TENABLE.AD
SAAS PLATFORM TECHNICAL PREREQUISITES

1. Document contributors:

<table>
<thead>
<tr>
<th>Author</th>
<th>Qualification</th>
<th>Contact address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Luc DELSALLE</td>
<td>Executive team</td>
<td><a href="mailto:hello@alsid.com">hello@alsid.com</a></td>
</tr>
</tbody>
</table>

2. Document history:

<table>
<thead>
<tr>
<th>Version</th>
<th>Date (dd/mm/yyyy)</th>
<th>Author</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01/12/2018</td>
<td>Luc DELSALLE</td>
<td>Initial document</td>
</tr>
<tr>
<td>1.1</td>
<td>21/07/2020</td>
<td>Luc DELSALLE</td>
<td>Update AD objects required access</td>
</tr>
<tr>
<td>1.2</td>
<td>01/12/2020</td>
<td>Luc DELSALLE</td>
<td>Update for Tenable.ad 3.0 release</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

I. Introduction .................................................................................................................................................. 3  
   1. Purpose of the document .......................................................................................................................... 3  
II. Platform interconnection ............................................................................................................................ 4  
   1. General considerations ............................................................................................................................. 4  
   2. Tenable Security Probe – Supported configuration and specification ................................................... 4  
   3. Tenable’s web portal configuration ......................................................................................................... 8  
   4. Network flow matrix ............................................................................................................................... 9  
   5. Technical summary .................................................................................................................................. 12  
III. Active Directory configuration .................................................................................................................. 13  
   1. General considerations ............................................................................................................................ 13  
   2. Domain controller to monitor .................................................................................................................. 14  
   3. User account .......................................................................................................................................... 14  
   4. Access to specific Active Directory objects or containers ....................................................................... 14  
   5. Configuring the monitored infrastructure to support Tenable’s Indicator-of-Attack ............................... 15  
   6. Technical summary ................................................................................................................................ 21  
IV. Managing application ................................................................................................................................. 22  
   1. General considerations ............................................................................................................................ 22  
   2. Tenable’s web portal ............................................................................................................................... 22  
   3. Connecting an event log collector ......................................................................................................... 24  
   4. Email notifications (general purpose and alerts) .................................................................................... 25  
   5. Tenable REST v3 API .............................................................................................................................. 25  
   6. Technical summary ................................................................................................................................ 26  
V. OPTIONAL Sysmon configuration file ......................................................................................................... 27  
VI. Global Architecture .................................................................................................................................... 29  
   1. General considerations ............................................................................................................................ 29  
VII. Prerequisite checklist ............................................................................................................................... 30  
   1. General considerations ............................................................................................................................ 30  
   2. Checklist ............................................................................................................................................... 30
1. 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 needed to deploy and operate **Tenable.ad** as a Software-as-a-Service (SaaS) platform managed by localized Tenable’s engineering teams. In particular, this document outlines the environment specifications (from a network and an application perspectives) and the tasks needed before turning security monitoring on.

**Tenable.ad** included two different modules that can be sold separately: the **Indicator-of-Exposure module** and the **Indicator-of-Attack module**. This guide will cover both modules deployment.

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 to validate several architectures and technical propositions. Once validated, Tenable’s delivery team (or its certified partners) will assist the customer on site with the commissioning.

To subscribe to the replication flows and start their monitoring, **Tenable.ad** requires to contact standard directory APIs specified by Microsoft. The platform only requires communicating with the Primary Domain Controller emulator (PDCe) with a regular user account (part of the "Domain Users" built-in group). In the SaaS architecture, Tenable will host a per-client dedicated platform on a cloud provider. This platform will be connected to the customer’s Active Directory using a lightweight application package acting as bridge between the corporate network and the cloud environment. Due to the specific nature of this connection, some specific network and filtering requirements will need to be made.

In addition to its Web application, **Tenable.ad** offers native alerting features, the ability to design specific analysis flows bound to a SIEM platform and a REST API to be easily integrated into a cybersecurity ecosystem. Specific network protocols (such as Syslog, SMTP or HTTP) thus need to be authorized.

