1. Document contributors:

<table>
<thead>
<tr>
<th>Author</th>
<th>Qualification</th>
<th>Contact address</th>
</tr>
</thead>
<tbody>
<tr>
<td>TENABLE</td>
<td>Technical team</td>
<td>Support Community</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>1.0</td>
<td>01/12/2018</td>
<td>Luc DELSALLE</td>
<td>Initial document</td>
</tr>
<tr>
<td>1.1</td>
<td>07/01/2020</td>
<td>Luc DELSALLE</td>
<td>Deployment option</td>
</tr>
<tr>
<td>1.2</td>
<td>06/02/2020</td>
<td>Luc DELSALLE</td>
<td>Update for 2.7.0</td>
</tr>
<tr>
<td>1.3</td>
<td>01/01/2021</td>
<td>Luc DELSALLE</td>
<td>Update for 3.0.0</td>
</tr>
<tr>
<td>1.4</td>
<td>02/08/2021</td>
<td>TENABLE</td>
<td>Update for 3.1.0</td>
</tr>
</tbody>
</table>
CONTENTS

I. INTRODUCTION ........................................................................................................................................................................... 4

II. ARCHITECTURE........................................................................................................................................................................... 5

III. HOSTING SPECIFICATION ............................................................................................................................................................... 9
  1. General considerations................................................................................................................................................................. 9
  2. Deployment options ..................................................................................................................................................................... 9
  3. Required resources .................................................................................................................................................................... 12
  4. Maintenance and updates .......................................................................................................................................................... 16
  5. Integrating Tenable.ad into an Active Directory domain .................................................................................................... 17
  6. Technical summary .................................................................................................................................................................. 18

IV. NETWORK SPECIFICATIONS ......................................................................................................................................................... 19
  1. General considerations .............................................................................................................................................................. 19
  2. Bandwidth throttling ............................................................................................................................................................... 19
  3. Network flow matrix ............................................................................................................................................................ 20
  4. Technical summary ............................................................................................................................................................ 23

V. ACTIVE DIRECTORY CONFIGURATION ............................................................................................................................................. 24
  1. General considerations .............................................................................................................................................................. 24
  2. Domain controller to monitor .................................................................................................................................................. 24
  3. User account ........................................................................................................................................................................... 25
  4. Access to specific Active Directory objects or containers ................................................................................................ 25
  5. Configuring the monitored infrastructure to support Tenable’s Indicator-of-Attack ................................................................ 26
    5.1. Tenable’s deployment script ............................................................................................................................................... 26
    5.2. Microsoft Sysmon ............................................................................................................................................................. 28
    5.3. Problem with Advanced Audit Policy Configuration GPO precedence ........................................................................ 30
    5.4. Uninstalling Tenable’s module from the Domain Controllers ........................................................................................ 31
    5.5. Update Tenable’s module on the Domain Controllers ................................................................................................ 31
  6. Technical summary ............................................................................................................................................................ 32

VI. MANAGING APPLICATION ............................................................................................................................................................... 33
  1. General considerations .............................................................................................................................................................. 33
  2. Tenable web portal ............................................................................................................................................................... 33
    2.1 Supported Internet browsers configuration ...................................................................................................................... 33
    2.2 TLS server certificate ........................................................................................................................................................... 33
    2.3 Client authentication ........................................................................................................................................................... 34
  3. Connecting an event log collector .............................................................................................................................................. 34
  4. Email notifications (general purpose and alerts) .................................................................................................................... 35
  5. Tenable REST v3 API ............................................................................................................................................................... 36
  7. Technical summary ............................................................................................................................................................ 36

VII. OPTIONAL SYSMON FILE ............................................................................................................................................................. 37

VIII. TROUBLESHOOTING ................................................................................................................................................................. 40
  1. IOA script antivirus detection .................................................................................................................................................. 40
IX. PREREQUISITE CHECKLIST ........................................................................................................................................................................ 41
  1. General considerations ............................................................................................................................................................................ 41
  2. Checklist ............................................................................................................................................................................................ 41
I. INTRODUCTION

1. Purpose of the document

Tenable.ad provides real-time security monitoring for Microsoft Active Directory (AD) infrastructures. Leveraging a non-intrusive approach based on the AD replication process, Tenable empowers security teams for their audit, threat hunting, detection and incident response tasks.

This document details:

- The technical requirements to deploy and operate Tenable.ad as an On-Premise platform, disconnected from the Internet and managed by the customer’s localized teams (or a certified partner).
- The environment specifications (from a network and an application perspective).
- The tasks to perform before turning on security monitoring.

This document is intended to be jointly prepared and reviewed by Tenable (or its certified partners) and the customer’s technical teams, as it requires the validation of several architectures and technical propositions. Once validated, Tenable’s delivery team or its certified partners can assist the customer on site with the commissioning.

To subscribe to the replication flows and start their monitoring, Tenable.ad must contact standard directory APIs specified by Microsoft. The platform only requires communication with the Primary Domain Controller emulator (PDCe) with a regular user account (part of the “Domain Users” built-in group). The deployment of a new GPO is also required to activate the attack detection engine.

For the On-Premises architecture, Tenable.ad is packaged as an installer file for deployment on a Windows Server environment (such as Windows Server 2019) provided by the customers. From a network perspective, the Active Directory infrastructures to monitor must be reachable from the virtualization environment. This document details the recommended architecture and computing power.

In its default configuration, Tenable.ad does not require Internet access to run. However, one of the key services that Tenable provides is its continuous integration process to allow regular (and sometimes unplanned) release of new detection capabilities and features. Thus, we strongly recommend that you design a process that regularly upgrades the product as part of the initial deployment.

In addition to its Web application, Tenable.ad also offers native alerting features, the ability to design specific analysis flows bound to a SIEM platform and a REST API that can easily integrate into a cybersecurity ecosystem. Thus you need to authorize specific network protocols (such as Syslog, SMTP or HTTP).

This technical document details precisely all the prerequisites introduced above. The last section in the document includes a checklist to help you keep track of the remaining prerequisites to gather.

On behalf of the entire Tenable’s team, we are proud to have the opportunity to work with you.
II. ARCHITECTURE

1. General considerations

Tenable.ad – General architecture

The On-Premises architecture of Tenable.ad is a software package hosted in a dedicated Windows Server environment provided and managed by the customer.

The platform relies on several Windows services hosted on virtual machines (VMs). The number and sizing of these VMs are detailed in the section **Hosting specification**.

