

3. Change the Location if needed by editing ONLY the drive letter. You can do this by clicking on the “Browse” button.

4. Click “Next” to install Tenable.ad.

   ![Features dialog on Security Engine Node (1)](image)

5. Wait for the end of the installation and click on **YES** to reboot the server.
Virtual machine #2: Cephei/Ceti Bridge components

The installation is fully automated using an executable file. To perform the installation:

1. Execute "Tenable.ad_v3.X.X.exe" with full Local Administrator privileges and click on the "Next" button.
2. In the next window, you can choose the features you want to deploy. By default, everything is selected. You must specify what you do not want to install. To deploy only Node, Cephei and CetiBridge, you must select only these features:
   - Cephei
   - CetiBridge
   - Electra
   - Enif
   - Equuleus
   - Eridanus
   - Kapteyz
3. Change the Location if needed by editing ONLY the drive letter. You can do this by clicking on the "Browse" button.
4. Click on the "Next" button and install Tenable.ad.

![Features dialog on Security Engine Node (2)](image)

5. Indicate the Storage Manager’s IP address in the two dedicated fields and type the password of the SQL database that you previously chose.
6. Click "Next".
7. To make the Tenable Web application and services (SAML, SMTP, etc.) available for end users, enter the DNS name (preferred) or the IP address that end users use to access Tenable’s platform.

By default, the installation process creates a self-signed certificate with the DNS name, or the IP typed. If you want to change this certificate, please refer to How to change IIS certificate for Tenable.ad Web Application.

8. Enter the RabbitMQ’s IP address and click on the “Next” button and install Tenable.ad.

9. Click “Install”.
10. Wait for the end of the installation and click on YES to reboot the server.

Virtual machine #3: Cancri and Caroli components

The installation is fully automated using an executable file. To perform the installation:

1. Execute “Tenable.ad_v3.X.X.exe” with full Local Administrator privileges and click on the “Next” button.
2. In the next window, you can choose the features you want to deploy. By default, everything is selected. You must specify what you do not want to install. To deploy only Cancri and Caroli, you must select only these features.
3. Change the Location if needed by editing ONLY the drive letter. You can do this by clicking on the “Browse” button.
4. Click on the “Next” button and install Tenable.ad.
5. Indicate RabbitMQ’s IP address and Eridanis’ IP address in the two dedicated boxes.
6. Click on the “Next” button and install Tenable.ad.

7. Click “Install”.
8. Wait for the end of the installation and click on YES to reboot the server.

**Virtual machine #4: Cygni components**

The installation is fully automated using an executable file. To perform the installation:

1. Execute “Tenable.ad_v3.X.X.exe” with full Local Administrator privileges and click on the “Next” button.
2. In the next window, you can choose the features you want to deploy. By default, everything is selected. You must specify what you do not want to install. To deploy only Cancri and Caroli, you must select only these features.
3. Change the Location if needed by editing ONLY the drive letter. You can do this by clicking on the “Browse” button. Then, click on the “Next” button and install Tenable.ad.
4. Indicate RabbitMQ’s IP address and Eridanis’ IP address in the two dedicated boxes, and click on the “Next” button to install Tenable.ad.

5. Click “Install”.
6. Wait for the end of the installation and click on YES to reboot the server.

3. Install the Directory Listener

This step in the process installs the following applications:

- Tenable component
  i. 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 due to legal restrictions, you can deploy one DL in the first subnet and another DL in the second subnet.
The installation is fully automated using an executable file. To perform the installation:

1. **Execute** “Tenable.ad_v3.X.X.exe” with full Local Administrator privileges and click on the “Next” button.
2. In the next window, you can choose the features you want to deploy. By default, everything is selected. You must specify what you do not want to install. To deploy only Cancri and Caroli, you must select only these features.
3. Change the Location if needed by editing ONLY the drive letter. You can do this by clicking on the “Browse” button. Here in our example, the driver letter is E. Then, click on the “Next” button and install Tenable.ad.

4. Indicate RabbitMQ’s IP address and Eridanis’ IP address in the two dedicated boxes, and click on the “Next” button to install Tenable.ad.

5. Click “Install”.
6. Wait for the end of the installation and click on YES to reboot the server.
4. Install the Directory Listener using DL package

The installation is fully automated using an executable file. To perform the installation:

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

2. In the next window, you can choose the features you want to deploy. By default, everything is selected. You must specify what you do not want to install. To deploy only Cancri and Caroli, you must select only these features.

