TENABLE.AD

SAAS PLATFORM TECHNICAL PREREQUISITES

1. Document contributors:

Author	Qualification	Contact address
Luc DELSALLE	Executive team	hello@alsid.com

2. Document history:

Version	Date (dd/mm/yyyy)	Author	Comments
1.0	01/12/2018	Luc DELSALLE	Initial document
1.1	05/02/2019	Antoine CAUCHOIS	Update VPN specs to IKE v 2
1.2	21/07/2020	Luc DELSALLE	Update AD objects required access
1.3	01/12/2020	Luc DELSALLE	Update for Tenable.ad 3.0 release

TABLE OF CONTENTS

I. Introduction 3

1. **Purpose of the document 3**

II. Platform interconnection 4

1. **General considerations 4**
2. **IPsec - Supported configuration 4**
3. **Cryptographic considerations 5**
4. **Bandwidth throttling 6**
5. **Tenable's web portal - Supported configuration 6**
6. **Network flow matrix 8**
7. **Technical summary 10**

III. Active Directory configuration 11

1. **General considerations 11**
2. **Domain controller to monitor 11**
3. **User account 12**
4. **Access to specific Active Directory objects or containers 12**
5. **Configuring the monitored infrastructure to support Tenable's Indicator-of-Attack 13**
6. **Technical summary 19**

IV. Managing application 20

1. **General considerations 20**
2. **Tenable's web portal 20**
3. **Connecting an event log collector 22**
4. **Email notifications (general purpose and alerts) 22**
5. **Tenable REST v3 API 23**
6. **Technical summary 24**

V. OPTIONAL Sysmon configuration file 25

VI. Global Architecture 27

1. **General considerations 27**
2. **Platform architecture when using a pure VPN-based access 27**
3. **Platform architecture when Tenable's web portal is accessible from the Internet 28**

VII. Troubleshooting 29

1. **IOA script antivirus detection 29**

VIII. Prerequisite checklist 30

1. **General considerations 30**
2. **Checklist 30**

I. INTRODUCTION

1. Purpose of the document

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

This document details the technical requirements 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-Attacks 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 and connect it to the customer's Active Directory using an IPsec VPN connection. Due to the specific nature of this connection, some specific network and filtering requirements will need to be made.

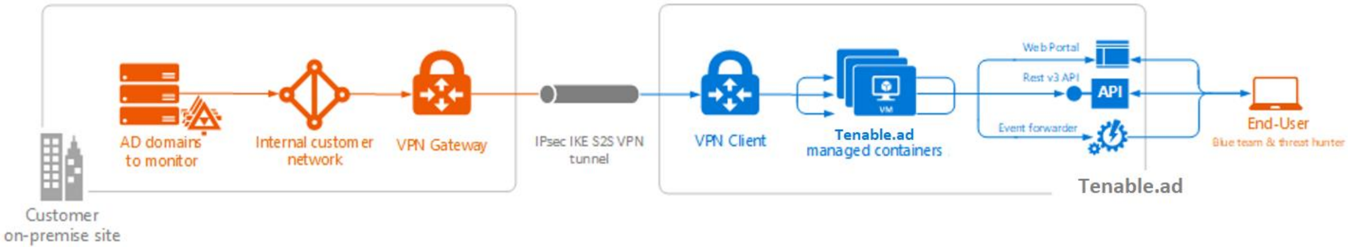
In addition to its Web application, Tenable.ad also offers native alerting features, the ability to design specific analysis flows bound to a SIEM platform and a REST API to be easily integrated into a cybersecurity ecosystem. Specific network protocols (such as Syslog, SMTP or HTTP) thus need to be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



Tenable.ad – General architecture

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.

This section will cover the required network configuration and resources to connect the product.

2. IPsec - Supported configuration

Several IPsec architectures can be used to establish the network tunnel between Tenable's platform and the customer's Active Directory infrastructures. Tenable supports site-to-site or inbound LAN interconnections.

Supported VPN technology	• IPsec L2TP, OpenVPN, Point-to-Point Tunneling protocol, Secure Socket Tunneling Protocol
Recommended VPN technology	• Site-to-Site IPsec L2TP (Layer Two Tunneling Protocol) connection

When using the recommended configuration (Site-to-Site IPsec connection), the concentrator crypto map should be configured to allow a /23 subnet to go through the tunnel, except (172.17.0.0/16, 172.30.0.0/16, 172.31.0.0/16, 192.0.2.0/24) dedicated for internal usage by Azure. In fact, Tenable's platform is using dynamic horizontal scaling which leads to the usage of multiple IP addresses to receive Active Directory flows.

VPN credentials should be provided to Tenable's engineering team before platform instantiation. The following authentication mechanisms are supported. In case the VPN uses two-factor authentication, a custom solution can be designed upon request.

Supported authentication types	• Pre-shared key for simple authentication • Certificate and private key for PKI-based authentication
Recommended authentication type	• Pre-shared key

Tenable.ad has been validated with the following devices configuration. Other configurations or devices will require to be evaluated by Tenable's engineering team and may require additional configuration.

