Solution Design



Advanced Threat Analytics Implementation Services

Prepared for

Customer Name

3/2/2018

Version Draft

Prepared by

**[Update in doc Properties]**

[Type Author Position Here]

[Type Author Email Here]

Contributors

**[Type Contributors Here]**

Revision and Sign-Off Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
|  |  | 0.1 | Initial draft for review/discussion |
|  |  |  |  |
|  |  |  |  |

Table 1: Change Record

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version Approved | Position | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table 2: Reviewers

Table of Contents

[1 Solution Design Summary 0](#_Toc506995961)

[1.1 Audience 0](#_Toc506995962)

[2 Detailed Solutions Design 1](#_Toc506995963)

[2.1 Solutions Architecture Overview 1](#_Toc506995964)

[2.2 Active Directory Domain Services 2](#_Toc506995965)

[2.2.1 Solution Architecture—Domain Controllers 3](#_Toc506995966)

[2.3 Solution Sizing 3](#_Toc506995967)

[2.3.1 Sizing—ATA Center 4](#_Toc506995968)

[2.3.2 Sizing—ATA Gateways 5](#_Toc506995969)

[2.3.3 Domain Controller Analysis for Sizing 6](#_Toc506995970)

[2.3.4 ATA Components Required for Solution Design 7](#_Toc506995971)

[3 Solution Configuration 9](#_Toc506995972)

[3.1 Certificate Configuration 9](#_Toc506995973)

[3.2 ATA Center 10](#_Toc506995974)

[3.2.1 Hardware Configuration 10](#_Toc506995975)

[3.2.2 Network Ports 11](#_Toc506995976)

[3.3 ATA Lightweight Gateway 12](#_Toc506995977)

[3.3.1 Hardware Configuration 12](#_Toc506995978)

[3.3.2 Network Ports 13](#_Toc506995979)

[3.4 ATA Gateway 14](#_Toc506995980)

[3.4.1 Hardware Configuration 14](#_Toc506995981)

[3.4.2 Network Ports 15](#_Toc506995982)

[3.4.3 Port-Mirroring Considerations 16](#_Toc506995983)

[3.4.4 Port-Mirroring Configuration—Hyper-V 17](#_Toc506995984)

[3.5 ATA Configuration 17](#_Toc506995985)

[3.5.1 System 17](#_Toc506995986)

[3.5.2 Data Sources 19](#_Toc506995987)

[3.5.3 Detection 20](#_Toc506995988)

[3.6 Notifications and Reports 22](#_Toc506995989)

[3.6.1 Language 22](#_Toc506995990)

[3.6.2 Notifications 22](#_Toc506995991)

[3.6.3 Scheduled reports 23](#_Toc506995992)

[3.6.4 Mail Server 23](#_Toc506995993)

[3.6.5 Syslog Server 24](#_Toc506995994)

[3.7 Miscellaneous 24](#_Toc506995995)

[3.7.1 Licensing 24](#_Toc506995996)

[3.8 Additional Network Configuration Information 24](#_Toc506995997)

[3.8.1 Endpoint or Device Firewall Configuration 24](#_Toc506995998)

[3.9 Event Collection 25](#_Toc506995999)

[3.9.1 Configuration of ATA Gateway to Listen for SIEM Events 26](#_Toc506996000)

[3.9.2 Configuration of Windows Event Forwarding 26](#_Toc506996001)

## Tables

[Table 1: Change Record 3](#_Toc506996002)

[Table 2: Reviewers 3](#_Toc506996003)

[Table 3: Active Directory Configuration Items 3](#_Toc506996004)

[Table 4: Domain Controller Information 3](#_Toc506996005)

[Table 5: ATA Center Sizing 4](#_Toc506996006)

[Table 6: ATA Lightweight Gateway Sizing 6](#_Toc506996007)

[Table 7: ATA Gateway Sizing 6](#_Toc506996008)

[Table 8: Analyzed Packets per Second 7](#_Toc506996009)

[Table 9: ATA Components for Solution Design 8](#_Toc506996010)

[Table 10: ATA Certificate Configuration 10](#_Toc506996011)

[Table 11: ATA Center Hardware for <type forest FQDN here> 11](#_Toc506996012)

[Table 12: Requirements—ATA Center Network Ports 12](#_Toc506996013)

[Table 13: Requirements—ATA Lightweight Gateway Hardware 13](#_Toc506996014)

[Table 14: Requirements—ATA Lightweight Gateway Network Ports 13](#_Toc506996015)

[Table 15: Requirements—ATA Gateway Hardware 15](#_Toc506996016)

[Table 16: Requirements—Gateway Network Ports 16](#_Toc506996017)

[Table 17: Port-Mirroring Considerations 17](#_Toc506996018)

[Table 18: Port-Mirroring Configuration 17](#_Toc506996019)

[Table 19: Center Configuration 18](#_Toc506996020)

[Table 23: Gateways Configuration Details 18](#_Toc506996021)

[Table 23: Updates Configuration Details 19](#_Toc506996022)

[Table 21: ATA Role Based Access Control 19](#_Toc506996023)

[Table 22: ATA Directory Services Connectivity 19](#_Toc506996024)

[Table 24: General (Honeytoken) Configuration 20](#_Toc506996025)

[Table 25: ATA Exclusions 22](#_Toc506996026)

[Table 28: Email notification configuration 22](#_Toc506996027)

[Table 29: Syslog notification settings 23](#_Toc506996028)

[Table 26: Mail Server Configuration 24](#_Toc506996029)

[Table 27: Syslog server configuration 24](#_Toc506996030)

[Table 30: Endpoint Firewall Configuration 25](#_Toc506996031)

[Table 31: Windows Event Log IDs 25](#_Toc506996032)

[Table 32: SIEM Configuration—Gateway 26](#_Toc506996033)

[Table 33: Windows Event Forwarding—Domain Controllers to Gateway 26](#_Toc506996034)