Tenable.ad is powered by three main categories of services:

- The directory listeners: working closely with the monitored domain controllers, the directory listeners receive real-time Active Directory flows and apply several treatments to decode, isolate, and correlate security changes.
- The security engine nodes: hosting analysis-related services, the security nodes support the Tenable security engine, internal communication bus, and end-user applications (such as the Web portal, the REST API or the alert notifier). This component is built upon different isolated Windows services.
- The storage managers: providing hot and cold storage support, the storage managers oversee serving data to the directory listeners and the security nodes. This component is the only one that must be persistent from an information-saving perspective. Internally, Microsoft MS SQL Server 2019 and InfluxDB are used to store internal data and configuration.

As a flexible and modern platform, Tenable.ad supports several deployment architectures to integrate easily into the most demanding security or business contexts. This document details the two main architectures that Tenable encourages customers to use. Tenable’s technical lead or certified partners remain at the customer’s disposal to design other tailor-made architectures if the centralized or distributed architecture proposed in this document does not match their specific expectations.
2. Architecture options

2.1. Centralized architecture

Using the centralized architecture, Tenable's services are hosted in a unique network zone. The main components (directory listeners, security engine nodes and storage managers) are working side-by-side and can communicate with each other without any network filtering.

To ensure proper network security, Tenable recommends that you secure this architecture by adding a firewall at the entrance of the zone. The ingoing and outgoing network flows are described in the Network flow matrix.

This architecture offers a comprehensive and easy to deploy environment.

- Each Tenable service is placed at the same logical place and is guarded by a unique firewall.
- Each service flow (Active Directory, end-users, alerts, etc.) goes through the same network equipment.
- This architecture makes the connection of new Active Directory domains easy as no service or additional configuration is required on the targeted domains.
The centralized architecture thus offers the best balance between manageability and security. This architecture is recommended for environments willing to ensure the best platform security. Despite all its advantages, the centralized architecture can be bandwidth consuming as it must transfer every Active Directory flow from the monitored domain controllers to the Tenable network zone.

2.2. Distributed architecture

With the distributed architecture, Tenable’s services are separated into several network zones.

- Tenable’s directory listeners are placed in the same network zone as the monitored domain controller.
- The security engine nodes and the storage managers are placed in a dedicated zone.

Tenable.ad – Distributed architecture

This architecture offers several advantages:

- Bandwidth reduction: Active Directory flows can be very intensive when monitoring large directories. By filtering relevant security changes and compressing the objects, the directory listeners reduce the bandwidth used by the platform.
- Better network filtering: An Active Directory infrastructure requires the use of numerous TCP and UDP ports, which can be leveraged during a cyberattack. Following the principle of least privilege, we recommend that you expose only these network ports when it is strictly necessary. By placing directory listeners in the same network zone as the domain controllers, Tenable.ad does not need to expose Active Directory ports to another network zone anymore.
- Isolated infrastructure: Specific contexts sometimes require a complete isolation of the Active Directory infrastructure from the rest of the Information System. Using the distributed architecture, Tenable’s platform only requires one ingoing and one outgoing network flow, which preserves the security of the isolated infrastructure.

To maintain good network security, Tenable’s directory listeners use a specific host-based firewall. Tenable also recommends using a specific firewall at the entrance of the zone hosting the security nodes and storage managers. The ingoing and outgoing network flows are described in the network flow matrix provided in Network flow matrix.
Despite its many advantages, the distributed architecture is more complex to deploy and to maintain, because it requires multiple network configurations in different network locations. This architecture is also less flexible since it requires the deployment of new directory listeners each time the customer wants to add a new domain to monitor. Hence, Tenable only recommends this architecture for highly sensitive environments requiring high-level network isolation.

3. Synthesis

**Supported architecture options**
- Centralized architecture (Tenable’s services are hosted in the same network zone)
- Distributed architecture (directory listeners are placed in the same network zone as the domain controllers, the other services of Tenable are hosted in another network zone)
- Tailor-made architecture (jointly defined with Tenable’s technical lead)

**Recommended architecture**
- Centralized architecture (Tenable’s services are hosted in the same network zone)

4. Technical summary

The following table summarizes the main takeaways about the architecture specification of the on-premises version of Tenable.ad.

**Technical Summary**
- Tenable.ad is available as a software packaged hosted in a dedicated Windows Server environment provided by the customer.
- The platform is made of three components: directory listeners, security engine nodes and storage managers.
- Two architectures can be used to deploy the product:
  - A centralized architecture where each of Tenable’s services is hosted in the same network zone.
  - A split architecture where Tenable’s Directory listeners are placed in the same network zone as the domain controllers. The security engine node and the storage manager components remain in another network zone.
- Tenable recommends using the centralized architecture for most deployments as it offers better flexibility and easy-to-achieve deployment.
III. HOSTING SPECIFICATION

1. General considerations

Tenable.ad acts as a software package hosted in a dedicated environment, provided, and managed by the customer. The environment needs to fulfill hosting specifications detailed in the following sections.

The product is deployed through an application package. This package needs to be deployed on top of a Windows operating system provided by the customer. Although potentially subject to side effects due to a non-certified system configuration, this approach offers the advantage of allowing the use of a master image validated by the client.

Once the platform is instantiated, Tenable.ad requires to be connected to the customer’s Active Directory infrastructures to initiate security monitoring. This section also covers the required network configuration to initiate security monitoring.

2. Deployment options

2.1. General considerations

Designed to seamlessly integrate itself into various information systems architectures, Tenable.ad can be deployed using an application package detailed in the following paragraphs.

2.2. Application package deployment

The only supported deployment approach relies on Tenable.ad’s deployment as an application package on top of an operating system provided by the customer.

The packages are pre-configured with the customer’s particularities and only contain Tenable services. Following Tenable requirements, the customer must provide the operating system’s master image where the application package will deploy.

Designed to integrate seamlessly into the most demanding environments, this deployment option allows maximum flexibility to customers and facilitates the product deployment because the system already fulfills each customer’s requirements.
However, several drawbacks must be considered. First, Tenable.ad will be installed on a system which has not been validated by Tenable’s development team. It could thus introduce unexpected side effects or performance drawbacks which will need to be investigated during deployment.

Tenable.ad has been designed as a micro-services architecture embedded into Windows services. These services have a dedicated purpose (storage, security analysis, application, etc.) and are all mandatories. Consequently, Tenable’s product may only be installed on operating systems supporting the micro-service paradigms.

The following table defines the operating systems which may be used to deploy Tenable’s product.

<table>
<thead>
<tr>
<th>Supported Microsoft Windows Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Windows Server 2016</td>
</tr>
<tr>
<td>● Windows Server 2019</td>
</tr>
</tbody>
</table>

Depending on the supported operating systems, some configurations must be avoided to allow the platform to run. Unsupported configurations are detailed in the following table. Please take into consideration that this knowledge base is not exhaustive.