3. Change the Location if needed by editing ONLY the drive letter. You can do this by clicking on the “Browse” button. Then, click on the “Next” button and install Tenable.ad.

4. Enter the IP address for RabbitMQ and click “Next”.

5. Click “Install”.

6. Wait for the end of the installation and click on **YES** to reboot the server.
   
   For more options, you can **install the DL using the “Expert Mode”**.

II. **ACTIVE DIRECTORY CONFIGURATION**

1. **General considerations**

   Tenable.ad is designed to be a non-intrusive solution able to monitor a directory infrastructure without requiring the deployment of agents, and with as little configuration change as possible 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 Directory Listener, and no additional cost within the infrastructure.

   - To **detect efficiently 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, you need to deploy a dedicated Group Policy Object using a dedicated deployment tool available in Tenable’s console. This GPO will activate, on all domain controllers, a WMI filter that writes to SYSVOL. This profits from the AD replication engine and Tenable’s ability to listen to SYSVOL events. A rolling mechanism removes the files that the WMI filter writes (using another WMI filter) to avoid filling the SYSVOL.

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

2. Domain controller to monitor

Tenable’s platform only requires communication with the Primary Domain Controller emulator (PDCe) using the network protocols previously described.

In the case of multiple domains (or forests) monitored by Tenable.ad, the PDCe of each domain must be reached.

From a performance perspective, Tenable recommends hosting the Tenable.ad platform on the physical network close to the PDCe to monitor. During the deployment process, the Tenable technical lead can assist the customer to select the most appropriate network.

3. User account

Tenable.ad must authenticate to the monitored infrastructure to access the replication flow.

In accordance with its non-intrusive approach, the platform only requires a non-administrative account to perform its operation. All the collected data is accessible for a simple user; no secret attribute (credentials, password hashes or Kerberos keys) is required for access to the Tenable platform.

Hence, Tenable recommends that you create a service account that is a member of the group “Domain Users” (at least) with the following specifications:

- Created on the main monitored domain
- Created in any Organizational Unit (preferably where other security service accounts are usually created)
- Standard user group membership (e.g., member of the Domain Users AD built-in group)

Tenable currently only supports explicit authentication based on a login and password. Therefore, we recommend using a predefined password with the PasswordNeverExpires attribute set, or with password renewal policies not being enforced. A strong and unpredictable password must be used.

Activating the Indicator-of-Attack feature requires deploying a new GPO on the infrastructure to monitor using a PowerShell script that the Tenable platform provides. You must run this script once for each feature deployment and requires an administrative account able to create a new GPO and link it to the organizational unit that hosts the Domain Controllers of the monitored domain.

4. Access to specific Active Directory objects or containers

The Tenable platform achieves its security monitoring without the need for administrative privileges. Despite its many advantages (operation safety, limited attack surface, etc.), this approach relies on the ability of the user account that the platform uses to read all the Active Directory objects stored in a domain (including user accounts, organizational units, groups, etc.).

Note: This section only applies for the platform benefiting from the Indicator-of-Exposure module.

By default, most of the objects natively benefit from a default read access for the group Domain Users that the Tenable service account uses. However, you must manually configure some containers to allow read access to the Tenable user account:

<table>
<thead>
<tr>
<th>Active Directory objects or containers requiring manual read access setup</th>
<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>
<td></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>
<td></td>
</tr>
</tbody>
</table>

- For each of the containers above, Tenable must grant access to the service account that the platform uses via the following command line:

  ```
dsacls "<__CONTAINER__>" /takeownership
  dsacls "<__CONTAINER__>" /g <__SERVICE_ACCOUNT__>:LCRP /I:T
  ```

- 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.
5. Configure the monitored infrastructure to support Tenable’s Indicator-of-Attack

**Note:** This section only applies for the platform benefiting from the Indicator-of-Attack module (IOA).

Here, we configure the monitored Domain Controllers to retrieve the required ETW information and to forward them to the Tenable.ad platform with focus on:

- Tenable’s deployment script, a PowerShell script used to deploy Windows-component requirements on the Domain Controllers.
- The installation of Microsoft Sysmon, a Windows system tool needed by some of the Tenable’s IOA to get relevant system data.
- The uninstallation or update of the Tenable deployment script.

### 5.1 Tenable deployment script

To retrieve the required ETW information within Tenable’s platform, we designed a unique system based on an agentless solution. This solution extracts ETW insertion strings\(^2\) data and forwards them to SYSVOL files using a simple PowerShell script. This approach only necessitates a one-time initialization step to:

- Setup the PowerShell script to be executed.
- Configure the necessary audit policies.