Vendor	Device Family	Minimum OS Version	IKE Configuration
A10 Networks, Inc.	Thunder CFW	ACOS 4.1.1	IKEv2
Allied Telesis	AR Series VPN Routers	2.9.2	IKEv1
Barracuda Networks, Inc.	Barracuda NextGen Firewall F-series	5.4.3	IKEv1, IKEv2
Barracuda Networks, Inc.	Barracuda NextGen Firewall X-series	Barracuda Firewall 6.5	IKEv1
Brocade	Vyatta 5400 vRouter	Virtual Router 6.6R3 GA	IKEv1
Check Point	Security Gateway	R77.30	IKEv1, IKEv2
Cisco	ASA	8.3	IKEv1, IKEv2
Cisco	ASR	IOS 15.1	IKEv1, IKEv2
Cisco	ISR	IOS 15.0	IKEv1, IKEv2
Citrix	NetScaler MPX, SDX, VPX	10.1	IKEv1
F5	BIG-IP series	12.0	IKEv1, IKEv2
Fortinet	FortiGate	FortiOS 5.6	IKEv2
Internet Initiative Japan (IIJ)	SEIL Series	SEIL/X 4.60	IKEv1
Juniper	SRX	JunOS 10.2	IKEv1, IKEv2
Juniper	J-Series	JunOS 10.4r9	IKEv1, IKEv2
Juniper	ISG	ScreenOS 6.3	IKEv1, IKEv2
Juniper	SSG	ScreenOS 6.2	IKEv1, IKEv2
Microsoft	Routing and Remote Access Service	Windows Server 2012	IKEv2
Open Systems AG	Mission Control Security Gateway	N/A	IKEv1
Palo Alto Networks	All devices running PAN-OS	PAN-OS 6.1.5	IKEv1, IKEv2
ShareTech	Next Generation UTM (NU series)	9.0.1.3	IKEv2
SonicWall	TZ Series, NSA Series, SuperMassive Series, E-Class NSA Series	SonicOS 5.8.x	IKEv2
Sophos	XG Next Gen Firewall	XG v17	IKEv2
Ubiquiti	EdgeRouter	EdgeOS v1.10	IKEv2
WatchGuard	All	Fireware XTM v11.11	IKEv1, IKEv2

3. Cryptographic considerations

Tenable recommends using high-standard encryption when defining the security of the IPsec connection.

A site-to-site IPsec connection with ESP mode offers an appropriate security layer phase. During the negotiation phase, the use of IKE version 1 or version 2 is supported. However, our recommendation is to use IKE version 2.

Deprecated encryption algorithms (e.g., the MD5 hash function, the DES encryption algorithm, RSA keys smaller than 2,048 bits or ECDSA keys smaller than 200 bits) are not recommended but supported.

IKEv2 Phase 1	Recommended	Comments
Authentication method	Strong pre-shared key	***TO BE EXCHANGED BY SMS OR SIGNAL***
Encryption Algorithm	AES-256	We can support: - AES256, SHA1 - AES256, SHA256 - AES128, SHA1 - AES128, SHA256 - 3DES, SHA1 - 3DES, SHA256
Authentication Algorithm (hash function)	SHA-256	

Diffie-Hellman (DH) Group	2	We can support: - 1 - 2 - 14 - 19 - 20 - 24
IKE SA Lifetime	28 800 seconds	Cannot be changed

IKEv2 Phase 2	Recommended	Comments
Encryption Algorithm	AES-256	We can support: - AES256, SHA256, - AES256, SHA1, - AES128, SHA1, - 3DES, SHA1
Authentication Algorithm (hash function)	SHA-256	
IPSec SA Lifetime (Time)	27 000 seconds	Can be changed
IPSec SA Lifetime (Bytes)	102,400,000 KB	Can be changed
Perfect Forward Secrecy (PFS)	Equal to DH Group	We can support: - None - PFS1 (DH Group1) - PFS2 (DH Group 2) - PFS2048 (DH Group 14) - PFS24 (DH Group 24) - ECP256 (DH Group 19) - ECP384 (DH Group 20)
Dead-peer-detection keepalives	Supported	N/A

4. 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 in the VPN tunnel.

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.

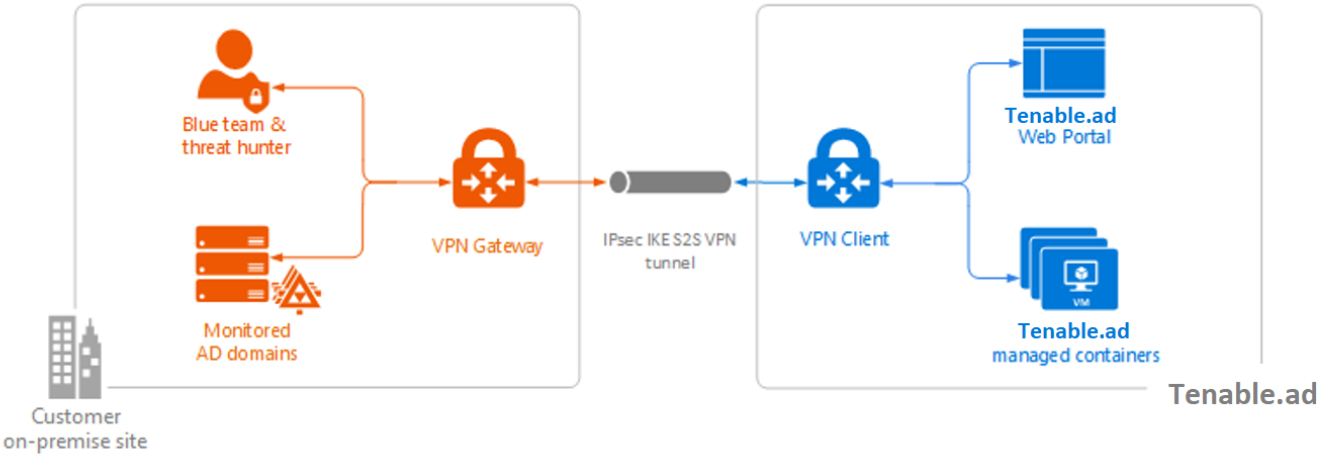
Active AD users count	Average number of objects received (per minute)	Minimum bandwidth speed	Recommended bandwidth speed
1 - 5 000	10	1 Mbit/sec	2 Mbit/sec
5 001 - 75 000	150	5 Mbit/sec	10 Mbit/sec
75 001 - 400 000+	700	15 Mbit/sec	30 Mbit/sec

5. Tenable's web portal - Supported 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 *Tenable's web portal* on page *20*.