<table>
<thead>
<tr>
<th>Currently known unsupported configurations when deploying Tenable as an application package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active anti-virus or EDR solution</td>
<td>Tenable’s platform requires intensive disk I/O. Using anti-virus and EDR may drastically decrease platform performances. An exception to allow Tenable services and data folder is required¹.</td>
</tr>
<tr>
<td>FIPS-compliant algorithms</td>
<td>For data privacy reasons, FIPS-compliant algorithms for encryption must not be activated.</td>
</tr>
<tr>
<td>Firewalling</td>
<td>Tenable services need to communicate with each other to offer reliable security monitoring. Local firewalling rules preventing outgoing traffic must be disabled. Local firewalling rules allowing incoming traffic on Tenable services must be granted².</td>
</tr>
<tr>
<td>Debug and backup privileges</td>
<td>During the installation process, Tenable’s platform requires the administrator account used for installation to have debug and backup privileges.</td>
</tr>
<tr>
<td>Service Accounts</td>
<td>Usage of service accounts must be allowed on the OS.</td>
</tr>
<tr>
<td>Erlang</td>
<td>HOMEDRIVE environment variable must NOT be customized. The PATHEXT environment variable must contain the .EXE and .BAT file extensions.</td>
</tr>
</tbody>
</table>

Deploying Tenable’s platform in a non-certified environment may create unexpected side effects. In particular, the deployment of third-party applications (such as a specific agent or daemon) in the master image may incur stability or performance issues. Tenable strongly recommends reducing the number of third-party applications to a minimum level.

Tenable’s platform requires local administrative rights to be functional. This level of access rights is required to ensure a proper service management. The credentials (e.g., the login and password) associated with the administrative account need to be communicated to the Tenable’s technical lead during the deployment process. When deploying a production environment, a password renewal process should be considered and jointly validated with Tenable’s technical lead.

¹ The supported hosting specifications are detailed in “Required resources”
² The required network configuration is detailed in “Network specifications”
As part of its upgrade program, Tenable frequently publishes updates to its systems to provide new detection capabilities and new product features. In an application package-based deployment, Tenable’s engineering team will only provide updates for its services. The customer will thus have to ensure a proper management of its operating systems, including the frequent deployment of security patches. Tenable micro-services architecture supports the immediate application of operating system patches.

The following table summarizes the actions required prior to a deployment.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosting specification</td>
<td>• Provide to Tenable’s technical lead the hosting specifications.</td>
</tr>
</tbody>
</table>
| Configuration review          | • Provide to Tenable’s technical lead the list of every third-party package installed on the system.  
• Provide to Tenable’s technical lead all the configurations made on the master image.  
• Provide to Tenable’s technical lead all the security hardening made on the master image.  
• Tenable’s technical team will review the provided information and inform the customer if configurations are required. |
| Network configuration         | • Reserve the resources and provide to Tenable’s technical lead the private IP addresses.                                                         |
| Access configuration          | • Reserve the resources and provide to Tenable’s technical lead the DNS name which will be used to access Tenable’s web portal.                   |
| Security configuration        | • Reserve the resources and provide to Tenable’s technical lead the TLS certificate (and its associated private key) which will be used to secure access to the web portal. |
| Platform configuration        | • Provide to Tenable’s technical lead the first name, family name and email addresses of the user accounts to create.  
• Provide to Tenable’s technical lead the IP address(es) and the domain name of each primary domain controller to monitor. |

3 Maintenance and update processes are described in “Maintenance and support services”
4 The supported hosting specifications are detailed in “Required resources”
2.3. Synthesis

**Supported deployment options**
- Application-based deployment (Tenable’s platform is installed on top of a system managed by the customer)

**Recommended deployment option**
- Application-based deployment (Tenable’s platform is installed on top of a system managed by the customer)

3. 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, storage services, and end-users.
- The storage manager provides 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. The volume can be computed using the following command line. This command line needs to be 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” needs to specify the Active Directory Domain Services instance to connect to. The value “dc.domain.com” needs to be replaced by the fully qualified domain name (FQDN) of the domain controller to use for counting.

After having collected the number of active users to monitor, the following sections will define the appropriate sizing requirements.

3.1. Directory Listeners sizing

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>
</tbody>
</table>
### 3.2. 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>
<tr>
<td>50 001 – 75 000</td>
<td>1 Virtual Machine</td>
<td>10 cores on 3 sockets</td>
<td>24 GB of RAM</td>
<td>300 GB (gold performance)</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
<td>1 Virtual Machine</td>
<td>12 cores on 4 sockets</td>
<td>32 GB of RAM</td>
<td>400 GB (gold performance)</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
<td>1 Virtual Machine</td>
<td>16 cores on 4 sockets</td>
<td>32 GB of RAM</td>
<td>400 GB (gold performance)</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
<td>1 Virtual Machine</td>
<td>16 cores on 4 sockets</td>
<td>64 GB of RAM</td>
<td>500 GB (gold performance)</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
<td>4 Virtual Machines</td>
<td>VM1: 8 cores on 2 sockets VM2: 12 cores on 4 sockets VM3: 16 cores on 4 sockets VM4: 16 cores on 4 sockets</td>
<td>VM1: 16 GB of RAM VM2: 32 GB of RAM VM3: 16 GB of RAM VM4: 32 GB of RAM</td>
<td>VM1: 1 TB VM2: 300 GB VM3: 100 GB VM4: 100 GB (Gold Performance)</td>
</tr>
</tbody>
</table>

### 3.3. Storage Manager sizing

As part of its security analysis, **Tenable.ad** requires to store the differences for each Active Directory change, no matter if this change comes from the Active Directory database or from the Sysvol network share. The Storage Manager component oversees storing these events in two databases: a Microsoft SQL Server instance and an InfluxDB instance.

Predicting the number of AD changes (named events in the product) to be stored 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 suggestions for two configurations:

- a **minimal** sizing that needs to be provided 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, but if you do not plan to monitor closely the platform and do not want to potentially grow disks in the future, use the recommended values.

Dealing with databases also imply to implement a specific disk layout to store the different database files and to ensure I/O performances compatible with the product’s activity.
This chapter 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 document includes two disks performance scenario. Just like the sizing, the minimal disk performances will cover the needs of most infrastructures. The recommended infrastructure offers better experience for large or very active AD infrastructures.

