TENABLE.ad Directory Listener

Installation Procedure — TLS

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>2.5.0</td>
<td>23/10/2019</td>
<td>ALSID</td>
<td>Initial document</td>
</tr>
<tr>
<td>2.5.1</td>
<td>31/10/2019</td>
<td>ALSID</td>
<td>Fix password input</td>
</tr>
<tr>
<td>2.6.0</td>
<td>19/02/2020</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>2.7.0</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>0308/2021</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. Prerequisites 6

II. Installation procedure 8
   1. Install Directory Listener 8

III. Active Directory configuration 11
   1. General considerations 11
   2. Domain controller to monitor 12
   3. User account 12
   4. Access to specific Active Directory objects or containers 12
   5. Configuring the monitored infrastructure to support Tenable’s Indicator-of-Attack 13

IV. Annexes 19
   1. Optional Sysmon configuration file 19
I. **INTRODUCTION**

1. **Document objectives**

   This document is intended to help you perform a clean installation of Tenable’s on-premises solution in TLS Mode. The required component is the Directory Listener to target audited domains.

   Note: For many examples, the “E” partition letter will be used by default for data partitioning.

2. **Abbreviations**

   The following table lists the abbreviations used within 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:

**Figure 2: Network flow matrix**

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></td>
<td>Replication, User and Computer Authentication,</td>
<td>SMB, CIFS, SMB2, DFSN, LSARPC,</td>
<td>TCP/445</td>
</tr>
<tr>
<td>Group Policy, Trusts</td>
<td>NbtSS, NetLogonR, SamR, SrvSvc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User and Computer Authentication, Forest Level Trusts</td>
<td>Kerberos TCP/88, TCP/464 and UDP/464</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User and Computer Authentication, Name Resolution, Trusts</td>
<td>DNS UDP/53 and TCP/53</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replication, User and Computer Authentication, Group Policy, Trusts</td>
<td>RPC, DCOM, EPM, DRSUAPI, NetLogonR, SamR, FRS TCP Dynamic (&gt; 1024)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory, Replication, User and Computer Authentication, Group Policy, Trusts</td>
<td>Global Catalog TCP/3268 and TCP/3269</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replication</td>
<td>RPC Endpoint Mapper TCP/135</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tenable Security probe</th>
<th>Tenable.ad SaaS platform</th>
<th>Tenable’s security probe TLS Tunnel</th>
<th>Advanced Message Queuing Protocol encrypted in TLS TCP/5671</th>
</tr>
</thead>
</table>

| End-users | Tenable.ad SaaS platform | Tenable’s end-user services (Web portal, REST API, etc.) | 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 -&gt; To)</th>
<th>Tenable’s usage (optional)</th>
<th>Type of traffic</th>
<th>Protocol and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email notifications</td>
<td>TCP/25, TCP/587, TCP/465, TCP/2525, TCP/25025</td>
<td>SMTP</td>
<td>TCP/25, TCP/587, TCP/465, TCP/2525, TCP/25025</td>
</tr>
<tr>
<td>Tenable.ad SaaS platform -&gt; Support services</td>
<td>(depending on the SMTP server’s configuration)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Syslog notifications</td>
<td>Syslog</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP/601, TCP/6515, UDP/514 (depending on the event log server’s configuration)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tenable REST API</td>
<td>TLS /HTTP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PKI infrastructure</td>
<td>HTTP/HTTPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP/80 or TCP/443</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity provider SAML server</td>
<td>TLS/HTTP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP/443</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity provider LDAP</td>
<td>LDAP/LDAPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP/389 and TCP/636</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity provider OAuth</td>
<td>HTTPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP/443</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. Prerequisites

4.1. Minimal configuration

The Tenable.ad_On-Premise_technical_prerequisites_vX.X document describes the sizing requirements to run the solution. Running Tenable.ad on a configuration thinner than these prerequisites is not supported.

### Directory Listeners - Sizing Matrix

<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, at least 2.6 GHz</td>
<td>12 GB of RAM</td>
<td>30 GB</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
<td>1 Virtual Machine</td>
<td>4 cores, at least 2.6 GHz</td>
<td>16 GB of RAM</td>
<td>30 GB</td>
</tr>
<tr>
<td>50 001 - 75 000</td>
<td>1 Virtual Machine</td>
<td>4 cores, at least 2.6 GHz</td>
<td>24 GB of RAM</td>
<td>30 GB</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
<td>1 Virtual Machine</td>
<td>4 cores, at least 2.6 GHz</td>
<td>32 GB of RAM</td>
<td>30 GB</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
<td>1 Virtual Machine</td>
<td>8 cores, at least 2.6 GHz</td>
<td>32 GB of RAM</td>
<td>30 GB</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
<td>1 Virtual Machine</td>
<td>8 cores, at least 2.6 GHz</td>
<td>64 GB of RAM</td>
<td>30 GB</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
<td>2 Virtual Machines</td>
<td>8 cores, at least 2.6 GHz</td>
<td>64 GB of RAM</td>
<td>30 GB</td>
</tr>
</tbody>
</table>

4.2. 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 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 the ‘Alsid’ or ‘Tenable’ prefix on the data partition. Therefore, do not create folders starting with ‘Alsid’ or ‘Tenable’ on the data partition.