Designed to seamlessly integrate itself into various information systems architectures, Tenable's portal can be deployed using two different configurations detailed in the following paragraph. The elected configuration needs to be communicated to Tenable's team to allow platform instantiation.

Despite their differences, the two configurations have been designed to offer the same high-level security boundaries to efficiently prevent illegitimate access.

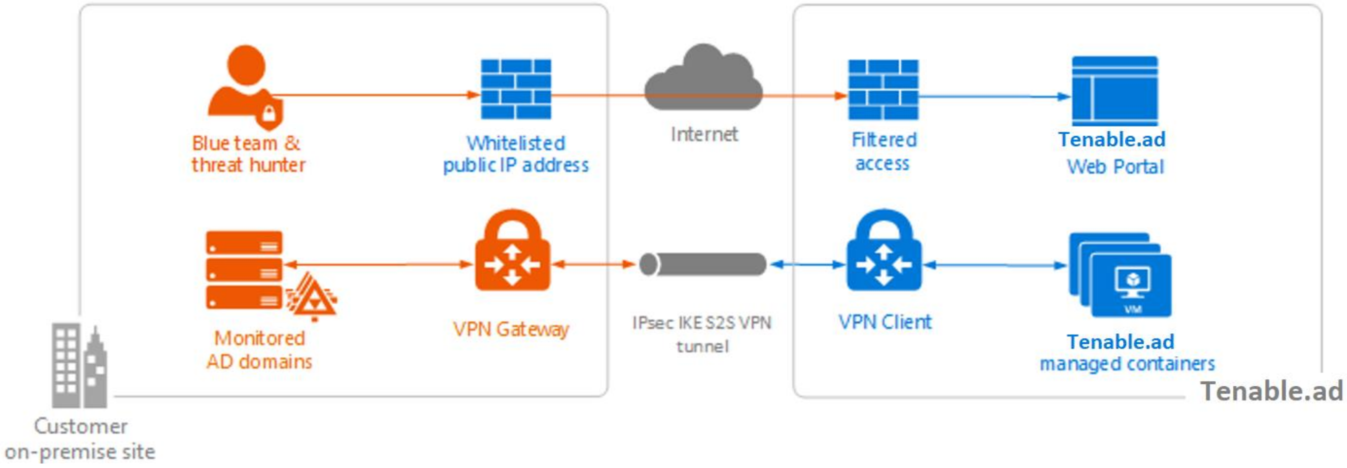


Tenable's web portal only accessible through the VPN tunnel

Acting as a pure remote enclave, this configuration enforces all the communication, including the one for the web portal, to go through the same IPsec VPN tunnel used to monitor the security of Active Directory domains. Except from the access used by Tenable's support team during the update and maintenance tasks, no Internet facing access is offered.

Presenting obvious security advantages from a data privacy perspective, this architecture could have several user-experience drawbacks. In case of an issue with the VPN connection, the platform will not be accessible at all. If the customer's network is built upon several physical locations, it may be difficult to offer peering between the local site and the customer's side of the VPN gateway.

Tenable's engineering team recommends this configuration for SMEs to mid-size organizations having strong data privacy regulations.



Tenable's web portal only accessible from the Internet

Offering more flexibility, this configuration allows Tenable's portal to be reachable from the Internet. The IPsec connection is still required to ensure security for the monitoring side, but only Active Directory flows will go through this tunnel. The web application flows will be routed to dedicated addresses exposed to the Internet.

In that configuration, each platform 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: *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.

Presenting a good balance between security and flexibility, Tenable's engineering team recommends this configuration in most cases.

Supported Web portal configuration	• Only accessible through VPN tunnel (pure VPN-based access) • Accessible from the Internet (using firewalling rules to allow access only from whitelisted IPs)
Recommended Web portal configuration	• Accessible from the Internet (using firewalling rules to allow access only from whitelisted IPs)

6. Network flow matrix

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

The following network matrix describes each required protocol and port used by Tenable's platform. These flows need to be opened between the PDCe to monitor and Tenable's monitoring platform.

Tenable's usage	Type of traffic	Protocol and Port	Destination
Directory, Replication, User and Computer Authentication, Group Policy, Trusts	LDAP/LDAPS	TCP/389 and TCP/636 ICMP/echo-request ICMP/echo-response	Primary Domain Controller emulator (PDCe)
Replication, User and Computer Authentication, Group Policy, Trusts	SMB, CIFS, SMB2, DFSN, LSARPC, NbtSS, NetLogonR, SamR, SrvSvc	TCP/445	Primary Domain Controller emulator (PDCe)
User and Computer Authentication, Forest Level Trusts	Kerberos	TCP/88, TCP/464 and UDP/464	Primary Domain Controller emulator (PDCe)
User and Computer Authentication, Name Resolution, Trusts	DNS	UDP/53 and TCP/53	Primary Domain Controller emulator (PDCe)
Replication, User and Computer Authentication, Group Policy, Trusts	RPC, DCOM, EPM, DRSUAPI, NetLogonR, SamR, FRS, DFS-R	TCP Dynamic (> 1024)	Primary Domain Controller emulator (PDCe)
Directory, Replication, User and Computer Authentication, Group Policy, Trusts	Global Catalog	TCP/3268 and TCP/3269	Primary Domain Controller emulator (PDCe)
Replication	RPC Endpoint Mapper	TCP/135	Primary Domain Controller emulator (PDCe)

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.