A downloadable deployment script from Tenable.ad persion this initialization step on each domain controller in **System > Configuration > Indicator of Attack**. This page lists the commands to execute (one for each domain registered in Tenable.ad).

To activate the monitoring process, the Tenable deployment script creates a GPO that embeds an immediate task to configure the PowerShell ETW script, which runs on each DC to extract ETW information. This immediate task also installs a WMI filter to restart the PowerShell script at boot.

---

**Tenable.ad does not support manually deploying a GPO from one domain to another. Please use the Tenable deployment script for each domain that you want to monitor.**

---

### Launch the Tenable deployment script

You launch the Tenable deployment script from a machine that is a member of the domain to monitor with an account that has:

- Enough administrative privileges to create a GPO and to link it to the organizational unit hosting the Domain Controllers of the domain to monitor (some customers run the script directly from one of the Domain Controllers, which is supported too).
- Various PowerShell modules installed and available: ActiveDirectory, GroupPolicy. Note that the ActiveDirectory PowerShell module must also be available on each DC of the domain.
- The RSAT-DFS-Mgmt-Con feature, because when you install the GPO, the deployment script checks for the replication status (a GPO cannot be installed while the DC is replicating)

---

\(^2\) ETW insertion strings are the same information used by Windows to build its Event Logs
Configuration adjustments

For each targeted domain, executing this Tenable deployment script applies the configuration changes listed below. You can modify some parameters (e.g. the GPO name) using command-line arguments passed when executing the script.

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

  Command line

  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.

<table>
<thead>
<tr>
<th>Configuration changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>- 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).</td>
</tr>
<tr>
<td>- Activate the Microsoft Advanced logging policy, by modifying a registry key(^3) (using the GPO).</td>
</tr>
<tr>
<td>- Apply a new Event Log policy to force Domain Controllers to generate the ETW information required by Tenable’s IOAs.</td>
</tr>
<tr>
<td>- Install a WMI event consumer that executes 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.</td>
</tr>
</tbody>
</table>

\(^3\) Specifically, the registry key is `MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy`, Set to 1
The GPO dynamically generates the new event log policy within the Tenable deployment script and activates it. 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.

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. Review these drawbacks 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.

- 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 uses 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 also consumes 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).

5.2 Microsoft Sysmon

The additional Microsoft Sysmon 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.

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>Indicators-of-Attack requiring Microsoft Sysmon</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 and driver can affect performances of the Domain Controllers hosting the AD infrastructure. Therefore, Tenable chooses not to automatically deploy Microsoft Sysmon. You must install it manually or use a dedicated GPO.

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

1. Once downloaded from the Sysinternal website, run the following command to install Microsoft Sysmon on the current machine:

   **Command line**

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)
.\Sysmon.exe -accepteula -i C:\TenableSysmonConfigFile.xml

The configuration file is available at the end of this document, Optional Sysmon configuration file, or on Tenable’s documentation portal7 where the file is entirely commented.

2. Add a registry key is needed for the WMI filters to know that Sysmon is installed:

<table>
<thead>
<tr>
<th>Command line</th>
</tr>
</thead>
<tbody>
<tr>
<td>reg add &quot;HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon/Operational&quot;</td>
</tr>
</tbody>
</table>

7 Tenable documentation portal: https://docs.tenable.com/Tenablead.htm
Uninstall Sysmon

In case the Sysmon tool indeed affects the performances of the AD infrastructure, run the following commands to uninstall Sysmon from the current machine:

**Command line**

```
.Sysmon64.exe -u
reg delete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon\Operational"
```

Sysmon – Screenshot of a Domain Controller running Sysmon

### 5.3 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.ad’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?**

1. 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:*```

---

© 2023 Tenable. All rights reserved.
2. 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.

1. Run the following command on a Domain Controller to pinpoint the winning GPO:

   **Command line**
   
   ```
   gpresult /scope:computer /h gpo.html
   ```

   - When identified, you modify the corresponding Advanced Audit Policy Configuration setting in the GPO to cover at least what Tenable.ad requires.
   - For example, if Tenable.ad requires "Success" and the higher priority GPO defines "Failure", then modify it to "Success and Failure".
   - Another example, if Tenable.ad requires "Success and Failure" and the higher priority GPO defines "Success", then modify it to "Success and Failure".