## Figures

[Figure 1: High-Level ATA Design 1](#_Toc506996035)

**Spell/grammar check is turned ON within all SDM Word templates -** Remember to turn off spell/grammar check before sending out the document if you want to avoid showing spelling and grammar red mark-ups. To turn this feature off, do the following:

1. Click on File
2. Click on the Options on the left
3. Click on Proofing
4. Scroll to bottom and check the two boxes shown below:



**To remove all the Visible Guidance (Hot Pink text with Grey Background) all at once:**

1. Click Ctrl H to open the Find and Replace box
2. Make sure your cursor is in the ‘Find what’ box.
3. Click on the More button at the bottom left
4. Click on the Format Button at the bottom left and select Style
5. Scroll down, locate select the “Visible Guidance”
6. Make sure the ‘Replace with’ box is empty:
7. Click ‘Replace All”
8. If not empty - click on the format button in the lower left hand corner. Scroll down and chose ‘(no style)’then replace all.

**IMPORTANT – Finalize This Document**

**REMOVE** all pink text, guidance, comments, changes, and hidden text in this document before submitting it to the customer. You can do this in two ways:

* **Save as PDF** and send the PDF version to the customer.   
  ~ OR ~
* **Inspect document and remove comments, revisions, any document properties you do not want included, personal information, and hidden text.** For guidance on how to do this, see Remove hidden data and personal information from Office documents

1. Solution Design Summary

Provide an overall summary of the contents of this document. This should include the criteria by which the design was established and how it was validated. It should also clearly identify the intended audience.

Justification: Some project participants may need to know only the document’s highlights, and summarizing creates that user view. It also enables the full reader to know the essence of the document before they examine the details. Expand below on the customer architecture.

This document details the design of Advanced Threat Analytics (ATA) at Customer Name, which is designed to meet the requirements and goals that were stated in the Vision and Scope document.

The solution design is visualized in an architecture overview and explained accordingly. After providing an overview of the in-scope domain controllers, general information about the solutions sizing options is given.

Using the general information about the solutions sizing as a basis, the specific sizing for Customer Name was performed. Using the results of this, the necessary hardware was defined and allocated. After the installation of ATA Center and Gateways, ATA was configured specifically. These configuration options are also detailed in this document.

Both, networking and the option to collect events, which can enhance ATA’s detection of suspicious activities, are also explained.

* 1. Audience

This solutions design document is intended for Customer Name teams that are responsible for designing, implementing, and operating a Microsoft Advanced Threat Analytics (ATA) solution.

1. Detailed Solutions Design
   1. Solutions Architecture Overview

**Instruction:** Describe how the features and functions will operate together to form the solution. It identifies the specific components of the solution and their relationships. A diagram illustrating these components and relationships is an excellent communication device. Update the diagram below outlining the details of the architecture. A Visio file containing the base diagrams has been provided as a part of this offers materials. Please use those to assist you with this activity.

**Please adapt the text for the solution’s architecture according to your design.**



Figure 1: High-Level ATA Design

Figure 1 illustrates the solutions design architecture.

Customer Name opted to use both, Lightweight and dedicated Gateways in their ATA design. Lightweight Gateways are installed on two DCs (DC1, DC2) while the traffic of DC3 and DC4 is mirrored to a dedicated endpoint: the ATA Gateway.

The Lightweight Gateways are installed on virtualized domain controllers. These domain controllers are hosted on specifically hardened Hyper-V hosts, which are defined as Tier 0 and administered using dedicated administrative workstations.

The ATA Gateway is installed as a virtual machine on the same Hyper-V host as DC3 and DC4. On the Hyper-V server, port mirroring is configured. Thus, all traffic which is sent over the network card of these DCs is forwarded to a defined endpoint. This endpoint is the ATA Gateway.

All gateways send their data to the ATA Center which is installed on dedicated physical hardware and is not domain joined. The ATA Center evaluates the traffic which it receives and enhances this information by using Windows Event Log IDs which are forwarded from the Customer Name’s SIEM.

On the ATA Center, MongoDB is the database which stores all suspicious activities as well as traffic which is received.

All traffic between the ATA Center and the Gateways is encrypted with Transport Layer Security (TLS).

* 1. Active Directory Domain Services

**Instruction:** Update the table below and record all Active Directory configurations for the solution. There should be one table listing per forest. If you are monitoring multiple forests, please copy and paste the table so you have one table entry per forest.

The following table outlines the configuration of Customer Name’s Active Directory Domain Services (AD DS) infrastructure for which ATA will provide detection services.

|  |  |  |
| --- | --- | --- |
| [Type Active Directory Forest Name Here] | | |
| Item | Details | Configuration |
| Number of domain controllers | The number of domain controllers that will be reached by ATA. See Port Mirroring Requirements. | Number of Domain Controllers |
| Domain Controller Operating System | The standard operating system for Customer Name on all Domain Controllers. | Record OS version/versions for DCs here |
| Domain Controller Locations | Datacenter locations where Customer Name has domain controllers deployed which ATA will be required to provide detection services for. | Type in the datacenter location here |
| Standard User Object | * An Active Directory Domain Services user account and password that has been granted read access to **all objects** in the domains to be monitored. * This account should be locked down in a way that it is not allowed to have interactive logon capabilities to any system within the forest. * This account should have read only permissions on the Deleted Objects container. This will allow ATA to detect bulk deletion of objects in the domain in addition to keeping ATA up to date with deleted objects. | Record username here. Domain\username |
| Optional:   * Honeytoken account | A user account of a user who has no network activities. This account will be configured as the ATA Honey Token user. | Record username here. Domain\username |

Table 3: Active Directory Configuration Items

* + 1. Solution Architecture—Domain Controllers

To provide more reliable detection services, ATA can monitor traffic to and from domain controllers. The following table provides information about domain controllers that ATA will monitor; this includes fully qualified domain name (FQDN) and datacenter location information.