This technical memento precisely details all the prerequisites introduced above. The last section in the document includes a checklist that will 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. PLATFORM INTERCONNECTION

1. General considerations

With a SaaS architecture, Tenable.ad acts as a dynamic platform hosted on a dedicated and secured environment, provided and managed by Tenable’s engineering team. Tenable is partnering with Microsoft so that Azure is the default cloud provider used to host customers’ platforms. However, Tenable develops an abstraction layer which allows the platform to be deployed on other providers (such as Amazon AWS, Google Cloud, Alibaba Cloud, Tencent Cloud, etc.). Please contact your designated technical lead if you are considering using an alternative cloud provider.

Once the platform is instantiated, Tenable.ad needs to be interconnected with the customer’s Active Directory infrastructures to initiate security monitoring. To that purpose, Tenable has designed a lightweight application package bridging the customer’s local Active Directory environment and the Tenable’s SaaS platform. Acting as a security probe, the application will filter Active Directory events to the ones related to security and forward them to the cloud environment through a mutually authenticated TLS tunnel.

This section will cover the required network configuration and resources to bridge the two environments using Tenable Security Probe.

2. Tenable Security Probe – Supported configuration and specification

2.1. General design

Tenable Security Probe bridges the customer’s local Active Directory infrastructure to the Tenable’s dedicated SaaS platform using an authenticated TLS 1.2 tunnel. Tenable Security Probe is deployed through an application package. This package needs to be deployed on top of an operating system provided by the customer. Although lightweight, Tenable Security Probe needs to fulfill hosting specifications detailed in the following sections.
Tenable Security Probe – Hosting architecture

Designed to seamlessly integrate into the most demanding environments, the Tenable Security Probe design allows maximum flexibility for customers and facilitates the product integration as it relies on a software running on an Operating System validated by customer’s system teams.

2.2. Hosting requirements

The Tenable Security Probe is a lightweight, resource-saving package designed to reduce at a minimal level its hosting requirements. The actual package’s size is less than 300MB. Following Tenable’s requirements, the customer must provide the operating system’s master image where the application package will be deployed. Tenable’s product has been designed to take the benefit of latest Operating System performance optimizations. It can be deployed on bare-metal or virtual environments. The following table defines the operating systems which may be used to deploy the Tenable Security Probe.

| Supported Microsoft Windows Operating Systems | • Windows Server 2016  
|                                               | • Windows Server 2019 |
| Supported GNU/Linux Operating Systems          | • None                |

Depending on the supported operating systems, some configurations must be avoided to allow the software 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>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
</tr>
<tr>
<td>Active anti-virus or EDR solution</td>
</tr>
<tr>
<td>FIPS-compliant algorithms</td>
</tr>
<tr>
<td>Firewalling</td>
</tr>
</tbody>
</table>

¹ The supported hosting specifications are detailed in “Hosting requirements” below
² The required network configuration is detailed in “Network flow matrix”
Deploying Tenable’s platform on 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.

The Tenable Security Probe only requires local administrative rights during the installation and maintenance phase. This level of access rights is required to set up the appropriate Windows Services and software’s watchdog to support failover. The credentials (e.g., the login and password) associated with the administrative account need to be communicated to 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.

As part of its upgrade program, Tenable frequently publishes updates to its systems to provide new detection capabilities and new product features. Tenable’s engineering team will provide updates for its Security Probe. The customer will have to ensure the deployment of every new version on the Operating System carrying the Tenable Security Probe. As part of a proper management of its operating systems, the customer will also be responsible for the frequent deployment any security patches at the Operating System level. Tenable supports the immediate application of operating system patches and supports unplanned appliance reboot.

2.3. Resources requirements

The Tenable Security Probe receives in real-time Active Directory flows. To ensure correct behavior, the software requires a certain amount of memory and computing power. Depending on the size of the Active Directory infrastructures to monitor, the deployment of multiple Tenable Security Probes may be required. As a metric, Tenable uses the number of Active Directory domain users to compute the number of instances to deploy.

After having collected the domains to monitor, the following table will define the appropriate sizing requirements.