Tenable's usage (optional)	Type of traffic	Protocol and Port	Destination
Tenable Web Application	HTTP/TLS	TCP/443	Customer's end-users
Email notifications	SMTP	TCP/25, TCP/587, TCP/465, TCP/2525, TCP/25025	Customer's SMTP servers

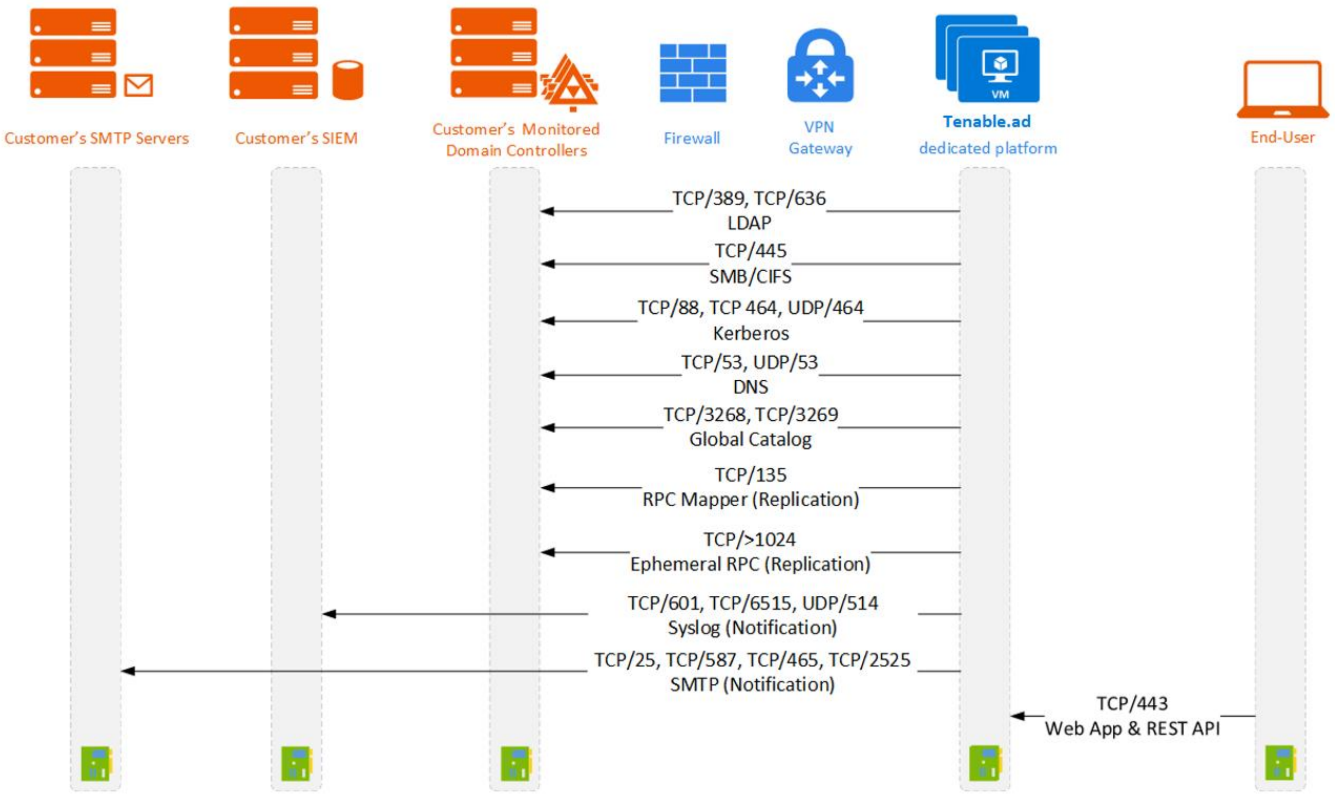
		(depending on the SMTP server's configuration)	
Syslog notifications	Syslog	TCP/601, TCP/6515, UDP/514 (depending on the event log server's configuration)	Customer's event log collector or SIEM
Tenable REST API	HTTP/TLS	TCP/443	Customer's end-user or third-party service provider

Note on RPC flows

Windows RPCs are not firewall-friendly. They dynamically determine which port is to be used once communication begins. Some firewalls have been known to try and extract 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 interconnection.



Network flows summary

7. Technical summary

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

Technical Summary
• Tenable.ad platform is hosted by default on Microsoft Azure and managed by Tenable's engineering team. The platform is connected to the client's infrastructure using a VPN connection. • A site-to-site IPsec connection must be established between Tenable's cloud and the customer's information system. • Tenable supports IPsec vendors for both IKE v1 and IKE v2. ESP mode should be used. • Tenable only requires connecting to the Primary Domain Controller emulator of each domain to monitor. • Standard, Microsoft-related network flows must be allowed between Tenable's platform and the Domain Controller to monitor.

III. ACTIVE DIRECTORY CONFIGURATION

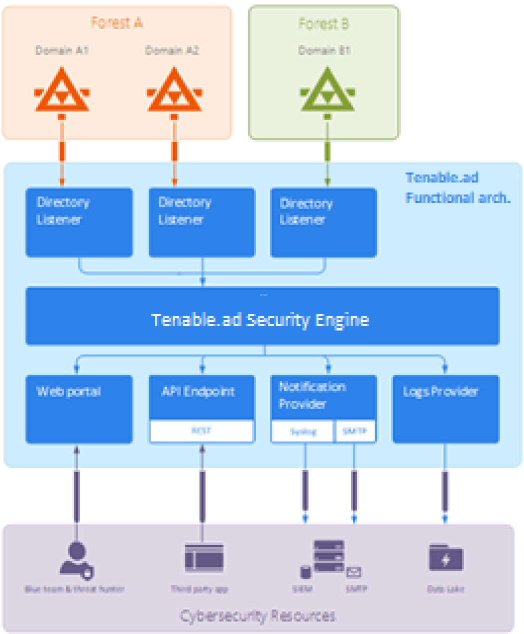
1. General considerations

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 specification[1].



Tenable.ad – Functional architecture

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 *8*.

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 to host 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.

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

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.

Note that there are rare cases where Tenable.ad cannot access some important Active Directory objects' attributes. This happens if Active Directory default permissions were significantly changed. In particular, if "Authenticated Users" was removed from the "Pre-Windows 2000 Compatible Access" group.