**Minimal and Recommended Computing Power**

<table>
<thead>
<tr>
<th>Storage managers – Minimal Computing Power Matrix</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Active AD users</td>
<td>Instance required</td>
</tr>
<tr>
<td>1 – 25 000</td>
<td>1 Virtual Machine</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
<td>1 Virtual Machine</td>
</tr>
<tr>
<td>50 001 - 75 000</td>
<td>1 Virtual Machine</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
<td>1 Virtual Machine</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
<td>1 Virtual Machine</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
<td>1 Virtual Machine</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
<td>1 Virtual Machine</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Storage managers – Recommended Computing Power Matrix</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Active AD users</td>
<td>Instance required</td>
</tr>
<tr>
<td>1 – 25 000</td>
<td>1 Virtual Machine</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
<td>1 Virtual Machine</td>
</tr>
<tr>
<td>50 001 - 75 000</td>
<td>1 Virtual Machine</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
<td>1 Virtual Machine</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
<td>1 Virtual Machine</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
<td>1 Virtual Machine</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
<td>1 Virtual Machine</td>
</tr>
</tbody>
</table>

**Supported and Recommended Disk Layout**

The installer requires three disks:

- 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.

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Storage managers – Minimal Disk Sizing Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Total Disk Space</td>
</tr>
<tr>
<td>1 – 25 000</td>
<td>450 GB</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
<td>550 GB</td>
</tr>
<tr>
<td>50 001 - 75 000</td>
<td>800 GB</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
<td>1 TB</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
<td>2 TB</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
<td>3 TB</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
<td>4 TB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Storage managers – Recommended Disk Sizing Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Total Disk Space</td>
</tr>
<tr>
<td>1 – 25 000</td>
<td>600 GB</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
<td>800 GB</td>
</tr>
<tr>
<td>50 001 - 75 000</td>
<td>1.2 TB</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
<td>2 TB</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
<td>4 TB</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
<td>6 TB</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
<td>8 TB</td>
</tr>
</tbody>
</table>

Minimal and Recommended Disk Performances

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).

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Storage managers – Disk Performance Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Minimal Disk Performance</td>
</tr>
<tr>
<td></td>
<td>Throughput (MB/sec)</td>
</tr>
<tr>
<td>1 – 25 000</td>
<td>150</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
<td>200</td>
</tr>
<tr>
<td>50 001 - 75 000</td>
<td>200</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
<td>200</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
<td>250</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
<td>250</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
<td>500</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>Total:</td>
<td>60 150</td>
</tr>
</tbody>
</table>

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

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

4. Maintenance and updates

4.1. Upgrading Tenable.ad

As part of its upgrade program, Tenable frequently publishes updates to provide new detection capabilities and new features to its platform. These upgrades include security patches for the underlying operating system. These updates are published on a dedicated web portal. Access to the web portal is available upon request to the customer’s technical lead.

<table>
<thead>
<tr>
<th>Tenable’s release portal</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://www.tenable.com/downloads/">https://www.tenable.com/downloads/</a></td>
</tr>
</tbody>
</table>
Tenable will publish, for each update, the installer update packages which will need to be deployed on every Windows Server machine. The upgrade procedure is also available on the portal.

During maintenance operations, engineering teams will require administrative access to the operating systems hosting Tenable.ad.

### 4.2. Maintenance and support services

Because maintaining servers in good security conditions matters, Tenable’s platform must be allowed to contact several support services such as the update management infrastructure or the time service. The following table summarizes the support services required by Tenable’s platform. The required network flows are described in the corresponding section.

<table>
<thead>
<tr>
<th>Support services required to be connected to Tenable’s platform</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service name</strong></td>
</tr>
<tr>
<td>Update management infrastructure</td>
</tr>
<tr>
<td>Time Server</td>
</tr>
<tr>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>Identity provider</td>
</tr>
</tbody>
</table>

### 5. Integrating Tenable.ad into an Active Directory domain

Tenable.ad is using Microsoft Server operating systems to operate. These systems may be connected to an Active Directory domain. This chapter offers guidelines on the opportunity to interconnect or not these systems to a customer’s Active Directory domain.

As a platform offering sensitive security information, Tenable does not recommend joining the platform’s servers to any Active Directory domain. In fact, working on an isolated environment allows for a clear separation between the monitored perimeter and the monitoring entity (i.e., Tenable’s platform). In this configuration, an attacker having initial access or limited privileges on the monitored domain will not be able to directly access Tenable’s platform and its security analysis results.

If the customer is having a trustful infrastructure, operating Tenable.ad on domain-joined servers is fully supported. This approach will improve server management as it will be part of the regular process the customer is using for every domain-joined server. In particular, Tenable’s servers will apply the same hardening policies as any other corporate server. However, this architecture should be recommended only on secure Active Directory environments. In fact, in the case of an Active Directory compromise, the following risks will need to be taken into consideration:

- An attacker having server-administration privileges will be able to gather more information about ways to compromise the system using data analyzed by Tenable.ad.
● The administrative access granted to Tenable’s engineering team or its certified partners could be forbidden by the security policy on domain-joined servers.

● An attack may corrupt Tenable’s security monitoring by hiding a security incident.

| Supported Active Directory integration | • Tenable’s platform joined to an Active Directory domain
| • Tenable’s platform isolated from the customer’s Active Directory infrastructure |
| Recommended Active Directory integration | • Tenable’s platform isolated from the customer’s Active Directory infrastructure |

6. Technical summary

The following table summarizes the main takeaways about the hosting specifications of the on-premises version of Tenable.ad.

**Technical Summary**

- Tenable.ad is deployed as an application package.
- The sizing matrix uses the number of active AD users. Depending on the volume, different system requirements will need to be provided.
- Upgrade packages are delivered through a web portal.
- Tenable.ad needs to be connected to several support services such as update management infrastructure, time server and identity provider.
- Although supported, it is not recommended to integrate Tenable’s platform to an Active Directory domain.
IV. NETWORK SPECIFICATIONS

1. General considerations

Tenable.ad is a non-intrusive security monitoring platform able to identify breaches and detect attackers on an Active Directory infrastructure. In this way, the platform needs to be interconnected with the customer’s Active Directory infrastructures to initiate security monitoring. It requires some network flows to be allowed between the different services of the platform.

This section will cover the required network configurations and resources to connect the product and start the monitoring.

2. Bandwidth throttling

Acting as a monitoring platform, Tenable.ad will be receiving directory objects through time. Depending on the scale of the infrastructure, this process can generate a certain volume of data.

In this way, an appropriate bandwidth must be allocated to guarantee for the data to be transmitted to the analysis platform in a reasonable time frame. The following table defines the required bandwidth depending on the size of the monitored infrastructure. The number of active Active Directory user accounts will be used as the base metric.