<table>
<thead>
<tr>
<th>Tenable Security Probe - Sizing Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active AD users</td>
</tr>
<tr>
<td>1 - 25 000</td>
</tr>
<tr>
<td>25 001 - 50 000</td>
</tr>
<tr>
<td>50 001 - 75 000</td>
</tr>
<tr>
<td>75 001 - 100 000</td>
</tr>
<tr>
<td>100 001 - 150 000</td>
</tr>
<tr>
<td>150 001 - 300 000</td>
</tr>
<tr>
<td>300 001 - 500 001+</td>
</tr>
</tbody>
</table>

Notes

- The requirements described in the preceding tables are for the well-being of the Tenable Security Probe. They do not take into consideration the operating system requirements in case of an application package-based deployment.
- The + above means that Tenable needs to assess the requirements on a case-by-case basis if the number of domain users to monitor 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 requests for administration, monitoring, or any other reason.
2.4. Software Configuration

**Tenable Security Probe** packages are pre-configured with the customer’s Information System and Active Directory particularities. In order to instantiate the appropriate packages, Tenable Engineering team (or certified partners) will require the following information.

| Required information to generate tailor-made Tenable Security Probe package |
|--------------------------------------------------|--------------------------------------------------|
| Requirements                                      | Description                                      |
| IP of the Operating System hosting the Tenable Security Probe | Provide to Tenable’s technical lead the IP address of the Operating System hosting the Tenable Security Probe. |
| IPs of the domain controllers to monitor          | Provide to Tenable’s technical lead the exhaustive list of the Primary Domain Controller emulators to monitor. |
| Storage cache location                            | Provide to Tenable’s technical lead the path of the volume disk used to store Tenable Security Probe temporary cache. |

2.5. Security Consideration

Carried out by the **Tenable Security Probe**, the bridging between the on-premises Active Directory infrastructure of the customer and Tenable’s dedicated SaaS platform is achieved using an encrypted and fully authenticated **Transport Layer Security** tunnel.

Tenable is using a **high-standard encryption** profile and the latest officially supported version of TLS (TLS 1.2). The **confidentiality and integrity of the tunnel** is verified at all times using a server AND a client certificates issued by Tenable’s PKI. The encryption and signature algorithms are following security best practices.

The following table synthesizes the default configuration applied on Tenable’s TLS tunnel.

| Tenable’s TLS tunnel security configuration |
|---------------------------------------------|---------------------------------------------|
| TLS version                                 | 1.2                                         |
| Use of TLS Auth Key                         | Yes                                         |
| Symmetric cryptographic cipher              | AES-256-GCM                                 |
| Asymmetric cryptographic cipher             | RSA 2048                                    |
| Signature Algorithm                         | SHA-256                                     |
| Diffie-Hellman parameters size              | 2048                                        |

**Notes**

- In this section, no specific action is required by the customer. Tenable’s Engineering will provide all the necessary certificates and configuration in the **Tenable Security Probe** package.

2.6. 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 large volume of data to be transmitted by the **Tenable Security Probe**.

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.

---

3 The disk space specifications are detailed in “Hosting requirements”
### 3. Tenable’s web portal configuration

The management of **Tenable’s platform** is achieved using a flexible and dynamic **web application**. Both security monitoring and platform configuration are available through this interface. More information is available in **Error! Reference source not found.** on page **Error! Bookmark not defined.**

**Tenable’s web portal only accessible from the Internet**

Offering more flexibility, Tenable’s portal is reachable from the Internet but filtered to only authorize Customer’s legitimate users. In a nutshell, the web application flows will be routed to dedicated addresses exposed to the Internet while the Active Directory flows go through the TLS tunnel provided by the **Tenable Security Probe**.

The Web portal will be accessible using a **DNS name, part of the “alsid.app” domain**. Customers can freely choose the name they are willing to use to access the application, e.g., a valid DNS name would be: `https://contoso.alsid.app`. This information needs to be shared with Tenable’s team before the platform deployment.

In order to maintain a strong security boundary, Tenable’s security team recommends limiting access to the portal to a **limited set of whitelisted IPs**. By activating this mechanism, only a limited set of public IP addresses will be allowed to reach the portal and access the authentication form. In this configuration, the customer will have to communicate to Tenable’s team the exhaustive list of public IP addresses to allow. This list can be updated upon a simple request to Tenable’s support team.