Missing data from those attributes leads to many issues: licensing (i.e. Tenable.ad cannot count correctly the active users only), dysfunctions in IOE/IOA options (e.g. Tenable.ad cannot ignore disabled users when configured), IOE/IOA false-positives and false-negatives (i.e. Tenable.ad cannot analyze security-wise the data it cannot collect), etc.

Check by browsing the Active Directory domain with the Tenable.ad service account and ensure that normal attributes are readable, especially: userAccountControl.

Reason preventing reading the attributes	Suggested action
"Authenticated Users" was removed from the "Pre-Windows 2000 Compatible Access" group, by error.	"Authenticated Users" can be re-added to the "Pre-Windows 2000 Compatible Access".
"Authenticated Users" was removed from the "Pre-Windows 2000 Compatible Access" group, on purpose.	The Tenable.ad service account can be added instead to the "Pre-Windows 2000 Compatible Access" group if it is acceptable as per your security policy.
Deny ACEs were added, or by default Allow ACEs were removed.	Study a specific workaround allowing Tenable.ad to read userAccountControl and other important attributes.

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:

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

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

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

5.1. Tenable's deployment script

To retrieve the required ETW information within Tenable's platform, a unique system based on an agent-less solution has been designed. This solution extracts ETW insertion strings[2] data and forwards them, using a simple PowerShell script, to SYSVOL files. This approach only necessitates a one-time initialization step to:

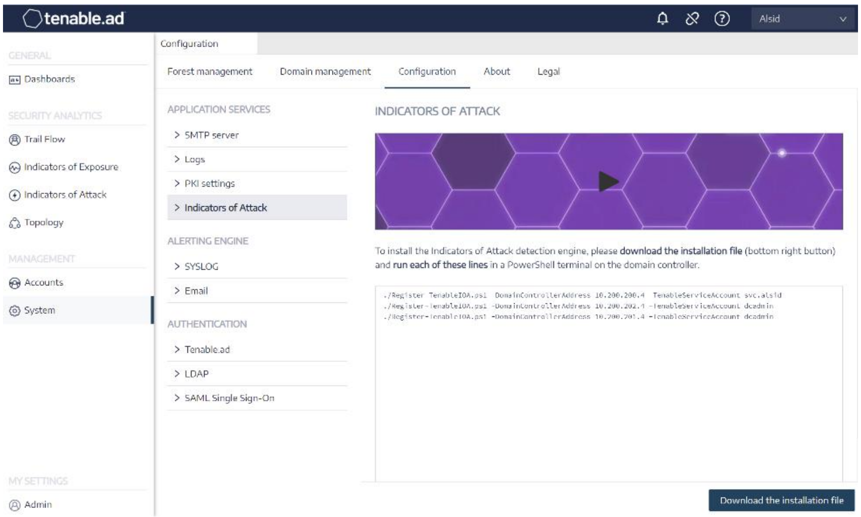
- Setup the PowerShell script to be executed.
- Configure the necessary audit policies.

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

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

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

[2] ETW insertion strings are the same information used by Windows to build its Event Logs



To install the Indicators of Attack detection engine, please **download the installation file** (bottom right button) and **run each of these lines** in a PowerShell terminal on the domain controller.

```
./Register-TenableIOA.ps1 -DomainControllerAddress 10.200.200.4 -TenableServiceAccount svc.alsid
./Register-TenableIOA.ps1 -DomainControllerAddress 10.200.202.4 -TenableServiceAccount dcadmin
./Register-TenableIOA.ps1 -DomainControllerAddress 10.200.201.4 -TenableServiceAccount dcadmin
```

Tenable.ad – Indicator-of-Attack setup view

Configuration adaptations

For each targeted domain, executing this Tenable deployment script will apply configuration changes, listed below. Some parameters (e.g. the GPO name), can be modified using command-line arguments passed when executing the script.

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

Command line

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

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

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

Configuration changes

- Add a GPO, named "Tenable.ad" by default, linked to the Domain Controllers OU by default. This GPO contains an immediate task configuring the PowerShell script running on each DC and installing a WMI filter that will start the PowerShell ETW script at boot, and the Advanced logging policy (see below).
- Activate the Microsoft Advanced logging policy, by modifying a registry key[3] (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

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

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[4].

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[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 and driver can affect performances of the Domain Controllers hosting the AD infrastructure. Therefore, Tenable chooses not to automatically deploy Microsoft Sysmon. It must be installed manually or by a dedicated GPO.

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

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

Once downloaded from the Sysinternal website[6], the following command will install Microsoft Sysmon on the current machine:

Command line

[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
[6] Sysinternal website: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

```
.\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[7] where the file is entirely commented.

This Sysmon installation is not sufficient by itself and a registry key is needed for the WMI filters to be aware of Sysmon being installed:

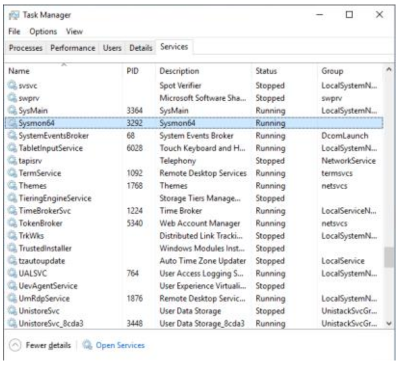
Command line