<table>
<thead>
<tr>
<th>Active AD users count</th>
<th>Average number of objects received (per minute)</th>
<th>Minimum bandwidth speed</th>
<th>Recommended bandwidth speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – 5 000</td>
<td>10</td>
<td>1 Mbit/sec</td>
<td>2 Mbit/sec</td>
</tr>
<tr>
<td>5 001 – 75 000</td>
<td>150</td>
<td>5 Mbit/sec</td>
<td>10 Mbit/sec</td>
</tr>
<tr>
<td>75 001 – 400 000+</td>
<td>700</td>
<td>15 Mbit/sec</td>
<td>30 Mbit/sec</td>
</tr>
</tbody>
</table>
3. Network flow matrix

To achieve its security monitoring, Tenable.ad requires to reach the Primary Domain Controller emulator (PDCe) of each domain. On each PDCe, several network ports and transport protocols need to be opened to ensure an efficient monitoring.

In addition to these network flows, other communications need to be considered, such as:

- The access to the end-user’s services
- The network flows between the different services of Tenable’s platform
- The network flows from the support services used by Tenable.ad (e.g., the update management infrastructure, the network time protocol, etc.).

For clarity reasons, the network matrix shown below gives more details about the various services involved.
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>1 Tenable’s Directory</td>
<td>Directory, Replication, User and Computer Authentication, Group Policy, Trusts</td>
<td>LDAP/LDAPS</td>
<td>TCP/389 and TCP/636, ICMP/echo-request, ICMP/echo-response</td>
</tr>
<tr>
<td>Listeners -&gt; Domain</td>
<td>Replication, User and Computer Authentication, Group Policy, Trusts</td>
<td></td>
<td>TCP/445</td>
</tr>
<tr>
<td>controllers</td>
<td>User and Computer Authentication, Forest Level Trusts</td>
<td>Kerberos</td>
<td>TCP/88, TCP/464 and UDP/464</td>
</tr>
<tr>
<td></td>
<td>User and Computer Authentication, Name Resolution, Trusts</td>
<td>DNS</td>
<td>UDP/53 and TCP/53</td>
</tr>
<tr>
<td></td>
<td>Replication, User and Computer Authentication, Group Policy, Trusts</td>
<td>RPC, DCOM, EPM, DRSUAPI, NetLogonR, SamR, FRS</td>
<td>TCP Dynamic (&gt; 1024)</td>
</tr>
<tr>
<td></td>
<td>Directory, Replication, User and Computer Authentication, Group Policy, Trusts</td>
<td>Global Catalog</td>
<td>TCP/3268 and TCP/3269</td>
</tr>
<tr>
<td></td>
<td>Replication</td>
<td>RPC Endpoint Mapper</td>
<td>TCP/135</td>
</tr>
<tr>
<td>2 Tenable’s Directory</td>
<td>Tenable’s communication bus</td>
<td>Advanced Message Queuing Protocol</td>
<td>TCP/5671 and TCP/5672</td>
</tr>
<tr>
<td>Listeners -&gt; Tenable’s</td>
<td>Tenable’s internal API flows. (Optional)</td>
<td>TL/HTTP</td>
<td>TCP/443</td>
</tr>
<tr>
<td>Security engine nodes</td>
<td>Tenable’s end-user services (Web portal, REST API, etc.)</td>
<td>TLS/HTTP</td>
<td>TCP/443</td>
</tr>
<tr>
<td>3 End-users</td>
<td>Time synchronization</td>
<td>NTP</td>
<td>UDP/123</td>
</tr>
<tr>
<td>-&gt; Tenable’s Security</td>
<td>Update infrastructure (e.g., WSUS or SCCM)</td>
<td>HTTP/HTTPS</td>
<td>TCP/80 or TCP/443</td>
</tr>
<tr>
<td>engine nodes</td>
<td>PKI infrastructure</td>
<td>HTTP/HTTPS</td>
<td>TCP/80 or TCP/443</td>
</tr>
<tr>
<td></td>
<td>Identity provider SAML server</td>
<td>TLS/HTTP</td>
<td>TCP/443</td>
</tr>
<tr>
<td></td>
<td>Identity provider LDAP</td>
<td>LDAP/LDAPS</td>
<td>TCP/389 and TCP/636</td>
</tr>
<tr>
<td></td>
<td>Identity provider OAuth</td>
<td>TLS/HTTP</td>
<td>TCP/443</td>
</tr>
</tbody>
</table>
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>5 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></td>
<td>Tenable REST API</td>
<td>HTTP/TLS</td>
<td>TCP/443</td>
</tr>
</tbody>
</table>

Tenable does not recommend separating the Security Engine Nodes and the Storage Manager services on different networks to avoid performance issues. However, from a network perspective, this configuration is also supported. If the customer is willing to split the Security Engine Nodes and the Storage Managers into two different subnets, the following table should apply. If you are considering this option, please contact your designated technical lead.

<table>
<thead>
<tr>
<th>Network flows (From &lt;-&gt; To)</th>
<th>Tenable’s usage</th>
<th>Type of traffic</th>
<th>Protocol and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 Tenable’s Security engine nodes &lt;-&gt; Tenable’s Storage Managers</td>
<td>MS SQL Server database access</td>
<td>MS SQL queries</td>
<td>TCP/1433</td>
</tr>
<tr>
<td></td>
<td>InfluxDB Server database access</td>
<td>InfluxDB queries over HTTP</td>
<td>TCP/8086</td>
</tr>
</tbody>
</table>

**Note on RPC flows**

Windows RPCs are not firewall friendly. They dynamically determine which port is to be used once communication begins. Some firewalls have been known to try and extract ports information from RPC streams, which ultimately leads to better security and thus should be enabled. However, if the client's firewall does not understand RPCs and is forced to allow all RPCs ports, keep in mind that all Windows workstations also need those to connect to the AD infrastructure.

**Note on support services**

Support services are often highly vendor- or configuration-specific, making the given port list arguably less relevant than what we would wish for. For instance, the WSUS service is by default listening on TCP/8530 for its 6.2 version and higher, but on TCP/80 otherwise. And this port can be configured to anything else by an administrator.

**Note on NAT support**

Every network connection, except from the end-user, will be initiated by Tenable’s platform. Tenable’s platform can thus be NATed through network interconnection.
4. Technical summary

The following table summarizes the main takeaways about the network interconnection with Tenable’s product.

<table>
<thead>
<tr>
<th>Technical Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Tenable.ad requires to reach the Primary Domain Controller emulator (PDCe) of each domain to be monitored.</td>
</tr>
<tr>
<td>• Most organizations will require at least a 100 Mbit/s bandwidth to ensure Tenable’s platform to receive changes in a reasonable time frame.</td>
</tr>
<tr>
<td>• Standard, Microsoft-related network flows must be allowed between Tenable’s directory listeners and the Domain Controller to monitor.</td>
</tr>
<tr>
<td>• AMQP flows need to be open between Tenable’s directory listeners and Tenable’s security engine nodes.</td>
</tr>
<tr>
<td>• Standard application flows (TLS, HTTP) need to be open between the end-users and Tenable’s security engine nodes.</td>
</tr>
<tr>
<td>• Support flows (WSUS, NTP, etc.) need to be open to every Tenable’s component.</td>
</tr>
</tbody>
</table>
V. 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 Tenable’s ability to listen to SYSVOL event. A file is created in SYSVOL for each domain controller and its contents are flushed periodically.