---

**Supported Web portal configuration**

- Accessible from the Internet (using firewalling rules to allow access only from whitelisted IPs)
4. Network flow matrix

To achieve its security monitoring, the Tenable Security Probe requires reaching the Primary Domain Controller emulator (PDCes) of each domain to be monitored. On each PDCe, several network ports and transport protocols need to be opened to ensure an efficient monitoring. After having received the Active Directory events, the Tenable Security Probe requires to forward these events to the dedicated Tenable.ad SaaS platform using a TLS tunnel. Finally, the Tenable.ad SaaS platform requires to reach customers services, e.g. SIEM or SMTP servers, to raise alerts. End-users should also be able to connect to the Tenable.ad console to review the security analysis.

For clarity reasons, the network matrix shown below gives more details about the various services involved.

![Network flow matrix diagram](image)

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>
</table>
### Network flows (From -> To)

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

2. **Tenable Security Probe -> Tenable.ad SaaS platform**

Tenable’s security probe TLS Tunnel

Advanced Message Queuing Protocol encrypted in TLS

TCP/5671

3. **End-users -> Tenable.ad SaaS platform**

Tenable’s end-user services (Web portal, REST API, etc.)

TLS/HTTP

TCP/443

In addition to the Active Directory protocols, some additional flows may be required depending on Tenable’s platform configuration. These protocols and ports need to be opened between Tenable’s platform and the targeted service.

### Network flows (From <-> To)

<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>Email notifications</td>
<td>SMTP</td>
<td></td>
<td>TCP/25, TCP/587,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>TCP/465, TCP/2525,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>TCP/25025</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(depending on the SMTP server’s configuration)</td>
</tr>
<tr>
<td>Syslog notifications</td>
<td>Syslog</td>
<td></td>
<td>TCP/601, TCP/6515,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UDP/514</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(depending on the event log server’s configuration)</td>
</tr>
<tr>
<td>Tenable REST API</td>
<td>TLS/HTTP</td>
<td></td>
<td>TCP/443</td>
</tr>
<tr>
<td>PKI infrastructure</td>
<td>HTTP/HTTPS</td>
<td></td>
<td>TCP/80 or TCP/443</td>
</tr>
<tr>
<td>Identity provider SAML</td>
<td>TLS/HTTP</td>
<td></td>
<td>TCP/443</td>
</tr>
<tr>
<td>server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity provider LDAP</td>
<td>LDAP/LDAPS</td>
<td></td>
<td>TCP/389 and TCP/636</td>
</tr>
</tbody>
</table>

©2021 TENABLE. ALL RIGHTS RESERVED.
**Note on RPC flows**

Windows RPCs are not firewall-friendly. They dynamically determine which port is to be used once the communication begins. Some firewalls have been known to try and extract port 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 RPC ports, keep in mind that each Windows workstation also needs those to connect to the AD infrastructure.

**Note on NAT support**

Every network connection will be initiated by Tenable’s platform. Tenable’s platform can thus be NATed through network interconnections.
5. 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 platform is hosted by default on Microsoft Azure and managed by Tenable’s engineering team.</td>
</tr>
<tr>
<td>• The platform is connected to the customer’s infrastructure using the Tenable Security Probe.</td>
</tr>
<tr>
<td>• The Tenable Security Probe is a software package which should be installed on top of a Windows Server image provided by the customer.</td>
</tr>
<tr>
<td>• The Tenable Security Probe only requires connecting to the Primary Domain Controller emulator of each domain to monitor.</td>
</tr>
<tr>
<td>• Standard Microsoft-related network flows must be allowed between the Tenable Security Probe and the Domain Controllers to monitor.</td>
</tr>
<tr>
<td>• The Tenable Security Probe is connected to the Tenable.ad SaaS platform using a secure TLS tunnel provided by Tenable’s engineering team.</td>
</tr>
<tr>
<td>• The customer’s End-User will access Tenable’s Web portal through Internet. This access will be secured using encryption and IP filtering.</td>
</tr>
</tbody>
</table>
III. ACTIVE DIRECTORY CONFIGURATION

1. General considerations

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

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

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

To initiate security monitoring, **Tenable.ad** requires to contact standard directory APIs specified by Microsoft and documented in the MS-DRSR open specifications⁴.