**Instruction:** Please update the following table with information specific to the domain controllers that ATA will be monitoring for this delivery. Add rows to your solution as needed.

|  |  |  |  |
| --- | --- | --- | --- |
| DC FQDN | Forest Name | Domain Name | Datacenter Location |
| DC1.contoso.com | Contoso.Com | Contoso.Com | Contoso HQ |
|  |  |  |  |

Table 4: Domain Controller Information

* 1. Solution Sizing

**Instruction:** Modify the tables in this section to record the customer’s specific sizing needs for this solution. This can also be kept as informational for your design and record your configuration items in the hardware section.

To determine the appropriate sizing for your ATA deployment, it is highly recommended that you capture network statistics for your domain controllers. This helps provide the most detailed information possible to design your solution.

Ideally, you should capture seven (7) or more days of average packets per second including lows and peaks to gain an understanding of your environment. If you have this available to you from your network team, please use that. Otherwise, ATA has a sizing tool to assist you. Please visit [ATA Capacity Planning](https://docs.microsoft.com/en-us/advanced-threat-analytics/plan-design/ata-capacity-planning) located on Microsoft docs online for more information about this ATA sizing and the sizing tool.

The following subsections outline the sizing of this solution.

* + 1. Sizing—ATA Center

The size of the ATA Center will depend on how much network traffic your domain controllers generate and how many suspicious activities that ATA detects and stores in its database. The following table provides general guidelines that can help you determine what size an ATA Center should be.

We recommend gathering ATA Center data for 30 days to determine normal user behaviors and produce behavioral analytics. The required disk space for the ATA database (on a per-domain controller basis) is defined in the following table. The recommendations are based on Customer Name–specific domain controller statistics.

This methodology will be used to determine the overall computational requirements for your ATA Center. That information will be documented in section 2.4.1 of this document.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Packets per Second\* | CPU (Cores\*\*) | Memory (GB) | Database Storage per Day (GB) | Database Storage per Month (GB) | IOPS\*\*\* |
| 1,000 | 2 | 32 | 0.3 | 9 | 30 (100) |
| 40,000 | 4 | 48 | 12 | 360 | 500 (750) |
| 200,000 | 8 | 64 | 60 | 1,800 | 1,000 (1,500) |
| 400,000 | 12 | 96 | 120 | 3,600 | 2,000 (2,500) |
| 750,000 | 24 | 112 | 225 | 6,750 | 2,500 (3,000) |
| 1,000,000 | 40 | 128 | 300 | 9,000 | 4,000 (5,000) |

Table 5: ATA Center Sizing

\* Total daily average number of packets-per-second from the all domain controllers being monitored by all ATA Gateways.

\*\* This includes physical cores, not hyper-threaded cores.

\*\*\* Average numbers (Peak numbers)

Notes

The ATA Center can handle an aggregated maximum of 1M packets per second from all the monitored domain controllers. In some environments, the same ATA Center can handle overall traffic that is higher than 1M. Contact askcesec@microsoft.com for assistance with such environments.

The amount of storage dictated here are net values. You should always account for future growth and to make sure that the disk the database resides on has at least 20% of free space.

If your free space reaches a minimum of either 20% or 200 GB, the oldest collection of data is deleted. Deletion continues to occur until 5% or 50 GB of free space remains at which point data collection stops working.

The storage latency for read and write activities should be below 10 ms.

The ratio between read and write activities is approximately 1:3 below 100,000 packets-per-second and 1:6 above 100,000 packets-per-second.

When running as a virtual machine dynamic memory or any other memory ballooning feature is not supported.

For optimal performance, set the **Power Option** of the ATA Center to **High Performance**.

When working on a physical server, the ATA database needs you to **disable** Non-uniform memory access (NUMA) in the BIOS. Your system may refer to NUMA as Node Interleaving, in which case you have to **enable** Node Interleaving to disable NUMA. For more information, see your BIOS documentation. This is not relevant when the ATA Center is running on a virtual server.

* + 1. Sizing—ATA Gateways

**Note for consultant**

Delete all ATA Lightweight Gateway references in this document in case you are opting for dedicated ATA Gateways only.

Delete all ATA Gateway references in this document in case you are opting for ATA Lightweight Gateways only.

* + - 1. ATA Lightweight Gateway

An ATA Lightweight Gateway is installed directly on the Domain Controller and monitors their traffic directly. It is recommended that you use an ATA Lightweight Gateway rather than an ATA Gateway whenever possible, as long as your domain controllers comply with the sizing table listed below. An ATA Lightweight Gateway can support the monitoring of one domain controller.

The following table provides some high-level suggestions regarding how to size Domain Controllers based on the amount of traffic being sent and received.

|  |  |  |
| --- | --- | --- |
| Packets per Second\* | CPU (Cores\*\*) | Memory (GB) |
| 1,000 | 2 | 6 |
| 5,000 | 6 | 16 |
| 10,000 | 10 | 24 |

Table 6: ATA Lightweight Gateway Sizing

\*Total number of packets-per-second on the domain controller being monitored by the specific ATA Lightweight Gateway.

\*\*Total number of non-hyper threaded cores that this domain controller has installed. While hyper threading is acceptable for the ATA Lightweight Gateway, when planning for capacity, you should count actual cores and not hyper threaded cores.

\*\*\*Total amount of memory that this domain controller has installed.

* + - 1. ATA Gateway

An ATA Gateway can support the monitoring of multiple domain controllers, depending on the amount of network traffic of the domain controllers being monitored. The following table provides some high-level suggestions regarding how to size your ATA Gateway based on the amount of network traffic being sent and received.

|  |  |  |
| --- | --- | --- |
| Packets per Second\* | CPU (Cores\*\*) | Memory (GB)\*\*\* |
| 1,000 | 1 | 6 |
| 5,000 | 2 | 10 |
| 10,000 | 3 | 12 |
| 20,000 | 6 | 24 |
| 50,000 | 16 | 48 |

Table 7: ATA Gateway Sizing

\*Total average number of packets-per-second from all domain controllers being monitored by the specific ATA Gateway during their busiest hour of the day.