```
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 commands 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"
```



Name	PID	Description	Status	Group
svsvc		Spot Verifier	Stopped	LocalSystemN...
swprv		Microsoft Software Sha...	Stopped	swprv
SysMain	3364	SysMain	Running	LocalSystemN...
Sysmon64	3292	Sysmon64	Running	
SystemEventsBroker	68	System Events Broker	Running	DcomLaunch
TabletInputService	6028	Touch Keyboard and H...	Running	LocalSystemN...
tapisrv		Telephony	Stopped	NetworkService
TermService	1092	Remote Desktop Services	Running	termsvcs
Themes	1768	Themes	Running	netsvcs
TieringEngineService		Storage Tiers Manage...	Stopped	
TimeBrokerSvc	1224	Time Broker	Running	LocalServiceN...
TokenBroker	5340	Web Account Manager	Running	netsvcs
TrkWks		Distributed Link Tracki...	Stopped	LocalSystemN...
TrustedInstaller		Windows Modules Inst...	Stopped	
tzautoupdate		Auto Time Zone Updater	Stopped	LocalService
UALSVC	764	User Access Logging S...	Running	LocalSystemN...
UevAgentService		User Experience Virtuali...	Stopped	
UmRdpService	1876	Remote Desktop Servic...	Running	LocalSystemN...
UnistoreSvc		User Data Storage	Stopped	UnistackSvcGr...
UnistoreSvc_8cda3	3448	User Data Storage_8cda3	Running	UnistackSvcGr...

Sysmon – Screenshot of a Domain Controller running Sysmon

5.3. Problem with Advanced Audit Policy Configuration GPO precedence

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

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

[7] Tenable documentation portal: https://doc.alsid.app

How to check?

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

Command line

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

Compare the output with the Tenable.ad advanced audit policy requirements[8]. For each setting required by Tenable.ad, ensure that the effective policy covers it, at least. This is also fine if the effective policy is more exhaustive, for example when Tenable.ad needs "Success" or "Failure" and the setting is "Success and Failure".

How to fix?

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

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

Command line

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

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

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

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

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

Then, check the new effective policy as instructed above.

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:

Command line

```
Register-TenableIOA.ps1 -Uninstall
```

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

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**.

1. 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.**

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 defined jointly 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 compliancy 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[9].

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.

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.

Supported Web Browsers including minimum version	
Microsoft	Edge version 38.14393 or Internet Explorer 11
Google	Chrome version 56.0.2924
Mozilla	Firefox version 52.7.3
Apple	Safari version 11.0

[9] Tenable online user and administrator documentation: http://doc.alsid.app

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 as the SaaS platform, a valid certificate will be provided by Tenable's engineering team. This certificate will be signed by the Comodo certification authority[10].

Supported TLS configuration and version	• TLS 1.1 to TLS 1.3 • Server certificate provided by Tenable as part of the SaaS platform • Certificate issued from the customer's private PKI • Alternative TLS certificate provided by the customer
Recommended TLS configuration and version	• TLS 1.2 • Server certificate provided by Tenable as part of the SaaS platform

2.3. Client authentication

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

Supported Client authentication	• Login and Password • SAML • LDAP
Recommended TLS configuration and version	• SAML authentication

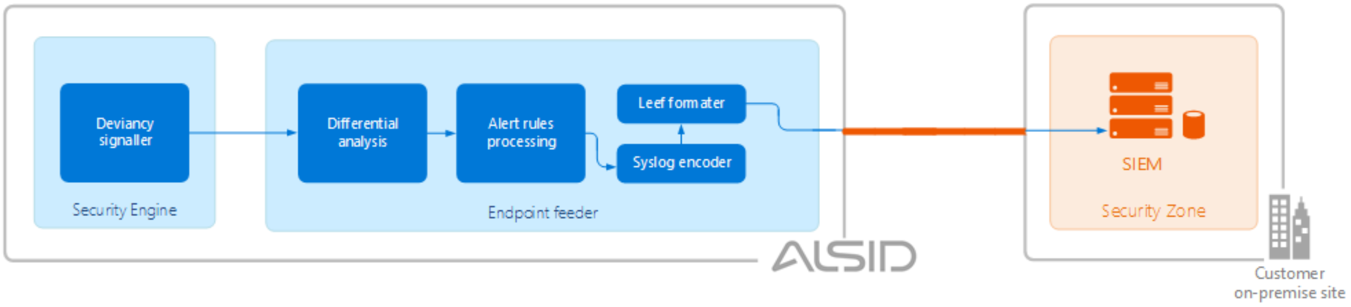
Please refer to Tenable's online documentation to review the technical prerequisites and configurations to be activated inside Tenable's portal to allow these authentication methods.

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

[10] Comodo CA support page: 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.



Integrated process managing SIEM's events

Tenable.ad is using the Syslog protocol to carry messages formatted following the LEEF format[11].

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.

Event log collectors successfully tested with Tenable's platform (non-exhaustive list)	• IBM QRadar • Splunk • RSA Netwitness • LogRhythm • Micro Focus ArcSight • Tibco Loglogic • McAfee Enterprise Security Manager

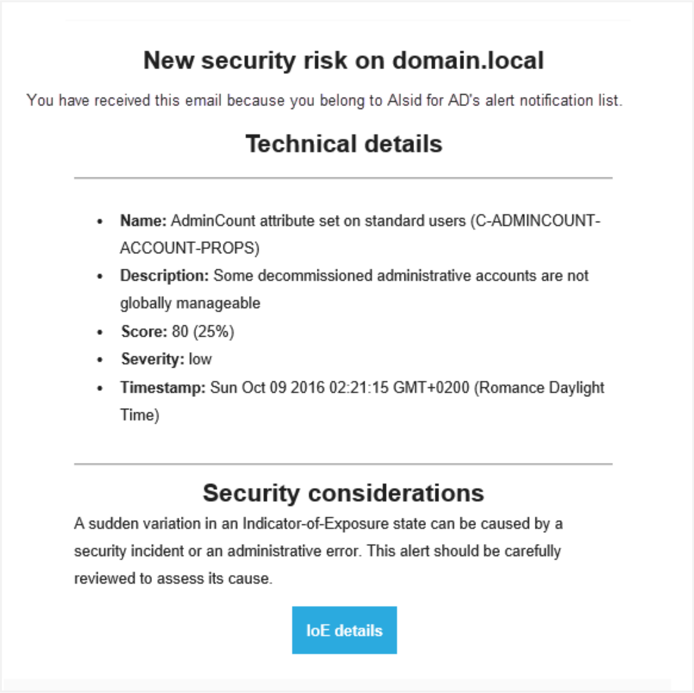
Please refer to Tenable's online documentation to review the technical prerequisites and configurations to be activated inside Tenable's portal to start event log forwarding and security alerts notification.

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.

[11] IBM's LEEF format specification: https://developer.ibm.com/qradar/wp-content/uploads/sites/89/2017/02/QRadar_LEEF_Format_Guide_V1.0.pdf



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-PROPS)
- **Description:** Some decommissioned administrative accounts are not globally manageable
- **Score:** 80 (25%)
- **Severity:** low
- **Timestamp:** Sun Oct 09 2016 02:21:15 GMT+0200 (Romance 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

Technical Summary

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

V. 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>0x1FFFFF</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x1F1FFF</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x1010</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x143A</GrantedAccess>
          </Rule>

          <!-- Detect process hollowing to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x0800</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x800</GrantedAccess>
          </Rule>
          <!-- Detect process process injection to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1055,technique_name=Process Injection" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x0820</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1055,technique_name=Process Injection" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x820</GrantedAccess>
          </Rule>
        </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>
```

