

TENABLE.AD

UPDATE PROCEDURE – TLS

a. Document contributors:

Author	Qualification	Contact address
TENABLE	DevOps team	support@alsid.com

b. Document history:

Version	Date (dd/mm/yyyy)	Author	Comments
2.4.0	12/07/2019	ALSID	Initial document
2.5.0	23/10/2019	ALSID	Update for 2.5.0
2.6.0	19/02/2020	ALSID	Update for 2.6.0
2.6.1	05/03/2020	ALSID	Update for 2.6.1
2.6.3	04/04/2020	ALSID	Update for 2.6.3
2.7.0	06/06/2020	ALSID	Update for 2.7.0
3.0.0.	01/12/2020	TENABLE	Update for 3.0.0

TABLE OF CONTENTS

I. Introduction	3
1. Document objectives	3
2. Abbreviations	3
3. Infrastructure presentation	3
4. Prerequisites	6
II. Update PROCEDURE	8
1. Update Directory Listener	8
2. Start Directory Listeners services	9
III. Active Directory configuration.....	10
1. General considerations.....	10
2. Access to specific Active Directory objects or containers.....	11
3. Configuring the monitored infrastructure to support Tenable's Indicator-of-Attack	11
IV. Annexes	18

I. INTRODUCTION

1. Document objectives

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

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

2. Abbreviations

The following table lists the abbreviations used in this documentation:

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

3. Infrastructure presentation

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

3.1. Network Overview

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

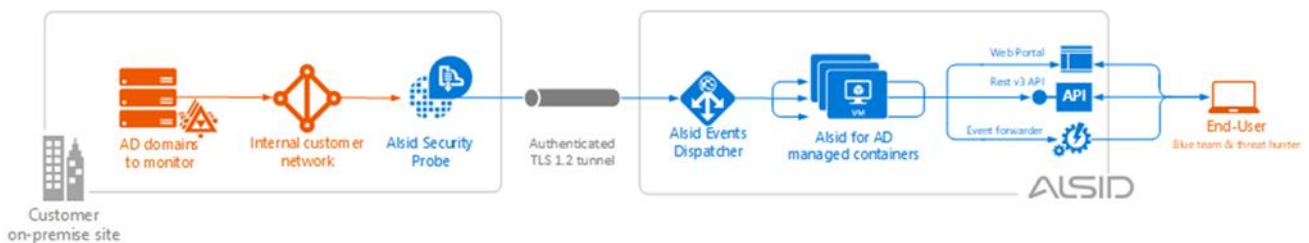


Figure 1: Network overview

To go further, please read the following schema and its associated network matrix. They describe each required protocol and port used by Tenable's platform:

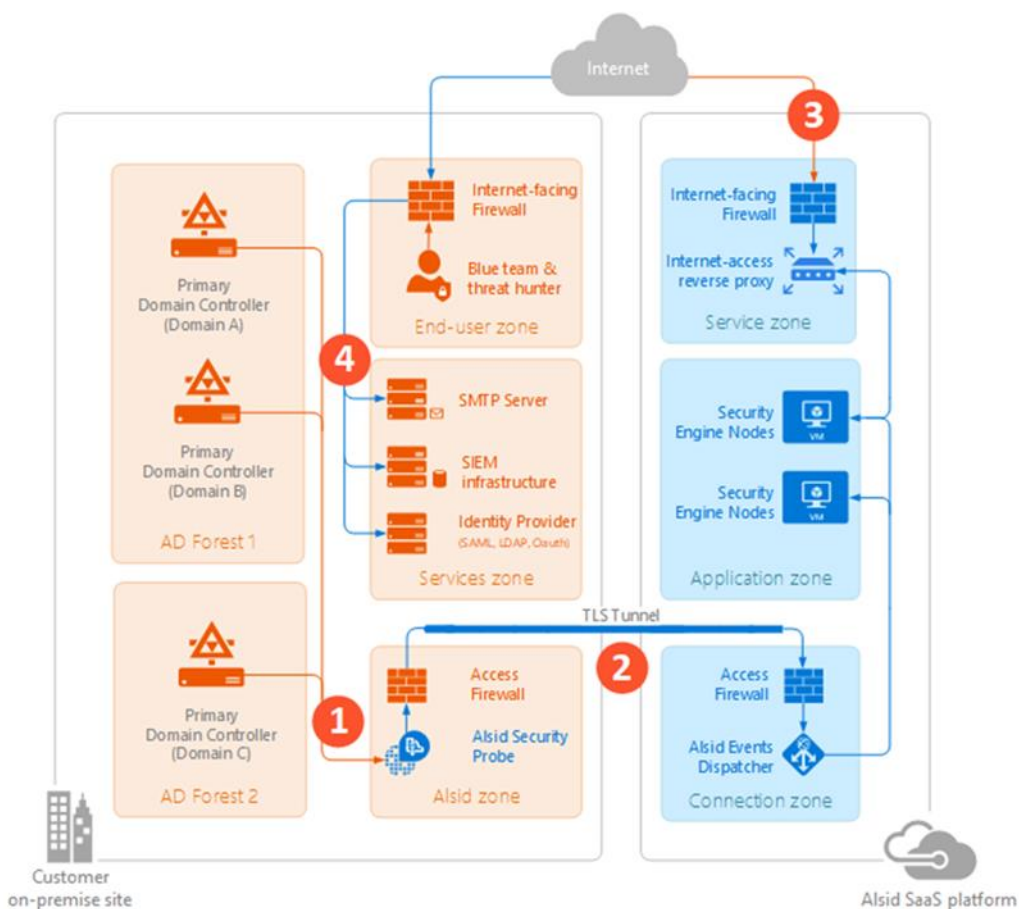


Figure 2: Network flow matrix

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

Network flows (From -> To)	Tenable's usage	Type of traffic	Protocol and Port
1 Tenable Security Probe -> Customer's Domain Controllers	Directory, Replication, User and Computer Authentication, Group Policy, Trusts	LDAP/LDAPS	TCP/389 and TCP/636 ICMP/echo-request ICMP/echo-response
	Replication, User and Computer Authentication, Group Policy, Trusts	SMB, CIFS, SMB2, DFSN, LSARPC, NbtSS, NetLogonR, SamR, SrvSvc	TCP/445
	User and Computer Authentication, Forest Level Trusts	Kerberos	TCP/88, TCP/464 and UDP/464
	User and Computer Authentication, Name Resolution, Trusts	DNS	UDP/53 and TCP/53
	Replication, User and Computer	RPC, DCOM, EPM, DRSUAPI,	TCP Dynamic (> 1024)

Network flows (From -> To)	Tenable's usage	Type of traffic	Protocol and Port
	Authentication, Group Policy, Trusts	NetLogonR, SamR, FRS	
	Directory, Replication, User and Computer Authentication, Group Policy, Trusts	Global Catalog	TCP/3268 and TCP/3269
	Replication	RPC Endpoint Mapper	TCP/135
<p>2</p> <p>Tenable Security probe -> Tenable for AD SaaS platform</p>	Tenable's security probe TLS Tunnel	Advanced Message Queuing Protocol encrypted in TLS	TCP/5671
<p>3</p> <p>End-users -> Tenable for AD SaaS platform</p>	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)	Tenable's usage (optional)	Type of traffic	Protocol and Port
<p>4</p> <p>Tenable for AD SaaS platform -> Support services</p>	Email notifications	SMTP	TCP/25, TCP/587, TCP/465, TCP/2525, TCP/25025 (depending on the SMTP server's configuration)
	Syslog notifications	Syslog	TCP/601, TCP/6515, UDP/514 (depending on the event log server's configuration)
	Tenable REST API	TLS /HTTP	TCP/443
	PKI infrastructure	HTTP/HTTPS	TCP/80 or TCP/443
	Identity provider SAML server	TLS/HTTP	TCP/443
	Identity provider LDAP	LDAP/LDAPS	TCP/389 and TCP/636