\*The total amount of domain controller port-mirrored traffic cannot exceed the capacity of the capture NIC on the ATA Gateway.

\*\*Hyper-threading must be disabled.

* + 1. Domain Controller Analysis for Sizing

As noted previously, the size of the ATA Center and the number and placement of ATA Gateway or ATA Lightweight Gateway components depends on how much network traffic a domain controller receives. This traffic is sent to the ATA Gateway or gathered locally by the ATA Lightweight Gateway for further distribution to the ATA Center.

As a part of the design sessions, analysis was completed to determine how many packets each in-scope domain controllers handles. The following table provides this information.

**Instruction:** Please update the following table with specific packet information for each of the in-scope domain controllers that ATA will monitor. More specific information may be found at <https://docs.microsoft.com/en-us/advanced-threat-analytics/ata-capacity-planning> to assist you with this process.

|  |  |  |
| --- | --- | --- |
| Domain Controller FQDN | Analyzed Packets per Second | Comments |
| DC FQDN | #### |  |

Table 8: Analyzed Packets per Second

* + 1. ATA Components Required for Solution Design

ATA design, as noted, is largely based on how much network traffic is generated to and from the in-scope domain controllers. Making use of the information that was collected during the design workshops, the required ATA components for Customer Name are as follows.

**Instruction:** Update the following table with specifics regarding the number of ATA components required for your delivery. Use the following guidelines for filling out the table:

**Component** – the component column represents either the ATA Center or ATA Gateway component. If your deployment is not a mix of ATA Gateways and ATA Lightweight Gateways, remove the row corresponding to the Gateway type that is not being deployed.

**Number** – the number column represents the total number of the components the solution requires. If you are monitoring a single forest, you would only have 1 ATA Center. Therefore, the value in this column would be “1”.

**Location Placement** – use this column to illustrate which datacenter or network location the components will be deployed to.

**Details** – the details column is where you provide commentary on the information for that row. For example, using the ATA Center component, if you were monitoring multiple forests, you would have 1 ATA Center per forest. Your details would explain that you would have 1 ATA Center monitoring forest A (e.g. contoso.com) and another ATA Center monitoring forest B (e.g. fabrikam.com). Use this to add that detail or any other specifics you feel would be helpful for your customer.

**Note:** The information provided in sections 2.3.4 will help you determine the number of ATA Gateway’s you need to deploy to support your customer’s delivery. You may only deploy 1 ATA Center per Active Directory forest so the number of Centers should match the number of forests that are in scope.

|  |  |  |  |
| --- | --- | --- | --- |
| Component | Number | Location Placement | Details |
| ATA Center | 1 | Primary Datacenter | One ATA Center will be deployed to provide detection services for the contoso.com forest. |
| ATA Gateway | 2 (modify as per your design) | Primary Datacenter | Two ATA Gateways will be deployed to provide detection services for domain controllers located in the contoso.com forest which are in the primary datacenter location.  Gateway 1 will provide detection services for the following DCs: <DC01>, <DC2>. Gateway 2 will provide detection services for the following DCs: <DC3>, <DC4> |
| ATA Lightweight Gateway | 2 (modify as per your design) | Primary Datacenter Domain  Controller Name | 2 ATA Lightweight Gateways will be deployed to provide detection services for domain controllers located in the contoso.com forest which are in the Branch Office Datacenter |

Table 9: ATA Components for Solution Design

1. Solution Configuration

**Instructions:** Sections 3.1 through 3.6 have been created assuming a single forest deployment of ATA. If your engagement includes deploying ATA to multiple forests, please copy the entire contents of section 3 for each forest and title the primary section header as “ATA Solution Configuration – ForestName” (e.g. ATA Solution Configuration – Contoso.com)

**Gateway Configuration:** If your solution includes only ATA Gateways, remove section 3.3; otherwise if your solution contains only ATA Lightweight Gateways, remove section 3.4. If your solution contains a mix of both, keep both sections and document accordingly.

* 1. Certificate Configuration

The following table outlines the certificate configuration that will be used for the ATA Center and Gateway. These certificates will be issued by the Customer Name internal certificate authority.

It is important to make sure the ATA Center and ATA Gateways have access to Customer Name’s CRL distribution point. If they do not have Internet access, follow [the procedure to manually import a CRL](https://technet.microsoft.com/library/aa996972%28v=exchg.65%29.aspx), taking care to install all the CRL distribution points for the whole chain.

Note

Self-signed certificates should be used for lab deployment or testing only.

**Instruction:** Update the following table with information about how the certificates will be issues for each of the listed needs.

|  |  |  |
| --- | --- | --- |
| Role | Certificate Configuration | Certificate Details |
| Center | The ATA Center requires a OWIN Web Server certificate for secure communications with ATA portal with the following configuration:   * A private key. * A provider type of either Cryptographic Service Provider (CSP) or Key Storage Provider (KSP). * A public key length of 2,048 bits. * A value set for KeyEncipherment and ServerAuthentication usage flags.   Notes  For example, you can use the standard Web server or Computer templates.  If Customer Name would like to use a user-friendly URL for the ATA Console, then ensure the ATA Center has that FQDN listed as a Subject Alternate Name (SAN). | ATA Center certificate:  Enter in the ATA Center Hostname:  e.g. ATACenter.contoso.com  Subject Alternate Names (SANs):  Enter the ATA Console URL. e.g. ATAConsole.contoso.com |
| Gateway | Lightweight Gateways, and Gateways, receive a non-exportable self-signed certificate through the Gateway setup, which will be used to secure the SSL communications with the ATA Center.  Note  This certificate is managed through ATA, so it will be automatically created, and renewed. | ATAGateway |

Table 10: ATA Certificate Configuration

* 1. ATA Center

This section details the ATA Center configuration.