To initiate security monitoring, Tenable.ad requires to contact standard directory APIs specified by Microsoft and documented in the MS-DRSR open specifications⁵.

![Tenable.ad – Functional architecture](image)

2. Domain controller to monitor

Tenable’s platform only requires communicating with the Primary Domain Controller emulator (PD Ce) using the network protocols described in *Network flow matrix*.

In case of multiple domains (or forests) being monitored by Tenable.ad, the PD Ce of each domain will need to 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, 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 able 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 an inherited 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:

| Active Directory objects or containers requiring manual read access setup |
|---|---|
| **Location of the container** | **Description** |
| CN=Deleted Objects, DC=<DOMAIN>, DC=<TLD> | Container hosting deleted objects |
| CN=Password Settings Container, CN=System, DC=<DOMAIN>, DC=<TLD> | [Optional] Container hosting Password Strategy Objects |

---

6 Administrative privileges are only required during the deployment of the Indicator-of-Attack feature.
For each of the above containers, Tenable requires to grant access to the service account used by the platform via the following command line:

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

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

Those commands need to be run on every domain monitored by Tenable’s platform.

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

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

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

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 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.

---

7 ETW insertion strings are the same information used by Windows to build its Event Logs
Configuration adaptations

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.

**Configuration changes**

- Add a GPO, named “Tenable.ad” by default, linked to the Domain Controllers OU by default. This GPO contains an immediate task configuring the PowerShell script running on each DC and installing a WMI filter that will start the PowerShell ETW script at boot, and the Advanced logging policy (see below).

- Activate the Microsoft Advanced logging policy, by modifying a registry key\(^8\) (using the GPO).

- Apply a new Event Log policy to force Domain Controllers to generate the ETW information required by Tenable’s IOAs.

- Install a WMI event consumer that will execute a VBS script (using the `ActiveScriptEventConsumer` class). This VBS script is run at boot and looks for a running PowerShell ETW script, which it will run if not found.

\(^8\) Specifically, the registry key is `MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy`, set to 1
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.

**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.

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

---

9 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)

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 Sysinternals website\(^\text{11}\), the following command will install Microsoft Sysmon on the current machine:

**Command line**

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

The configuration file is available at the end of this document, in *VII OPTIONAL Sysmon configuration file* - page, or on Tenable's documentation portal\(^\text{12}\) where the file is entirely commented. This Sysmon installation is not sufficient by itself and a registry key is needed for the WMI filters to be aware of Sysmon being installed:

**Command line**

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

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

**Command line**

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


\(^\text{12}\)
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’s needs, it will win and Tenable.ad will miss required events for attack detection.

---

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

---

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

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

Compare the output with the Tenable.ad advanced audit policy requirements\(^\text{13}\). 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".

---

\(^\text{13}\)
How to fix it?
If the effective policy is insufficient, it means that a GPO with a higher precedence defines conflicting settings. Look for GPOs linked to higher levels (Domain or Site) in Enforced mode that define Advanced Audit Policy Configuration.

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

<table>
<thead>
<tr>
<th>Command line</th>
</tr>
</thead>
<tbody>
<tr>
<td>gpresult /scope:computer /h gpo.html</td>
</tr>
</tbody>
</table>

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.

5.4. Uninstalling Tenable’s module from the Domain Controllers
In case of an uninstallation of Tenable’s product, the configuration can be rolled back using the Tenable’s deployment script.

To uninstall the audit policies, WMI filters and initial GPO, simply run the following command:

<table>
<thead>
<tr>
<th>Command line</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register-TenableIOA.ps1 -Uninstall</td>
</tr>
</tbody>
</table>

This command creates a new GPO, named “Tenable.ad cleaning” by default, that will be used to clean the previously installed GPO’s. The previous GPO and its SYSVOL files, including the registry setting the advanced logging policy, and the WMI filters will be cleaned.

If you had changed the initial GPO’s name, e.g. to comply to your naming conventions, you will have to pass it to the uninstall step too for the script to know which GPO to uninstall.

This new GPO also needs to be replicated over the entire domain, and the GPO refresh interval passed, for the uninstall process to be complete. Tenable recommends letting it run for a week, then simply manually removing this cleaning GPO.

5.5. Update Tenable’s module on the Domain Controllers
To update the Tenable’s IoA module, you must:

5. Uninstall the script currently in use by running it with the “-Uninstall” parameter
6. Wait a couple of hours so the cleaning GPO is properly replicated and applied by all domain controllers (at the time of writing, the script will enforce a 4-hour delay)
7. Delete manually the cleaning GPO
8. Download the new script version

9. Install it as explained above

6. Technical summary

<table>
<thead>
<tr>
<th>Technical Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Tenable.ad requires to access the Primary Domain Controller emulator (PDCe) of each monitored domain.</td>
</tr>
<tr>
<td>● The platform requires a regular service account that will be a member of the “Domain Users” group.</td>
</tr>
<tr>
<td>● Manual read access needs to be granted on specific containers.</td>
</tr>
<tr>
<td>● The authentication method for the service account must be a predefined user and password account. A password renewal process should be defined jointly between the customer and Tenable’s engineering team.</td>
</tr>
<tr>
<td>● Tenable’s Indicators-of-Attack require to run a one-time deployment script. Using a GPO, this script configures the Domain Controllers to provide meaningful ETW information in the Sysvol to be collected by Tenable.</td>
</tr>
<tr>
<td>● Some Indicators-of-Attack require Microsoft Sysmon to be deployed on the Domain Controllers.</td>
</tr>
</tbody>
</table>
VI. MANAGING APPLICATION

1. General considerations

Tenable.ad offers a complete set of services to review, manage and receive relevant information about the security state of the monitored infrastructure.

The platform is entirely manageable using its web portal displaying real-time information. In particular, the platform will display the live Active Directory security flows and allow security teams to achieve security compliance tasks, threat hunting or incident response tasks. The platform also includes all the administrative panels to manage the monitoring of new infrastructures. Using the fine-grained role-based access control implemented in the product platform, administrators will have the ability to manage the access rights of each user or service connected to the platform. More information about the platform can be found in the product’s official documentation.