4. Prerequisites

4.1. Minimal configuration

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

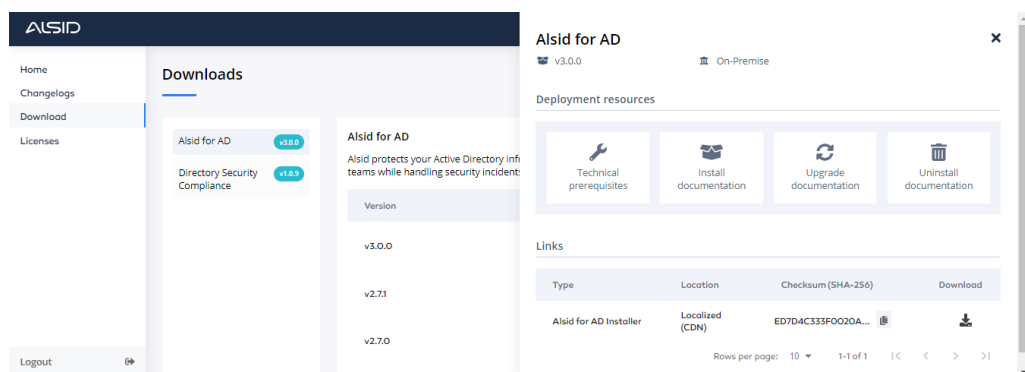
Tenable Security Probe - Sizing Matrix				
Active AD users	Instance required	vCPU (per instance)	Memory (per instance)	Disk space (per instance)
1 – 25 000	1 Virtual Machine	2 cores, at least 2.6 GHz	12 GB of RAM	30 GB
25 001 – 50 000	1 Virtual Machine	4 cores, at least 2.6 GHz	16 GB of RAM	30 GB
50 001 - 75 000	1 Virtual Machine	4 cores, at least 2.6 GHz	24 GB of RAM	30 GB
75 001 – 100 000	1 Virtual Machine	4 cores, at least 2.6 GHz	32 GB of RAM	30 GB
100 001 – 150 000	1 Virtual Machine	8 cores, at least 2.6 GHz	32 GB of RAM	30 GB
150 001 – 300 000	1 Virtual Machine	8 cores, at least 2.6 GHz	64 GB of RAM	30 GB
300 001 – 500 001+	2 Virtual Machines	8 cores, at least 2.6 GHz	64 GB of RAM	30 GB

4.2. Additional support information

- Tenable.ad works with Windows Server 2016 with the latest available update.
- Tenable.ad installer requires Local Administrator rights on Windows Server 2016. If the account used for the installation is not the built-in one, make sure that this account can run programs without restrictions.
- Tenable.ad services require Local Administrator rights to run local services on the machine.
- Tenable.ad requires a dedicated data partition. Tenable.ad must not be run on the OS partition to prevent system freeze if the partition is full.
- Tenable.ad must be considered as a black-box: Each machine must be considered as dedicated to the product and must not be shared for another purpose.
- Tenable.ad can create any folder starting with the 'Alsid' or 'Tenable' prefix on the data partition. Therefore, do not create folders starting with 'Alsid' nor 'Tenable' on the data partition.

4.3. Install binaries

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



Tenable.ad – Release portal

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

- certs.zip

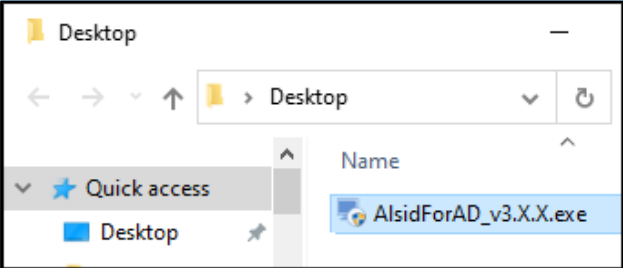
This package contains the files required to perform installation/uninstallation/update and to reconfigure the solution with different IP addresses (if needed).



It is highly recommended to reboot all machines before starting a new installation.

Deployment on Windows Server (Full-Desktop Experience)

The installer binary must be placed in a valid location on each server to be set up. In the following example, on the Directory Listener TLS machine, we put it on the Desktop:

Binaries location	Binaries content
C:\Users\Administrator\Desktop\	

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

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

Deployment on Windows Server Core

The installation mechanism is fully automated through an installer. To perform the installation:

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

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

II. UPDATE PROCEDURE

1. Update Directory Listener

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

- Tenable component
 - Ceti



Expert Mode: this configuration (TLS mode) requires checking the “Expert mode” box on the first installer window to display the additional feature.