* + 1. Hardware Configuration

**Instruction:** Using the data you captured in section 2.3.3, and the location information listed in section 2.2.1, provide specific details surrounding the ATA deployment.

Each section will have tables to help you illustrate the eventual ATA design and configuration. Please modify the tables in this section to record the customer’s specific configuration needs for this solution.

This section outlines the hardware configuration for the ATA Center.

**Instruction:** You should have a single table listed for each in-scope forest. If you have more than one forest, please copy and paste the following table as many times as needed. Update the table caption to be specific to the forest.

The following table provides information about the hardware configuration that will be needed to support this ATA Center deployment.

|  |  |  |
| --- | --- | --- |
| Component | Center Hardware Details | Configuration |
| Processor | See center-sizing section (Table 5: ATA Center Sizing). | Update based on sizing exercise here |
| Memory | See center-sizing section (Table 5: ATA Center Sizing). | Update based on sizing exercise here |
| Available disk space  Database storage | See center-sizing section (Table 5: ATA Center Sizing). | Enter based on sizing exercise here  Database location:  <Record Database location here. Review operations and implementation guides for further requirements. Its recommended to move the database to dedicated disks and drive.> |
| Network | One network adapter, one IP address  Note  If using physical server in VLAN environment, it is recommended to use two network adapters. | ATA Center IP: x.x.x.x |
| Virtual machine  Physical computer | Installation of the ATA Center as a virtual machine is supported.  <<Update this section to reflect choice reasoning>> | Physical or Virtual |
| BIOS  <delete this row if the ATA center is running on a virtual server> | The ATA database requires that Customer Name DISABLE nonuniform memory access (NUMA) in the BIOS. | Confirm Disabled (Y, N) and add commentary if the answer is “N”. |

Table 11: ATA Center Hardware for <type forest FQDN here>

* + 1. Network Ports

**Instruction:** Modify the tables in this section to record the customer’s specific configuration needs for this solution. Remove or configure optional configuration items.

The following table lists the minimum ports that are needed by the ATA Center.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Protocol | Transport | Port | To or From | Direction | IP Address |
| SSL (ATA communications) | TCP | 443 | ATA Gateway | Inbound | ATA Center IP Address: x.x.x.x |
| HTTP | TCP | 80 | Customer Name network | Inbound | ATA Center IP Address: x.x.x.x |
| HTTPS | TCP | 443 | Customer Name network and ATA Gateway | Inbound | ATA Center IP Address: x.x.x.x |
| SMTP (optional) | TCP | 25 | SMTP server | Outbound | ATA Center IP Address: x.x.x.x |
| SMTPS (optional) | TCP | 465 | SMTP server | Outbound | ATA Center IP Address: x.x.x.x |
| Syslog (optional) | TCP | 514 | Syslog server | Outbound | ATA Center IP Address: x.x.x.x |
| LDAP | TCP and UDP | 389 | Domain controllers | Outbound | ATA Center IP Address: x.x.x.x |
| LDAPS (optional) | TCP | 636 | Domain controllers | Outbound | ATA Center IP Address: x.x.x.x |
| DNS | TCP and UDP | 53 | DNS servers | Outbound | ATA Center IP Address: x.x.x.x |
| Kerberos (optional if domain joined) | TCP and UDP | 88 | Domain controllers | Outbound | ATA Center IP Address: x.x.x.x |
| Netlogon (optional if domain joined) | TCP and UDP | 445 | Domain controllers | Outbound | ATA Center IP Address: x.x.x.x |
| Windows Time (optional if domain joined) | UDP | 123 | Domain controllers | Outbound | ATA Center IP Address: x.x.x.x |

Table 12: Requirements—ATA Center Network Ports

* 1. ATA Lightweight Gateway
     1. Hardware Configuration

**Instruction:** It is recommended that the customer, where possible and where existing DC compute resources can handle it, deploy the Lightweight Gateway where possible. Please modify the tables in this section to record the customer’s specific configuration needs for this solution.

**Note:** If the Domain Controller does not have the necessary amount of resources required by the ATA Lightweight Gateway, the domain controller performance will not be affected, but the ATA Lightweight Gateway might not operate as expected.

**Caution Note:** The ATA Lightweight Gateway includes a monitoring component which evaluates the available compute and memory capacity on the domain controller on which is is running. The monitoring process runs every 10 seconds and dynamically updates the CPU and memory utilization quota on the ATA Lightweight Gateway process to make sure that at any given point in time, the domain controller has at least 15% of free compute and memory resources.

An ATA Lightweight Gateway will support and monitor only the Domain Controller it is installed on. The following table details the Domain Controllers that the ATA Lightweight Gateway is installed on.

|  |  |  |  |
| --- | --- | --- | --- |
| Domain Controller Name | Packets per Second | CPU (Cores) | Memory (GB) |
| DC1 name | 9,568 (change as per sizing report) | 12 cores (change as per sizing report and sizing guidance) | 32 GB (change as per sizing report and sizing guidance) |
| DC2 name | 9,568 (change as per sizing report) | 12 cores (change as per sizing report and sizing guidance) | 32 GB (change as per sizing report and sizing guidance) |

Table 13: Requirements—ATA Lightweight Gateway Hardware

* + 1. Network Ports

Note

As part of the resolution process performed by the ATA Lightweight Gateway, the following ports need to be open inbound on devices on the network from the ATA Lightweight Gateways.