Tenable’s platform also natively includes powerful notification and alerting features which can be connected to a large set of third-party services such as an event log collector (e.g., a SIEM), an email service provider (using SMTP) or a ticketing system. When a new security incident appears, Tenable’s platform can raise notifications (e.g., offenses) to inform security teams so that immediate actions can be taken. Tenable’s platform can also forward its refined security monitoring flows to other services for further correlation. Internal application logs (access, security, health check, etc.) can also be forwarded using various network protocols for archiving or security purposes.

Finally, Tenable’s platform can be easily integrated into a security ecosystem thanks to its RESTv3 API which exposes management, logging or notification capabilities. More information about the API specification can be found in Tenable’s online documentation.

2. Tenable web portal

2.1 Supported Internet browsers configuration

Tenable.ad offers a modern and lightweight web interface in charge of managing security monitoring and helping various security teams who are looking for meaningful security information.

As any modern application, Tenable’s portal does not require any specific configuration or plugin from client browsers. Built as a dynamic one-page app, it requires modern Internet browsers to provide a fluent experience.

<table>
<thead>
<tr>
<th>Supported</th>
<th>Web Browsers including minimum version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
<td>Edge version 38.14393 or Internet Explorer 11</td>
</tr>
<tr>
<td>Google</td>
<td>Chrome version 56.0.2924</td>
</tr>
<tr>
<td>Mozilla</td>
<td>Firefox version 52.7.3</td>
</tr>
<tr>
<td>Apple</td>
<td>Safari version 11.0</td>
</tr>
</tbody>
</table>

2.2 TLS server certificate

Privacy and security must be a major concern for sensitive applications such as Tenable’s web portal. Tenable thus requires the use of the SSL/TLS encryption mechanism to access its application.

---

14 Tenable’s online user and administrator documentation: [https://docs.tenable.com/Tenablead.htm](https://docs.tenable.com/Tenablead.htm)
Tenable strongly recommends using a valid certificate to prevent any man-in-the-middle attack. A valid certificate recognized by the customer's Certificate Authority should be provided by the customer to Tenable’s engineering team during the deployment.

| Supported TLS configuration and version | TLS 1.1 to TLS 1.3  
|                                       | Self-signed certificate provided by Tenable  
|                                       | Certificate issued from the customer’s private PKI  
|                                       | Alternative TLS certificate provided by the customer |

| Recommended TLS configuration and version | TLS 1.2  
|                                         | Certificate issued from the customer’s private PKI |

2.3 Client authentication

Tenable.ad supports several authentication methods to be used by end-users. These authentication methods have been designed to address most companies’ requirements. Tenable’s platform also supports multi-factor authentication.

| Supported Client authentication | Login and Password  
|                                | SAML  
|                                | LDAP |

| Recommended Client authentication | SAML authentication |

Please refer to Tenable’s online documentation to review the technical prerequisites and configurations to be activated inside Tenable’s portal to allow these authentication methods.

On the first connection, the login and password authentication mechanism will be the only one activated. A default account will be provided during the kick-off meeting by Tenable’s technical lead.

3. Connecting an event log collector

Tenable’s platform can be configured to send notifications (such as alerts or security offenses) to an event log collector. Leveraging Tenable decoding and filtering capabilities, the platform also offers the ability to redirect a subset of the traffic flows to a collector for further correlation.
Integrated process managing SIEM's events

Tenable.ad is using the Syslog protocol to carry messages formatted following the LEEF format. Using this approach, Tenable is supporting most of the SIEMs or event log collectors available in the market. The following table summarizes the platforms on which Tenable's solution has been successfully tested.

<table>
<thead>
<tr>
<th>Event log collectors successfully tested with Tenable’s platform (non-exhaustive list)</th>
</tr>
</thead>
<tbody>
<tr>
<td>● IBM QRadar</td>
</tr>
<tr>
<td>● Splunk</td>
</tr>
<tr>
<td>● RSA Netwitness</td>
</tr>
<tr>
<td>● LogRhythm</td>
</tr>
<tr>
<td>● Micro Focus ArcSight</td>
</tr>
<tr>
<td>● Tibco Loglogic</td>
</tr>
<tr>
<td>● McAfee Enterprise Security Manager</td>
</tr>
</tbody>
</table>

Please refer to Tenable’s online documentation to review the technical prerequisites and configurations to be activated inside Tenable’s portal to start event log forwarding and security alerts notification.

4. Email notifications (general purpose and alerts)

Tenable’s solution is using email notifications to send general purpose information to customers (such as password recovery information) but also notifications about security incidents.

In order to activate this feature, a user account allowed to send emails to the selected SMTP server needs to be provided in Tenable’s portal. This account can be the same account as the one used to connect to the Active Directory infrastructure.

Generic email template for a security incident detected by Tenable

Please refer to Tenable’s online documentation to review the technical prerequisites and configurations to be activated inside Tenable’s portal to trigger email notifications.

5. Tenable REST v3 API

Tenable.ad exposes a public API which may be used to connect the platform to third-party services. This API supports the REST (representational state transfer) v3 standard and is accessible using HTTP.

Most routes are authenticated and require a specific API token which may be retrieved inside Tenable’s portal.

Please refer to Tenable’s online documentation to review the technical prerequisites and configurations to be activated inside Tenable’s portal to use the API.

7. Technical summary

**Technical Summary**

- Tenable.ad can be managed through a web application or a REST API.
- The web application requires at least TLS 1.1. Tenable will provide a default server certificate, but the customer should create a dedicated one.
- Advanced authentication (e.g., SAML or LDAP) is offered by the platform.
- Security-related information (such as alerts, networking flows or application logs) can be sent using the syslog protocol and can be integrated in a SIEM.
- Email messages can be activated on the platform to send general purpose emails or to inform about an Active Directory security issue.
VII. OPTIONAL SYSMON FILE

```xml
<VII. OPTIONAL SYSMON FILE>

<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">
      <filecreate time onmatch="include">
        <!-- NOTE: Using "include" with no rules means nothing in this section will be logged -->
      </filecreate time>
    </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">
      <image load onmatch="include">
        <!-- NOTE: Using "include" with no rules means nothing in this section will be logged -->
      </image load>
    </rulegroup>

    <!-- SYSMON EVENT ID 8: REMOTE THREAD CREATED [CreateRemoteThread] -->
    <rulegroup name="" grouprelation="or">
      <createthread onmatch="include">
        <targetimage name="lsass" condition="is">C:\Windows\system32\lsass.exe</targetimage>
      </createthread>
    </rulegroup>

    <!-- SYSMON EVENT ID 9: RAW DISK ACCESS [RawAccessRead] -->
    <rulegroup name="" grouprelation="or">
  </sysmon>