The update mechanism is fully automated through an installer file. To perform the update, execute “*Tenable.ad_v3.X.X.exe*” with full Local Administrator privileges, check “*Expert mode*” and click on the “*Next*” button.

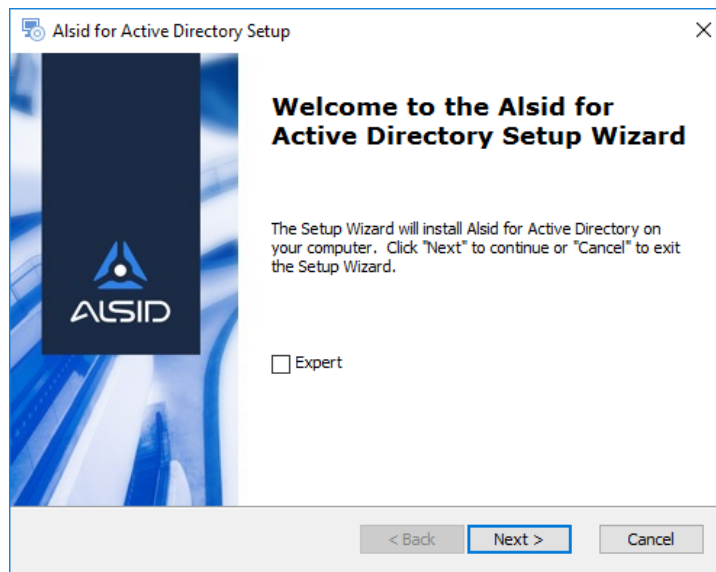


Figure 3: Welcome dialog on Directory Listener

On the next dialog, features and location are automatically preselected based on the previous installation. As mentioned just before, here you can see that only the **DirectoryListener** feature must be selected. Click on the “*Next*” button.

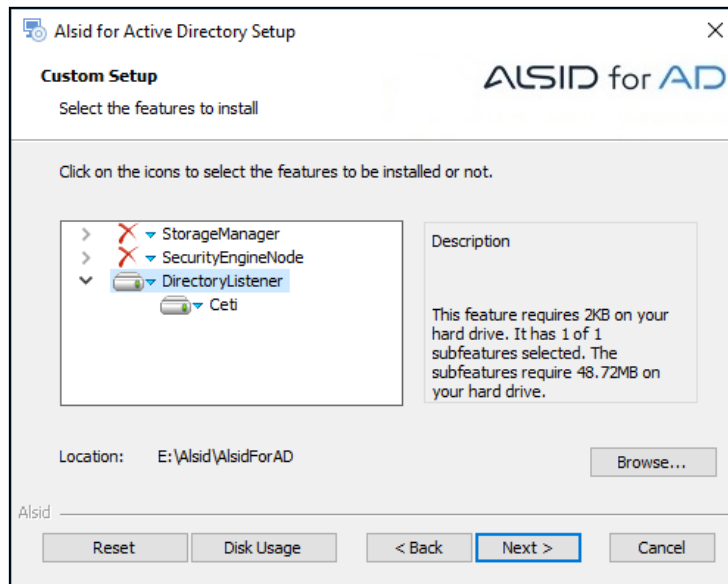


Figure 4: Features dialog on Directory Listener

RabbitMQ’s IP address is automatically filled based on the previous version. You can check if this is consistent, then click on the “Next” button and update Tenable.ad.