* NTLM over RPC
* NetBIOS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Protocol | Transport | Port | To or From | Direction |
| DNS | TCP and UDP | 53 | DNS servers | Outbound |
| NTLM over RPC | TCP | 135 | All devices on the network (active name resolution) | Outbound |
| NetBIOS | UDP | 137 | All devices on the network (active name resolution) | Outbound |
| SSL | TCP | 443 | ATA Center IP Address: <tbd> | Outbound |
| Syslog (optional) | UDP | 514 | SIEM Server | Inbound |

Table 14: Requirements—ATA Lightweight Gateway Network Ports

* 1. ATA Gateway
     1. Hardware Configuration

**Instruction:** If you are not deploying any full ATA Gateway systems, you may delete this section. Otherwise, modify the tables in this section to record the customer’s specific configuration needs for this solution if the deployment consists of deploying full ATA Gateways.

**Note:** The ATA Gateway uses its memory to buffer captured data and sends it to the Center. This is at a default setting of 1,000,000 entities and is configurable. Depending on the load of domain controller connected to the Gateway, this can generate a tremendous amount of data.

**Caution Note:** If communication between the Center and the Gateway is disrupted, the Gateway will cache in memory. 1,000,000 entities can take up to 5GB of memory. Once this limit is reached, it will stop collecting network traffic until communication is restored with the Center. Depending on the domain controller load, this can be hours or minutes.

An ATA Gateway will support multiple domain controllers and is based on the amount of traffic domain controllers send and receive; the following configuration is recorded.

|  |  |  |
| --- | --- | --- |
| Component | Gateway Hardware Details | Configuration |
| Processor | See Gateway-sizing section (Table 7: ATA Gateway Sizing). | Update based on sizing exercise here |
| Memory | See Gateway-sizing section (Table 7: ATA Gateway Sizing). | Update based on sizing exercise here |
| Network | The Gateway requires two or more network adapters:   * A **management adapter** will be used for communications on the company network. * A **capture adapter** will be used to capture traffic to and from the domain controllers. | **Management:**  This adapter will be configured as follows:  Management IPs: x.x.x.x  Preferred and Alternate DNS Servers: x.x.x.x & x.x.x.x  DNS Suffix for Connection: contoso.com  DNS suffix for this connection” should be the DNS name of the domain being monitored  **Capture:**  This adapter will be configured as follows:  Capture IP Address: 1.1.1.1  Capture Subnet: 255.255.255.255  Configure port mirroring for the capture adapter as the destination of the domain controller network traffic. |
| Virtual machine  Physical computer | Update this to reflect choice reasoning  Installation of the ATA Gateway as a virtual machine is supported if the domain controllers that are being monitored are also running as virtual machines on the same virtualization host. | Type in “Physical” or “Virtual” depending on customer’s choice. If virtual, list the virtualization platform. |

Table 15: Requirements—ATA Gateway Hardware

* + 1. Network Ports

**Instruction:** modify the tables in this section to record the customer’s specific configuration needs for this solution. Remove or configure optional configuration items.

The following table lists the minimum ports that the ATA Gateway requires to be configured on the management adapter.

Note

As part of the resolution process done by the ATA Gateway, the following ports need to be open inbound on devices on the network from the ATA Gateways.

* NTLM over RPC (TCP Port 135)
* NetBIOS (UDP port 137)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Protocol | Transport | Port | To or From | Direction |
| LDAP | TCP and UDP | 389 | Domain controllers | Outbound |
| Secure LDAP (LDAPS) | TCP | 636 | Domain controllers | Outbound |
| LDAP to Global Catalog | TCP | 3268 | Domain controllers | Outbound |
| LDAPS to Global Catalog | TCP | 3269 | Domain controllers | Outbound |
| Kerberos | TCP and UDP | 88 | Domain controllers | Outbound |
| Netlogon | TCP and UDP | 445 | Domain controllers | Outbound |
| Windows Time | UDP | 123 | Domain controllers | Outbound |
| DNS | TCP and UDP | 53 | DNS Servers | Outbound |
| NTLM over RPC | TCP | 135 | All devices on the network | Outbound |
| NetBIOS | UDP | 137 | All devices on the network | Outbound |
| SSL | TCP | 443 | ATA Center IP Address: <tbd> | Outbound |
| Syslog (optional) | UDP | 514 | SIEM Server | Inbound |

Table 16: Requirements—Gateway Network Ports

* + 1. Port-Mirroring Considerations

The main data source ATA uses comes from deep-packet inspection of network traffic to and from your domain controllers. Port mirroring needs to be configured before ATA can access that network traffic. Port mirroring copies the traffic from the source port to the destination port. ATA works with most solutions that can mirror traffic—if the traffic can be port-mirrored to ATA, it can be used to analyze threats to your system.

The following table outlines Gateway considerations for port mirroring in physical computer or virtual machine scenarios.

|  |  |  |
| --- | --- | --- |
| ATA Gateway | Domain Controller | Considerations |
| Virtual | Virtual on same host | * The virtual switch needs to support port mirroring. * Moving one of the virtual machines to another host by itself might cause port mirroring to not work. |
| Virtual | Virtual on different hosts | Confirm that your virtual switch supports this scenario. |
| Virtual | Physical | This requires a dedicated network adapter. Otherwise, ATA will see the traffic that is coming in and out of the host, including the traffic it sends to the ATA Center. |
| Physical | Virtual | Confirm that your virtual switch supports this scenario and that the port-mirroring configuration of your physical switches is based on the scenario.   * If the virtual host is on the same physical switch, you will need to configure a switch-level span. * If the virtual host is on a different switch, you will need to configure a remote switched port analyzer (RSPAN) or an encapsulated remote switched port analyzer (ERSPAN)\*. |
| Physical | Physical on the same switch | The physical switch must support a switched port analyzer (SPAN) or port mirroring. |
| Physical | Physical on a different switch | This requires physical switches to support RSPAN or ERSPAN\*. |

Table 17: Port-Mirroring Considerations

**\*** ERSPAN is only supported when decapsulation is performed before the traffic is analyzed by ATA

Virtual Gateways are required for each virtualization host on which a virtual domain controller is running. To configure port mirroring, Customer Name needs to refer to the vendor's documentation.