---

2. Domain controller to monitor

Tenable’s platform only requires communicating with the Primary Domain Controller emulator (PDCe) using the network protocols described in Network flow matrix on page 9.

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

From a performance perspective, Tenable recommends hosting Tenable.ad SaaS platform on the same region than the PDCe to monitor. During the deployment process, the hosting region will be chosen by the customer’s engineering team in a joint effort with Tenable.

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

<table>
<thead>
<tr>
<th>Active Directory objects or containers requiring manual read access setup</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location of the container</td>
<td>Description</td>
</tr>
<tr>
<td>CN=Deleted Objects, DC=&lt;DOMAIN&gt;, DC=&lt;TLD&gt;</td>
<td>Container hosting deleted objects</td>
</tr>
<tr>
<td>CN=Password Settings Container, CN=System, DC=&lt;DOMAIN&gt;, DC=&lt;TLD&gt;</td>
<td>[Optional] Container hosting Password Strategy Objects</td>
</tr>
</tbody>
</table>
For each of the above containers, Tenable requires to grant access to the service account used by the platform via the following command line:

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

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

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

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

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

---

5 ETW insertion strings are the same information used by Windows to build its Event Logs
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.

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:

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

Synthesis of the technical changes made by Tenable’s deployment script

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

<table>
<thead>
<tr>
<th>Configuration changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Add a GPO, named “Tenable.ad” by default, linked to the Domain Controllers OU by default. This GPO contains an immediate task configuring the PowerShell script running on each DC and installing a WMI filter that will start the PowerShell ETW script at boot, and the Advanced logging policy (see below).</td>
</tr>
<tr>
<td>• Activate the Microsoft Advanced logging policy, by modifying a registry key(^\text{6}) (using the GPO).</td>
</tr>
</tbody>
</table>

\(^\text{6}\) Specifically, the registry key is `MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy`, set to 1
• Apply a new Event Log policy to force Domain Controllers to generate the ETW information required by Tenable’s IOAs.

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

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

More technical information describing step-by-step changes operated by Tenable deployment script is available on Tenable’s online documentation, reachable at https://doc.alsid.app

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

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

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

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

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

---

7 Microsoft documentation: https://docs.microsoft.com/en-us/windows/win32/etw/about-event-tracing#missing-events
8 Sysmon official website: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
Tenable understands that installing an additional Windows service and driver can affect performances of the Domain Controllers hosting the AD infrastructure. Therefore, **Tenable chooses not to automatically deploy Microsoft Sysmon.** It must be installed manually or by a dedicated GPO.

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

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

Once downloaded from the Sysinternal website\(^9\), the following command will install Microsoft Sysmon on the current machine:

**Command line**

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

The configuration file is available at the end of this document, in paragraph **V OPTIONAL Sysmon configuration file**, or on Tenable’s documentation portal\(^10\) 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**

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

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

**Command line**

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

---


\(^10\) Tenable documentation portal: [https://doc.alsid.app](https://doc.alsid.app)
5.3. Problem with Advanced Audit Policy Configuration GPO precedence

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

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

How to check?

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

<table>
<thead>
<tr>
<th>Command line</th>
</tr>
</thead>
<tbody>
<tr>
<td>auditpol.exe /get /category:*</td>
</tr>
</tbody>
</table>

Compare the output with the Tenable.ad advanced audit policy requirements\(^\text{11}\). 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".

\(^\text{11}\) [https://doc.alsid.app/v3.0.0/docs/understand-etw-data-retrieval-by-alsid](https://doc.alsid.app/v3.0.0/docs/understand-etw-data-retrieval-by-alsid)
How to fix?

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

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

<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, the WMI filter and the 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 can download the new script version and re-run the installation as explained above.
6. Technical summary

**Technical Summary**

- Tenable.ad requires to access the Primary Domain Controller emulator (PDCe) of each monitored domain.
- The platform requires a regular service account that will be a member of the “Domain Users” group.
- Manual read access needs to be granted on specific containers.
- The authentication method for the service account must be a predefined user and password account. A password renewal process should be jointly defined between the customer and Tenable’s engineering team.
- Tenable’s Indicator-of-Attack module requires 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.
- Some Indicators-of-Attack require Microsoft Sysmon to be deployed on the Domain Controllers.
IV. 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’s 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.