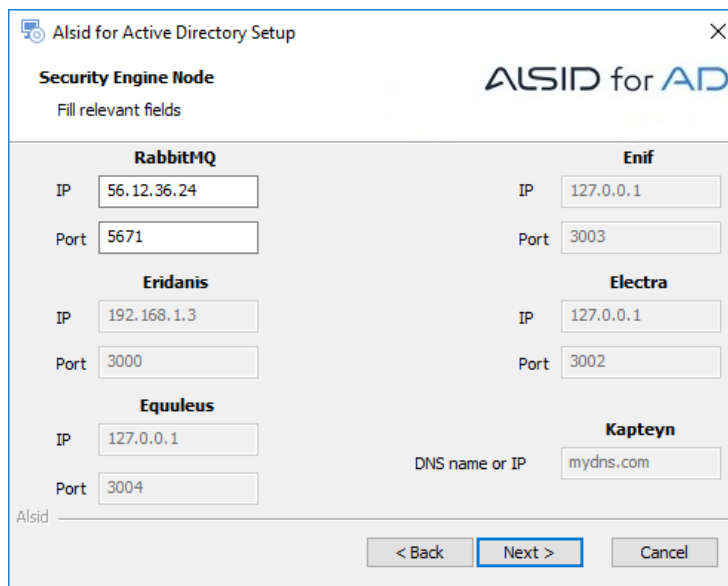


Figure 5: Security Engine Node settings dialog on DL update

At the end of the installation, **WAIT** until the server asks for a reboot. **Do NOT reboot it now!** Leave it like this for the moment and go to the next page.

2. Start Directory Listeners services

Databases and SEN must be running before starting DL services. Wait for the signal of Tenable DevOps team to reboot the machine and turn on the Ceti service.

III. ACTIVE DIRECTORY CONFIGURATION

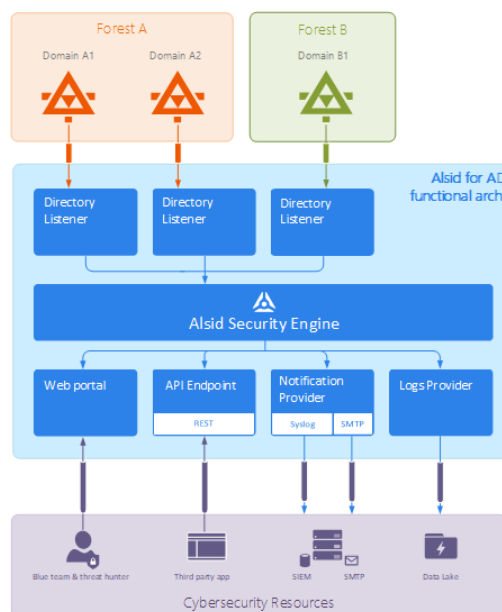
1. General considerations

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

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

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

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



Tenable.ad – Functional architecture

¹ Technical reference available on: <https://msdn.microsoft.com/en-us/library/cc228086.aspx>

2. Access to specific Active Directory objects or containers

Tenable's platform achieves its security monitoring without the need of administrative privileges. Despite its many advantages (operation safety, limited attack surface, etc.), this approach relies on the ability of the user account used by the platform to read all the Active Directory objects stored in a domain (including user accounts, organizational units, groups, etc.). This section only applies for the platform benefiting from the **Indicator-of-Exposure module**.

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:

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

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

Command line
<pre>dsacl " <__CONTAINER__>" /takeownership dsacl " <__CONTAINER__>" /g <__SERVICE_ACCOUNT__>:LCRP /I:T</pre>

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

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

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

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

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**.

3.1. 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 strings² data and forwards them, using a simple PowerShell script, to SYSVOL files. This approach only necessitates a one-time initialization step to:

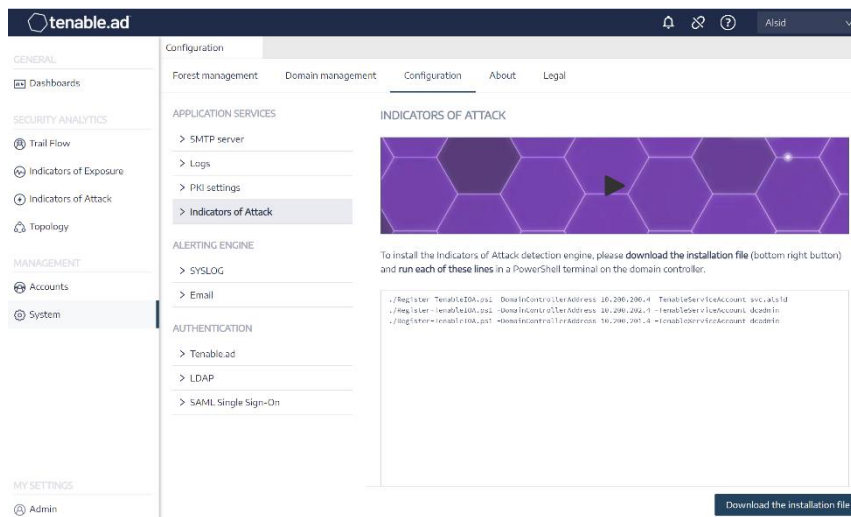
- Setup the PowerShell script to be executed.
- Configure the necessary audit policies.