VI. GLOBAL ARCHITECTURE

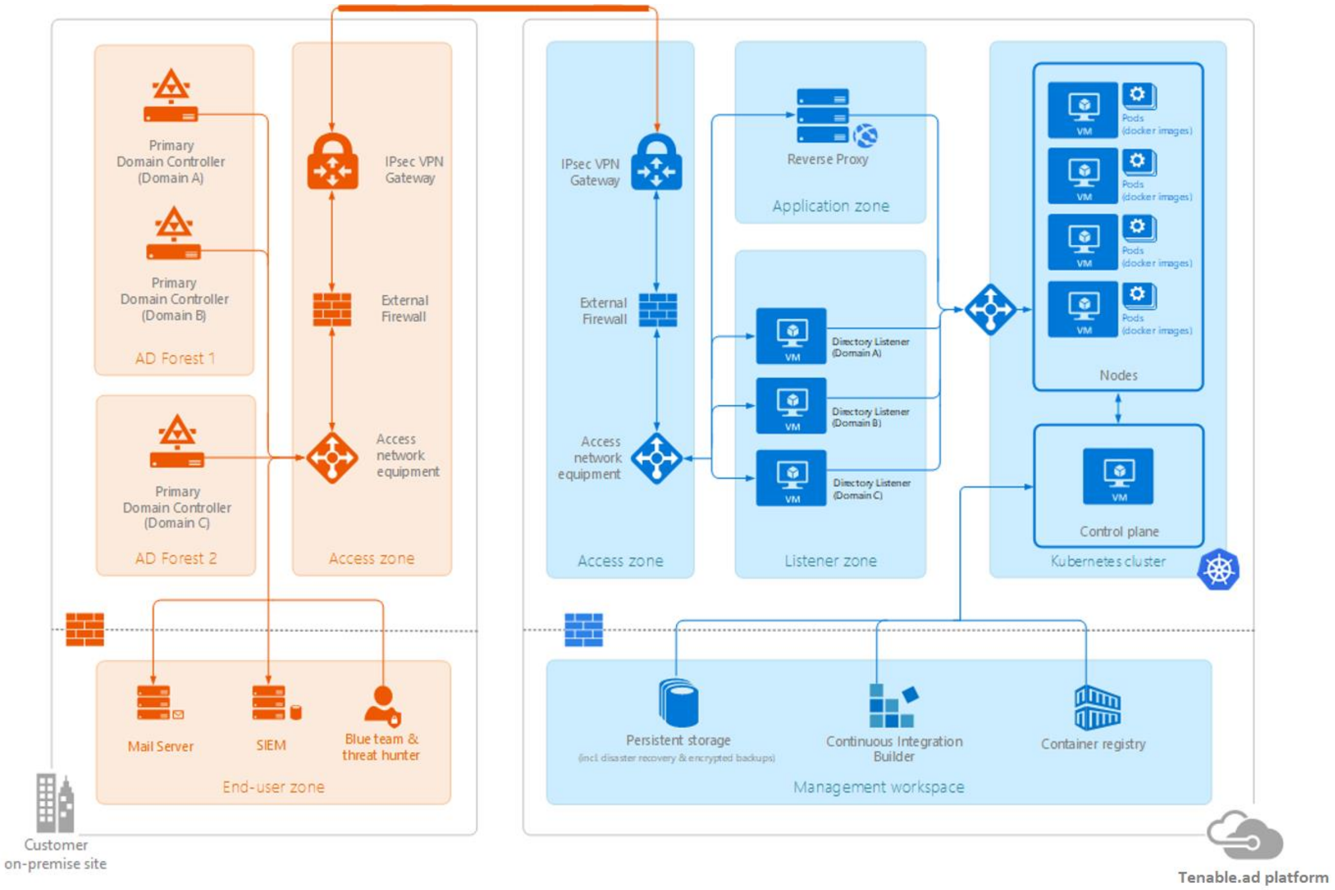
1. General considerations

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 sections summarize the Tenable.ad SaaS platform in both architectures. The first diagram shows the infrastructure deployed when a pure VPN-based access is chosen. The second diagram shows the infrastructure deployed when the application portal is reachable from the Internet.