![Tenable.ad – Web interface](image-url)

---

12 Tenable online user and administrator documentation: [https://doc.alsid.app](https://doc.alsid.app)
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 Web Browsers including minimum version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>Google</td>
</tr>
<tr>
<td>Mozilla</td>
</tr>
<tr>
<td>Apple</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 application. Tenable thus requires the use of the SSL/TLS encryption mechanism to access its application.

Tenable strongly recommends using a valid certificate to prevent any man-in-the-middle attack. As part of the SaaS platform, a valid certificate will be provided by Tenable’s engineering team. This certificate will be signed by the Comodo certification authority.¹³

<table>
<thead>
<tr>
<th>Supported TLS configuration and version</th>
</tr>
</thead>
<tbody>
<tr>
<td>• TLS 1.1 to TLS 1.3</td>
</tr>
<tr>
<td>• Server certificate provided by Tenable as part of the SaaS platform</td>
</tr>
<tr>
<td>• Certificate issued from the customer’s private PKI</td>
</tr>
<tr>
<td>• Alternative TLS certificate provided by the customer</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recommended TLS configuration and version</th>
</tr>
</thead>
<tbody>
<tr>
<td>• TLS 1.2</td>
</tr>
<tr>
<td>• Server certificate provided by Tenable as part of the SaaS platform</td>
</tr>
</tbody>
</table>

### 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.

---

¹³ Comodo CA support page: [https://support.comodoca.com/Com_KnowledgeMainPage](https://support.comodoca.com/Com_KnowledgeMainPage)
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.

Integrating process managing SIEM’s events

Tenable.ad is using the Syslog protocol to carry messages formatted following the LEEF format⁴.

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>
<th>IBM QRadar</th>
<th>Splunk</th>
<th>RSA Netwitness</th>
<th>LogRhythm</th>
<th>Micro Focus ArcSight</th>
<th>Tibco Loglogic</th>
<th>McAfee Enterprise Security Manager</th>
</tr>
</thead>
</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.

New security risk on domain.local

You have received this email because you belong to Alsid for AD’s alert notification list.

Technical details

- Name: AdminCount attribute set on standard users (C-ADMINCOUNT-ACCOUNT-PR(OPS))
- Description: Some decommissioned administrative accounts are not globally manageable
- Score: 80 (25%)
- Severity: low
- Timestamp: Sun Oct 09 2016 02:21:15 GMT+0000 (Romania Daylight Time)

Security considerations

A sudden variation in an Indicator-of-Exposure state can be caused by a security incident or an administrative error. This alert should be carefully reviewed to assess its cause.