* + 1. Port-Mirroring Configuration—Hyper-V

**Instruction:** Modify the tables in this section to record the customer’s specific configuration needs for this solution. Remove or configure optional configuration items. Elaborate on the configuration below.

The following table outlines the Hyper-V configuration that will be used for this solution.

Note

Port-mirroring is a feature in Microsoft Hyper-V’s Virtual Switch that was added in Windows Server 2012. Thus, the virtualization hosts need to run (at least) Windows Server 2012.

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Type | Virtual Machine Name | Virtual Machine Host |
| Center | Destination | Enter VM Name | Enter Host Name |
| Gateway | Source | Enter VM Name | Enter Host Name |

Table 18: Port-Mirroring Configuration

* 1. ATA Configuration

The information in this section is configured through the ATA portal (that is, the management interface) and helps configure ATA to verify that it is capturing information about your environment in an efficient manner.

* + 1. System

**Instruction:** Update the information in this section with the settings that you applied for the customer’s ATA deployment. Each subsection lists a table that has entries you will update to depict their final ATA deployment configuration.

* + - 1. Center

**Instruction:** Update the following table with information specific to your customer deployment.

|  |  |  |
| --- | --- | --- |
| Setting | Value | Comments |
| URL | Enter ATA Center IP Address and Port |  |
| Certificate | Enter certificate details |  |

Table 19: Center Configuration

* + - 1. Gateways

**Instructions:** Update the following table with information for all Gateways that are being deployed for this customer.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Gateway Name | Gateway Type | DC’s Monitored | Domain Synchronizer Candidate (Yes/No) | Syslog Listener (Yes/No) | Windows Event Forwarding Collection (Yes/No) | Comments |
| ATA GW1 | Lightweight | DC1.Contoso.Com | Yes | No | Yes | This Gateway has been installed onto DC1. |
| ATA GW2 | Full | DC2.Contoso.Com  DC3.Contoso.Com | Yes |  |  | This Gateway is monitoring multiple DC’s in the “Seattle” AD site. |

Table : Gateways Configuration Details

* + - 1. Updates

Updates for ATA can be downloaded automatically or manually.

Update all Gateways automatically is set to: ON/OFF

Automatically restart the domain controller on which the Lightweight Gateway is installed, is set to: ON/OFF

The Gateways are updated as follows:

**Instructions:** Update the following table with information for Updates that are being deployed for this customer.

|  |  |  |  |
| --- | --- | --- | --- |
| Gateway Name | Gateway Type | Automatic Update | Automatic Restart |
| ATA GW1 | Lightweight | On/Off | On/Off |
| ATA GW2 | Full | On/Off | On/Off |

Table 23: Updates Configuration Details

* + - 1. ATA Role Based Access Control – RBAC

ATA includes three roles with different sets of permissions. These groups are created as local security groups during the ATA setup process.

**Instruction:** Update the following table with information specific to your customer deployment.

|  |  |  |
| --- | --- | --- |
| Group Name | Members | Comments |
| Microsoft Advanced Threat Analytics Administrators | Username/group: <add username/group>  Domain: <add domain> | Team in charge of deploying and managing ATA (adding new gateways, etc). |
| Microsoft Advanced Threat Analytics Users | Username/group: <add username/group>  Domain: <add domain> | Permissions to change and manage alert states (team in charge to follow-up / handle alerts generated by ATA). |
| Microsoft Advanced Threat Analytics Viewers | Username/group: <add username/group>  Domain: <add domain> | Team(s) that might be interesting to leverage ATA information for their daily activities (security team, misc. admins, etc.) |

Table 21: ATA Role Based Access Control

* + 1. Data Sources
       1. Directory Services

**Instruction:** Update the following table with information specific to your customer deployment.

|  |  |  |
| --- | --- | --- |
| Setting | Value | Comments |
| Username Password | Read-only Service account information:  Username:  Domain: |  |
| Domain | Domain name: |  |
| Single label domain | YES/NO |  |

Table 22: ATA Directory Services Connectivity

* + - 1. SIEM

Syslog is configured as ON/OFF. This setting enables the Syslog listener for all Gateways on port 514 using the UDP protocol. Make sure to configure your SIEM to send events via Syslog.

* + - 1. VPN

Radius Accounting is configured as ON/OFF. This setting enables the Radius listener for all Gateways on port 1813 using the UDP protocol.

* + 1. Detection
       1. General

Honeytoken accounts can be added here.

A honeytoken account is a user account that has been created to attract a potential attacker. This account is typically set up to appear as a higher-level access account, but it is actually configured with minimal capabilities and is monitored heavily. This account should be named in a way that would attract unwanted use, but it should be heavily locked down so that if it is actually used it cannot do anything in the environment. If you use this type of an account, verify that it does not have the ability to log on interactively or be used to enumerate your directory.

ATA can monitor such an account and will alert you if it is used. The following table provides information about the honeytoken user(s) that were configured in ATA to be monitored:

|  |  |  |
| --- | --- | --- |
| Account Name | AD Forest Location | Explanation |
| <honeytoken account> |  | This account is located in the ds.contoso.com forest and has been restricted to not logon interactively nor can it read AD. ATA will monitor the attempted use of this account object. |

Table 24: General (Honeytoken) Configuration

* + - 1. Exclusions

ATA provides you the ability to provide exclusions for various detections given ATA the ability to learn your environment.