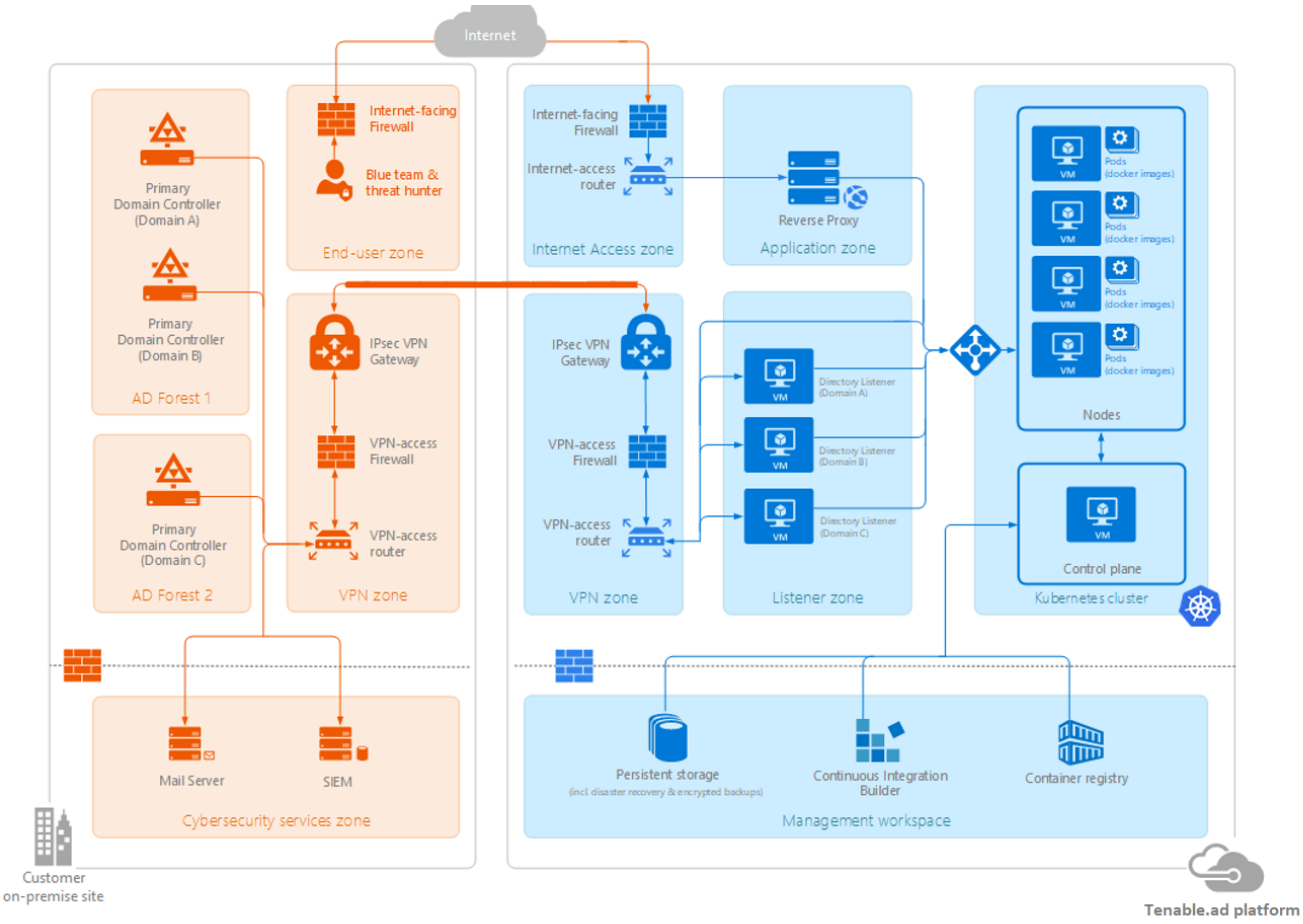
The orange part symbolizes the customer's information system, the blue part is entirely managed by Tenable.

2. Platform architecture when using a pure VPN-based access



Tenable.ad SaaS platform – Pure VPN access

3. Platform architecture when Tenable's web portal is accessible from the Internet



Tenable.ad SaaS platform – VPN access and web portal accessible from the Internet

VII. TROUBLESHOOTING

1. IOA script antivirus detection

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

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

If you encounter issues with the IOA feature such as:

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

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

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

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

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

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

VIII. 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

Items	Status	Customer Specifics
Confirmation of required agreements (NDA, Evaluation Software License), if applicable.	YES/NO	
VPN configuration is compatible with Tenable's VPN gateway, as reflected in the current document.	YES/NO	
The private subnet (/23) has been reserved in the VPN concentrator's crypto map and has been communicated to Tenable's Technical Lead.	YES/NO	
Required network flows have been opened from the VPN concentrator to the Primary Domain Controller emulator of each domain to monitor.	YES/NO	
The public IP of the VPN concentrator has been communicated to Tenable's Technical Lead.	YES/NO	
The Pre-Shared Key used to authenticate on the VPN concentrator has been communicated to Tenable's Technical Lead	YES/NO	
The option defining the accessibility to the Web Portal (through VPN tunnel or from the Internet) has been chosen and communicated to Tenable.	YES/NO	
If the console is accessible from the Internet, a DNS prefix for the Web Portal has been chosen and communicated to Tenable's Technical Lead. URL format: https:// your-choice .alsid.app	YES/NO	
If the console is accessible from the Internet, the list of public IP addresses to whitelist has been chosen and communicated to Tenable	YES/NO	
The private IP addresses of each Primary Domain Controller emulator have been communicated to Tenable's Technical Lead.	YES/NO	
A regular user account has been created on each Active Directory forest to monitor.	YES/NO	
On the specific Active Directory containers, access right has been granted to Tenable service account.	YES/NO	
The domain user accounts information has been communicated to Tenable's Technical Lead. Format: *NetBIOSName\SamAccountName*	YES/NO	
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.	YES/NO	
The list of optional configurations to activate (email notification, Syslog event forwarding, etc.) has been communicated to Tenable's Technical Lead.	YES/NO	
A Project Lead on the customer's side has been identified and will be available to validate common objectives with Tenable's Customer Manager.	YES/NO	
Technical staff on the customer's side is identified and available to respond to potential technical issues (VPN down, PDCe unreachable, etc.)	YES/NO	