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

3. Then, check the new effective policy as instructed above.

---

8 [https://doc.alsid.app/v3.0.0/docs/understand-etw-data-retrieval-by-alsid](https://doc.alsid.app/v3.0.0/docs/understand-etw-data-retrieval-by-alsid)
4. 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. The login page for Tenable.ad displays.

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

- Self-signed certificate
- Web App binding

The installation process creates and places a self-signed certificate in the IIS Server Certificate store.

1. To access this certificate, go to Windows Start > Windows Administrative Tools > Internet Information Services (IIS) Manager
2. Click on the Server Name on the ‘Connections’ left pane followed by a double-click on ‘Server Certificates’.

![Certificates view in IIS Manager](image)

During installation, IIS Site Binding is created by using the HTTPS port (443 by default) and the self-signed certificate.

3. 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.
4. Right-click on your site (Default Web Site, in this example) and choose ‘Edit Bindings’. A new window ‘Site Bindings’ appears
5. Select the ‘https’ binding and click on ‘Edit’.
6. On the ‘Edit Site Binding’ window that appears, you can find installed IIS certificates in the dropdown menu at the bottom of the dialog.
To use your certificate for the Tenable.ad web application, you must:

1. Install your certificate in IIS
2. Edit site binding to use your installed certificate.

To install the IIS Certificate:

1. 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’.
2. Choose ‘Import’ on the right pane menu and import your certificate.

3. You can also choose any other way to install the IIS certificate. The end goal is to have your certificate appear on the IIS Server Certificates list.
4. To edit the 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:

5. Right-click on the website on the left pane and restart to take effect.
2. Meta-Kapteyn configuration file

Meta-Kapteyn installation requires at least two instances of Tenable.ad. For example, let us consider that we are installing Meta-Kapteyn with this configuration:

```
DB  StorageManager services  192.168.1.2
SEN  SecurityEngineNodes services  192.168.1.3
DL  DirectoryListener service  192.168.1.4
```

```
DB  StorageManager services  192.168.10.2
SEN-1  NodeJS services  192.168.10.3
SEN-2  Cygni services  192.168.10.4
SEN-3  Cancri and Caroli services  192.168.10.5
SEN-4  RabbitMQ service  192.168.10.6
DL  DirectoryListener service  192.168.10.7
```
The configuration file must be like:

"InstanceName";"EridanisNodeIp";"EnifNodeIp";"EquuleusNodeIp";"ElectraNodeIp"
"InfrastructureA";"192.168.1.3";"192.168.1.3";"192.168.1.3";"192.168.1.3"
"InfrastructureB";"192.168.10.3";"192.168.10.3";"192.168.10.3";"192.168.10.3"

3. How to back up Storage Manager

3.1 InfluxDB

- To perform a remote backup:
  1. Open a PowerShell (x64) window as an administrator
  2. Move to C:\Tenable\Tenable.ad\StorageManager\AfadInfluxDB\InfluxDB
  3. Run the following command (replace the yellow part by the real expected value):

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

- To perform a local backup:
  1. Open a PowerShell (x64) window as an administrator
  2. Move to C:\Tenable\Tenable.ad\StorageManager\AfadInfluxDB\InfluxDB
  3. Run the following command (replace the yellow part by the real expected value):

```
inluxd backup -portable <path-to-backup-files>
```

- To restore remotely:
  1. Open a PowerShell (x64) window as an administrator
  2. Move to C:\Tenable\Tenable.ad\StorageManager\AfadInfluxDB\InfluxDB
  3. Run the following command (replace the yellow part by the real expected value):