```

<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]-->
<RouteGroup name="" groupRelation="or">
  <!-- Detect Access to LSASS-->
  <Rule groupRelation="and">
    <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    <GrantedAccess>0x1FFFFF</GrantedAccess>
  </Rule>
  <Rule groupRelation="and">
    <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    <GrantedAccess>0x1F1FFF</GrantedAccess>
  </Rule>
  <Rule groupRelation="and">
    <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    <GrantedAccess>0x1010</GrantedAccess>
  </Rule>
  <Rule groupRelation="and">
    <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    <GrantedAccess>0x143A</GrantedAccess>
  </Rule>
  <!-- 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 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>
</RuleGroup>

<!--SYSMON EVENT ID 11 : FILE CREATED [FileCreate]-->
<RouteGroup name="" groupRelation="or">
  <Rule groupRelation="and">
    <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    <GrantedAccess>0x1FFFFF</GrantedAccess>
  </Rule>
  <Rule groupRelation="and">
    <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    <GrantedAccess>0x1F1FFF</GrantedAccess>
  </Rule>
  <Rule groupRelation="and">
    <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    <GrantedAccess>0x1010</GrantedAccess>
  </Rule>
  <Rule groupRelation="and">
    <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    <GrantedAccess>0x143A</GrantedAccess>
  </Rule>
  <Rule groupRelation="and">
    <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    <GrantedAccess>0x0800</GrantedAccess>
  </Rule>
  <Rule groupRelation="and">
    <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    <GrantedAccess>0x800</GrantedAccess>
  </Rule>
  <Rule groupRelation="and">
    <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    <GrantedAccess>0x143A</GrantedAccess>
  </Rule>
  <Rule groupRelation="and">
    <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    <GrantedAccess>0x0800</GrantedAccess>
  </Rule>
  <Rule groupRelation="and">
    <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
    <GrantedAccess>0x800</GrantedAccess>
  </Rule>
</RuleGroup>

<!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
<!--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-->
<!--Cannot be filtered.-->

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

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

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

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

</EventFiltering>
</Sysmon>
VIII. TROUBLESHOOTING

1. IOA script antivirus detection

Most security best practices advise against installing antivirus/EPP/EDR software on domain controllers (or any other tool with a central management console). However, if you choose to do it anyway, please note that your antivirus/EPP/EDR might detect and even block or delete required items for IOA events collection on domain controllers.

Our script does not include malicious code, and it is not even obfuscated; but occasional detections are normal given our usage of PowerShell and WMI and the agentless nature of our implementation.

If you encounter issues with the IOA feature such as:

- Error messages during installation
- False-positive or false-negative in detection

Please review your antivirus/EPP/EDR security logs to check for any detection, blocking, or deletion of Tenable.ad components.

Below is a non-exhaustive list of components that could be affected:

- ScheduledTasks.xml file in the Tenable.ad GPO applied to domain controllers
- Tenable.ad scheduled task on domain controllers which launches powershell.exe

If you encounter such events, please follow the appropriate steps to add security exceptions in your tools for the concerned item(s).

In particular, Symantec Endpoint Protection is known to raise "CL.Downloader!gen27" detections during the IOA installation phase. In that case, you can add this specific known risk to your exceptions policy.
IX. PREREQUISITE CHECKLIST

1. General considerations

This final section gathers all the prerequisites previously detailed in this document and synthesizes them as a handy checklist that may be used to track the acquisition of those resources and configurations.

2. Checklist

<table>
<thead>
<tr>
<th>Items</th>
<th>Status</th>
<th>Customer Specifics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirmation of required agreements (NDA, Evaluation Software License), if applicable.</td>
<td>YES/N O</td>
<td></td>
</tr>
<tr>
<td>The type of architecture (centralized or split) has been chosen and has been communicated to Tenable's Technical Lead.</td>
<td>YES/N O</td>
<td></td>
</tr>
<tr>
<td>The number of active AD users into the targeted domains to monitor has been counted. This number has been communicated to Tenable's Technical Lead.</td>
<td>YES/N O</td>
<td></td>
</tr>
<tr>
<td>The computing and memory resources have been reserved following Tenable’s sizing matrix.</td>
<td>YES/N O</td>
<td></td>
</tr>
<tr>
<td>The subnet (/24) has been reserved for Tenable’s platform and has been communicated to Tenable’s Technical Lead.</td>
<td>YES/N O</td>
<td></td>
</tr>
<tr>
<td>The private IP of each virtual machine used to deploy Tenable’s platform has been communicated to Tenable’s Technical Lead.</td>
<td>YES/N O</td>
<td></td>
</tr>
<tr>
<td>The type and IP address of the update management infrastructure has been communicated to Tenable’s Technical Lead.</td>
<td>YES/N O</td>
<td></td>
</tr>
<tr>
<td>The type and IP address of the time server has been communicated to Tenable’s Technical Lead.</td>
<td>YES/N O</td>
<td></td>
</tr>
<tr>
<td>The type and IP address of the PKI server has been communicated to Tenable’s Technical Lead.</td>
<td>YES/N O</td>
<td></td>
</tr>
<tr>
<td>The type and IP address of the identity provider has been communicated to Tenable’s Technical Lead.</td>
<td>YES/N O</td>
<td></td>
</tr>
<tr>
<td>Required network flows have been opened for every service required by Tenable.ad.</td>
<td>YES/N O</td>
<td></td>
</tr>
<tr>
<td>The private IP addresses of each Primary Domain Controller emulator have been communicated to Tenable’s Technical Lead.</td>
<td>YES/N O</td>
<td></td>
</tr>
<tr>
<td>A regular user account has been created on each Active Directory forest to monitor.</td>
<td>YES/N O</td>
<td></td>
</tr>
<tr>
<td>On the specific Active Directory containers, access right has been granted to Tenable service account.</td>
<td>YES/N O</td>
<td></td>
</tr>
<tr>
<td>The domain user accounts information has been communicated to Tenable’s Technical Lead. Format: NetBIOSName\SamAccountName</td>
<td>YES/N O</td>
<td></td>
</tr>
<tr>
<td>A TLS certificate issued for Tenable’s Web Portal has been issued from the customer’s PKI and has been communicated to Tenable’s Technical Lead. If not, Tenable’s Technical Lead needs to be informed of the use of self-signed certificate.</td>
<td>YES/N O</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>YES/N O</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>The list of Tenable.ad user accounts to create has been communicated to Tenable’s Technical Lead. Required information: first and last name, email address and desired login.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The list of optional configurations to activate (email notification, Syslog event forwarding, etc.) has been communicated to Tenable’s Technical Lead.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A Project Lead on the customer’s side has been identified and will be available to validate common objectives with Tenable’s Customer Manager.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical staff on the customer’s side is identified and available to respond to potential technical issues (network filtering issue, PDCe unreachable, etc.).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>