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



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

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



Tenable.AD – Indicator-of-Attack setup view

² 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 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 key³(using the GPO).
- Apply a new Event Log policy to force Domain Controllers to generate the ETW information required by Tenable's IOAs.
- Install a WMI event consumer that will execute a VBS script (using the **ActiveScriptEventConsumer** class). This VBS script is run at boot and looks for a running PowerShell ETW script, which it will run if not found.

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

More technical information describing step-by-step changes operated by **Tenable deployment script** is available on Tenable's online documentation, 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.

³ Specifically, the registry key is `MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy`, set to 1

Tenable's incident detection module is based on the ETW data, thus bound by their limitations as defined by Microsoft⁴.

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

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

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

3.2. Microsoft Sysmon

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

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.

Indicators-of-Attack requiring Microsoft Sysmon	
Name of the indicator	Reason
OS Credential Dumping: LSASS Memory	Detecting Process Injection

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

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



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

⁴ Microsoft documentation: <https://docs.microsoft.com/en-us/windows/win32/etw/about-event-tracing#missing-events>

⁵ Sysmon official website: <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

Once downloaded from the Sysinternal website⁶, 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 in the annexes of this document or on Tenable's documentation portal⁷ 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:

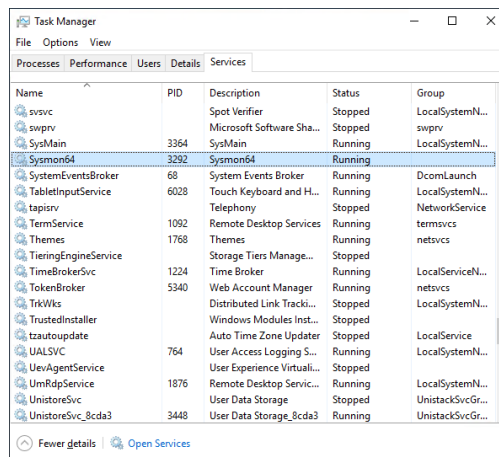
Command line

```
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"
```



Sysmon – Screenshot of a Domain Controller running Sysmon

⁶ Sysinternal website: <https://docs.microsoft.com/en-us/sysinternals/>

⁷ Tenable documentation portal: <https://doc.alsid.app>

3.3. Problem with Advanced Audit Policy Configuration GPO precedence

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



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

How to check?

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

Command line

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

Compare the output with the Tenable.ad advanced audit policy requirements⁸. For each setting required by Tenable.ad, ensure that the effective policy covers it, at least. This is also fine if the effective policy is more exhaustive, for example when Tenable.ad needs "Success" or "Failure" and the setting is "Success and Failure".

How to fix?

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

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

Command line

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

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

⁸ <https://doc.alsid.app/v3.0.0/docs/understand-etw-data-retrieval-by-alsid>

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

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

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

Then, check the new effective policy as instructed above.

3.4. Update Tenable's module on the Domain Controllers

To update the Tenable's IoA module, you can download the new script version and re-run the installation as explained above.



When updating, it is not necessary and even discouraged, to go through an uninstall phase before re-installing.

IV. ANNEXES

1. Optional Sysmon configuration 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">
      <FileCreateTime onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreateTime>
    </RuleGroup>

    <!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect]-->
    <RuleGroup name="" groupRelation="or">
      <NetworkConnect onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </NetworkConnect>
    </RuleGroup>

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

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

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

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

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

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

    <!--SYSMON EVENT ID 10 : INTER-PROCESS ACCESS [ProcessAccess]-->
    <RuleGroup name="" groupRelation="or">
      <ProcessAccess onmatch="include">
        <!-- Detect Access to LSASS-->
        <Rule groupRelation="and">
          <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
          <GrantedAccess>0x1FFFF</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>
</ProcessAccess>
</RuleGroup>

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

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

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

<!--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>

```