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

- To restore locally:
  1. Open a PowerShell (x64) window as an administrator
  2. Move to C:\Tenable\Tenable.ad\StorageManager\AfadInfluxDB\InfluxDB
  3. Run the following command (replace the yellow part by the real expected value):

```
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/)

3.2 MSSQL

Please follow the official documentation to perform MSSQL backup or restoration: [https://docs.microsoft.com/en-us/sql/t-sql/statements/backup-transact-sql?view=sql-server-ver15](https://docs.microsoft.com/en-us/sql/t-sql/statements/backup-transact-sql?view=sql-server-ver15)

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

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

Directory Listener settings dialog with Expert Mode

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.

1. In the following installation, we use only one subnet. Then, click on “Next” to install Tenable.ad.
2. Click “Install”.

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

5. **What is a complex password?**

Password policies depend on business sectors and legal restrictions.

This is a well-known topic in the cybersecurity world and some articles are published every year to answer the question: What is a complex password in our time? We are not going to answer it, but we will explain what a complex password for the installer is.

We must match the complexity requirements of any customer. That is why we based our criteria on the current password policy that is applied to create a new local account on the machine.

If you want to know more about it, please refer to: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy.
6. Horizontally scale up/down services to improve data processing performance?

Scale Up

Scaling Cancri

The scaling up mechanism of this component goes through its reconfiguration using an environment variable. To perform the scaling:

1. Open a PowerShell (x64) window as an administrator
2. Define the environment variable "ALSID_CASSIOPEIA_CANCRI_Application__MaxConcurrentPublishToEridanis" (default value is 100; a too high value might be more harmful, because it scales with the number of CPUs)
   ```powershell
   [Environment]::SetEnvironmentVariable("ALSID_CASSIOPEIA_CANCRI_Application__MaxConcurrentPublishToEridanis", "IntegerValue", "Machine")
   ```
3. Restart Cancri’s service
   ```powershell
   Restart-Service -Name Alsid_Cancri
   ```

Example:

```
[Environment]::SetEnvironmentVariable("ALSID_CASSIOPEIA_CANCRI_Application__MaxConcurrentPublishToEridanis", "200", "Machine")
Restart-Service -Name Alsid_Cancri
```

Scaling Caroli

The scaling up mechanism of this component is fully automated through a PowerShell Script. To perform the scaling:

1. Open a PowerShell (x64) window as an administrator
2. Define the environment variable "ALSID_CASSIOPEIA_CAROLI_Application__SpeedCoefficient" (default value is 6; a too high value might be more harmful, because it scales with the number of CPUs)
   ```powershell
   [Environment]::SetEnvironmentVariable("ALSID_CASSIOPEIA_CAROLI_Application__SpeedCoefficient", "IntegerValue", "Machine")
   ```
3. Restart Caroli’s service
   ```powershell
   Restart-Service -Name Alsid_Caroli
   ```

Example:

```
[Environment]::SetEnvironmentVariable("ALSID_CASSIOPEIA_CAROLI_Application__SpeedCoefficient", "14", "Machine")
```

Scaling Eridanis

To scale up the total number of Eridanis instances, the ERIDANIS_WORKER_COUNT environment variable must be updated.

1. Open a PowerShell (x64) window as an administrator
2. Run the following command (replace the yellow part by the real expected value):
   ```powershell
   [System.Environment]::SetEnvironmentVariable('ERIDANIS_WORKER_COUNT', '<number of Eridanis instances>', 'Machine')
   Restart-Service -Name 'alsid_Eridanis'
   ```
Example (we want 3 instances of Eridanis):

```powershell
[System.Environment]::SetEnvironmentVariable('ERIDANIS_WORKER_COUNT', 3, 'Machine')
Restart-Service -Name 'alsid_Eridanis' -Force
```

7. 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>

  <!--SYSMON EVENT ID 4 : RESERVED FOR SYSMON SERVICE STATUS MESSAGES-->
  <!--Cannot be filtered.-->

  <!--SYSMON EVENT ID 5 : PROCESS ENDED [ProcessTerminate]-->
  <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 6 : 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 7 : 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 8 : REMOTE THREAD CREATED [CreateRemoteThread]-->
  <RuleGroup name="" groupRelation="or">
    <CreateRemoteThread onmatch="include">
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x1FFFFF</GrantedAccess>
    </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-->
      <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      <GrantedAccess>0x3FFFFFFF</GrantedAccess>
    </ProcessAccess>
  </RuleGroup>
</EventFiltering>
</Sysmon>
```
<RuleGroup groupRelation="and">
  <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
  <GrantedAccess>0x143A</GrantedAccess>
</Rule>
<!-- Detect process hollowing to LSASS-->
<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>
<!-- Detect process injection to LSASS-->
<Rule groupRelation="and">
  <TargetImage name="technique_id=T1055,technique_name=Process Injection" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
  <GrantedAccess>0x0820</GrantedAccess>
</Rule>
<Rule groupRelation="and">
  <TargetImage name="technique_id=T1055,technique_name=Process Injection" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
  <GrantedAccess>0x820</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>
  </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>
  </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>
  </FileCreateStreamHash>
</RuleGroup>
<!--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>
  </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>
  </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>
  </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>
  </FileDelete>
</RuleGroup>
</EventFiltering>
</Sysmon>