4.3. Install Binaries

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

To configure the TLS installation, another file containing all the required certificates is provided:

- certs.zip

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

⚠️ It is highly recommended to reboot all machines before starting a new installation.
**Deployment on Windows Server (Full-Desktop Experience)**

The installer binary must be placed in a valid location on each server to be set up. In the following example, on the Directory Listener TLS 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 folder" /></td>
</tr>
</tbody>
</table>

- Extended debug logging can be activated with the following command (replace the first path by your installer file location, and the second by your log file path):

  ```
  C:\Users\Administrator\Desktop\Tenable.ad_DL_v3.X.X 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 installer file location):

  ```
  C:\Users\Administrator\Desktop\Tenable.ad_DL_v3.X.X
  ```
II. INSTALLATION PROCEDURE

Tenable.ad provides an installer for the Directory Listener component but does not configure the host beyond what is necessary for the product to run. In particular, all the machine 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 Directory Listener

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

- Tenable component
  - Ceti

![Expert Mode: This configuration (TLS mode) requires checking the "Expert mode" box on the first installer window to display the additional features.]

The installation mechanism is fully automated through an installer file. To perform the installation, execute “Tenable.ad_DL_v3.X.X.exe” with full Local Administrator privileges, check “Expert mode” and click on the “Next” button.

On the next dialog, 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 DirectoryListener feature, you must select only this feature.
Once this is done, 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 drive letter is E. Then, click on the “Next” button.

![Features dialog on Directory Listener](image)

Indicate RabbitMQ’s public IP address communicated by Tenable in the dedicated field. Also put the correct port number before clicking on the “Next” button and install Tenable.ad.

![Security Engine Node settings dialog on DL install](image)
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 because we want to target only one DC. Then, click on the "Yes" radio button to enable the TLS mode and click on the "Next" button.

![Directory Listener settings dialog on DL install](image)

Enter the TLS configuration information and click "Next".

![TLS settings dialog on DL install](image)
Click on the “Browse” button and select the ZIP file communicated by the Tenable team before installation. You must type the password associated with the PFX certificate in the second field. Then, click on the “Next” button.

![Tenable.ad_D1L Setup](image1)

Click on “Install” to start the installation.

![Tenable.ad_D1L Setup](image2)

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

### III. **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 specifications\(^1\).

2. Domain controller to monitor

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

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

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

3. User account

Tenable.ad needs to 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 by a simple user, no secret attribute (credentials, password hashes or Kerberos keys) is accessed by Tenable’s platform.

In this way, Tenable encourages to create a service account that will be 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, it is recommended to use 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 to deploy a new GPO on the infrastructure to monitor using a PowerShell script provided by Tenable’s platform. This script needs to be run once per feature deployment and requires an administrative account to create a new GPO and link it to the organizational unit hosting the Domain Controllers of the monitored domain.

4. 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.

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>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 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>dsacl &quot;&lt;<strong>CONTAINER</strong>&gt;&quot; /takeownership</td>
</tr>
<tr>
<td>dsacl &quot;&lt;<strong>CONTAINER</strong>&gt;&quot; /g &lt;<strong>SERVICEACCOUNT</strong>&gt;:LCRP /I:T</td>
</tr>
</tbody>
</table>
```

In the previous table, `<__CONTAINER__>` refers to the container to grant access to. `<__SERVICEACCOUNT__>` 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. 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 (IOA) and is focused on how to configure the monitored Domain Controllers to retrieve the required ETW information and to forward them to Tenable.ad
platform. 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.

### 5.1. Tenable’s deployment script

To retrieve the required ETW information within Tenable’s platform, a unique system based on an agent-less solution has been designed. This solution extracts ETW insertion strings\(^2\) 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.
- 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](image)

**Configuration adaptations**

\(^2\) ETW insertion strings are the same information used by Windows to build its Event Logs
For each targeted domain, executing this Tenable deployment 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:

```
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 (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 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.</td>
</tr>
</tbody>
</table>

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, reachable at https://doc.alsid.app/.

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. 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.

---

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
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).

5.2. 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.

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. 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\(^6\), the following command will install Microsoft Sysmon on the current machine:

```
.\\Sysmon64.exe -accepteula -i C:\TenableSysmonConfigFile.xml
```

The configuration file is available at the end of this document, 1 Optional Sysmon configuration file - page, or on Tenable’s documentation portal\(^7\) 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:

```
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 commands will uninstall Sysmon from the current machine:

```
```


\(^6\) Sysinternals website: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

\(^7\) Tenable documentation portal: https://docs.tenable.com/Tenablead.htm
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?

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

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

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?

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**

```
gpresult /scope:computer /h gpo.html
```

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.
IV.  ANNEXES

1. 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="lsass" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      </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">
          <GrantedAccess>0x1FFFFF</GrantedAccess>
        </Rule>
        <Rule groupRelation="and">
          <GrantedAccess>0x1F1FFF</GrantedAccess>
        </Rule>
        <Rule groupRelation="and">
          <GrantedAccess>0x1010</GrantedAccess>
        </Rule>
        <Rule groupRelation="and">
          <GrantedAccess>0x143A</GrantedAccess>
        </Rule>
      </ProcessAccess>
    </RuleGroup>
  </EventFiltering>
</Sysmon>
```
<!-- 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>

<!-- 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>

<!-- SYSMON EVENT ID 16 : SYSMON CONFIGURATION CHANGE-->

<RuleGroup name="" groupRelation="or">
  <!--Cannot be filtered.-->
</RuleGroup>

<!-- 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>
</Sysmon>