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.
6. Technical summary

<table>
<thead>
<tr>
<th>Technical Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Tenable.ad can be managed through a web application or a REST API.</td>
</tr>
<tr>
<td>• The web application requires at least TLS 1.1. Tenable will provide the server certificate.</td>
</tr>
<tr>
<td>• Advanced authentication (SAML or LDAP) is offered by the platform.</td>
</tr>
<tr>
<td>• 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.</td>
</tr>
<tr>
<td>• Email messages can be activated on the platform to send general purpose emails or to inform about an Active Directory security issue.</td>
</tr>
</tbody>
</table>
V. OPTIONAL SYSMON CONFIGURATION FILE

```xml
<sysmon schemaversion="4.40">
  <eventfiltering>
    <!-- SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
    <rulegroup name="" grouprelation="or">
      <processcreate onmatch="exclude">
        <!-- NOTE: Using "exclude" with no rules means everything in this section will be logged-->
      </processcreate>
    </rulegroup>

    <!-- SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHANGED IN THE FILESYSTEM [FileCreateTime]-->
    <rulegroup name="" grouprelation="or">
      <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-->
    <rulegroup name="" grouprelation="or">
      <reserved for sysmon service status messages>
        <!-- Cannot be filtered.-->
      </reserved for sysmon service status messages>
    </rulegroup>

    <!-- SYSMON EVENT ID 5 : PROCESS ENDED [ProcessTerminate]-->
    <rulegroup name="" grouprelation="or">
      <processterminate onmatch="exclude">
        <!-- NOTE: Using "exclude" with no rules means everything in this section will be logged-->
      </processterminate>
    </rulegroup>

    <!-- SYSMON EVENT ID 6 : DRIVER LOADED INTO KERNEL [DriverLoad]-->
    <rulegroup name="" grouprelation="or">
      <driverload onmatch="include">
        <!-- NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </driverload>
    </rulegroup>

    <!-- SYSMON EVENT ID 7 : DLL (IMAGE) LOADED BY PROCESS [ImageLoad]-->
    <rulegroup name="" grouprelation="or">
      <imageload onmatch="include">
        <!-- NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </imageload>
    </rulegroup>

    <!-- SYSMON EVENT ID 8 : REMOTE THREAD CREATED [CreateRemoteThread]-->
    <rulegroup name="" grouprelation="or">
      <createremotethread onmatch="include">
        <targetimage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</targetimage>
        <grantedaccess>0x1FFFFF</grantedaccess>
      </createremotethread>
    </rulegroup>

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

    <!-- SYSMON EVENT ID 10 : INTER-PROCESS ACCESS [ProcessAccess]-->
    <rulegroup name="" grouprelation="or">
      <processaccess onmatch="include">
        <!-- Detect Access to LSASS-->
        <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>0x100</grantedaccess>
        </rule>
        <rule grouprelation="and">
          <targetimage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</targetimage>
          <grantedaccess>0x43A</grantedaccess>
        </rule>
      </processaccess>
    </rulegroup>
  </eventfiltering>
</sysmon>
```
VI. GLOBAL ARCHITECTURE

1. General considerations

Tenable.ad has been built upon a micro-services architecture embedded into containers managed by Kubernetes. A resilient and secured networking infrastructure ensures fast and secure access to receive Active Directory flows and allows platform management.

The following diagram summarizes the Tenable.ad SaaS platform. The orange part symbolizes the customer’s information system, the blue part is entirely managed by Tenable.

---

Tenable.ad SaaS platform – Tenable Security Probe and web portal access
VII. 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/NO</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/NO</td>
<td></td>
</tr>
<tr>
<td>The computing and memory resources have been reserved following the sizing matrix of the Tenable Security Probe.</td>
<td>YES/NO</td>
<td></td>
</tr>
<tr>
<td>The IPs of the domain controllers to monitor and the IP address of the Tenable Security Probe have been communicated to Tenable’s Technical Lead.</td>
<td>YES/NO</td>
<td></td>
</tr>
<tr>
<td>Required network flows have been opened from the Tenable Security Probes to the Primary Domain Controller emulator of each domain to monitor.</td>
<td>YES/NO</td>
<td></td>
</tr>
<tr>
<td>Required network flows have been opened from the Tenable Security Probes to the Internet in order to bridge the traffic between the two environments.</td>
<td>YES/NO</td>
<td></td>
</tr>
<tr>
<td>Required network flows have been opened from the Tenable.ad dedicated platform to the Companies services willing to receive product’s alerts (SIEM, SMTP Server, etc.).</td>
<td>YES/NO</td>
<td></td>
</tr>
<tr>
<td>A DNS prefix for the Web Portal has been chosen and communicated to Tenable’s Technical Lead. URL format: <a href="https://__your-choice__.alsid.app">https://__your-choice__.alsid.app</a></td>
<td>YES/NO</td>
<td></td>
</tr>
<tr>
<td>The list of public IP addresses to authorize has been chosen and communicated to Tenable.</td>
<td>YES/NO</td>
<td></td>
</tr>
<tr>
<td>A regular user account has been created on each Active Directory forest to monitor.</td>
<td>YES/NO</td>
<td></td>
</tr>
<tr>
<td>On the specific Active Directory containers, access right has been granted to Tenable service account.</td>
<td>YES/NO</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/NO</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>YES/NO</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>YES/NO</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>YES/NO</td>
<td></td>
</tr>
<tr>
<td>Technical staff on the customer’s side is identified and available to respond to potential technical issues (VPN down, PDCe unreachable, etc.)</td>
<td>YES/NO</td>
<td></td>
</tr>
</tbody>
</table>