|  |  |  |
| --- | --- | --- |
| Exclusion | Setting | Tips |
| **Instruction: Delete this row if you are delivering ATA v1.8! This exclusion will be added with ATA v1.9 only. If you are delivering ATA v1.9, format the row according to the one below and delete the “Instruction” text.**  Suspicious service creation |  | **Instruction: Delete this row if you are delivering ATA v1.8! This exclusion will be added with ATA v1.9 only. If you are delivering ATA v1.9, format the row according to the one below and delete the “Instruction” text.**  Investigate what caused this, if it is a legitimate service creation by one of the machines in the organization and it would repeat in the future, then you may exclude it. |
| Abnormal modifications of sensitive groups | Users: | You may want to exclude users that normally modify sensitive groups |
| Identity theft using pass the ticket attack | IP addresses and subnets:  Computers: | You may want to exclude subnets in which the IP addresses change frequently, like VPN subnets |
| Identity theft based on abnormal behavior | Users: | Conduct detailed investigation to assess if the entity needs to be excluded. |
| Kerberos golden ticket activity | Users: | Conduct detailed investigation to assess if the entity needs to be excluded. |
| Malicious data protection private information request | IP addresses and subnets:  Computers: | You may want to exclude any product that uses Active directory replication API |
| Malicious replication of directory services | IP addresses and subnets:  Computers: | Conduct detailed investigation to assess if the entity needs to be excluded. |
| Reconnaissance using account enumeration | IP addresses and subnets:  Computers: | You may want to exclude security scanners |
| Reconnaissance using directory services queries | IP addresses and subnets:  Computers: | You may want to exclude security scanners |
| Reconnaissance using DNS | IP addresses and subnets:  Computers: | You may want to exclude security scanners |
| Reconnaissance using SMB session enumeration | IP addresses and subnets:  Computers: | You may want to exclude security scanners |
| Remote execution attempt detected | IP addresses and subnets:  Computers: | You may want to exclude machines used by administrator or any machine that needs to perform remote administrative tasks on domain controllers |
| Unusual protocol implementation | IP addresses and subnets:  Computers: | Based on your investigation, if it is concluded that machine is expected to exhibit this behaviour |

Table 25: ATA Exclusions

* 1. Notifications and Reports
     1. Language

<Language> was selected as the language in the ATA console.

* + 1. Notifications

Both, mail notifications and Syslog notifications can be configured in ATA.

**Instruction:** the following section is the recording of the notifications configuration. Please update with your customer’s settings.

ATA will send email alerts using the following settings:

|  |  |
| --- | --- |
| Value | Setting |
| New suspicious activity is detected | ON/OFF  Email recipient(s): |
| New health issue is detected | ON/OFF  Email recipient(s): |

Table 28: Email notification configuration

**Instruction:** the following section is the recording of the syslog notifications configuration. Please update with your customer’s settings. If you are not configuring SIEM integration as a part of this deployment, you may add the following statement:

SIEM integration is out of scope for this deployment and there has not been any configuration settings set for this configuration option.

This section outlines the syslog notification configuration that will be used for Customer Name’s ATA deployment. Using this configuration, ATA will send information to syslog servers (e.g. SIEM systems) using the following settings:

|  |  |
| --- | --- |
| Value | Setting |
| New suspicious activity is detected | ON/OFF |
| Existing suspicious activity is updated | ON/OFF |
| New health issue is detected | ON/OFF |

Table 29: Syslog notification settings

* + 1. Scheduled reports

When configuring a mail server, scheduled reports can be sent. Two types of scheduled reports can be generated:

* a summary of suspicious activities and health issues
* every modification to sensitive groups in Active Directory, including modifications which generated a suspicious activity.
  + 1. Mail Server

The following table contains the email alerting configuration.

**Instruction:** Please update the following table to illustrate specific configuration information for your customer.

|  |  |  |
| --- | --- | --- |
| Field | Description | Value |
| SMTP server endpoint (required) | FQDN of the SMTP server. | For example: smtp.contoso.com |
| SSL | Toggle SSL if the SMTP server requires SSL.  Note  If the administrator enables SSL, Customer Name will also need to change the Port number. | Default is disabled  OFF/ON |
| Authentication | Enable if the SMTP server requires authentication.  Note  If Customer Name enable authentication, the administrator must provide the user name and password of an email account that has permission to connect to the SMTP server. | Default is disabled  OFF/ON |
| Send from (required) | The email address that the alert will be sent from. | For example: ATA@contoso.com |

Table 26: Mail Server Configuration

* + 1. Syslog Server

ATA may be configured to forward information about the suspicious activities it detects to Security Information and Event Management (SIEM) systems. ATA may send information using two specific RFC formats; 5424 and 3164. The settings are specific to the listening SIEM endpoint system. The following table lists the settings for Customer Name’s SIEM integration:

**Instruction:** Update the following table to reflect the settings used by your customer. If you are not configuring SIEM integration as a part of this deployment, you may add the following statement:

|  |  |  |  |
| --- | --- | --- | --- |
| Syslog Server Endpoint | Port | Transport | Format |
| Syslog.contoso.com  FQDN of the Syslog server | 514  Optionally change the port number (default 514) | Can be UDP, TCP, or TLS (Secured Syslog) | This is the format that ATA uses to send events to the SIEM server - either RFC 5424 or RFC 3164. |

Table 27: Syslog server configuration

* 1. Miscellaneous
     1. Licensing

In this section the activated license for ATA is displayed.

* 1. Additional Network Configuration Information

**Instruction:** Modify the tables in this section to record the customer’s specific configuration needs for this solution.

This section provides network configuration information that can help with the deployment of the ATA solution for Customer Name.

* + 1. Endpoint or Device Firewall Configuration

To adequately provide detection services, ATA needs access to information about the devices that are on the network. To do this, a series of network ports must be opened between the ATA Gateways and devices that in the environment that ATA is reviewing. The following table illustrates the ports that must be opened if there are firewalls between the ATA Gateway and the devices in your network environment.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Port Name | Type | Port | Entities | Direction |
| NetBIOS | UDP | 137 | All devices on the network | Inbound |
| NTLM over RPC | TCP | 135 | All devices on the network | Inbound |

Table 30: Endpoint Firewall Configuration

* 1. Event Collection

**Instructions:** This section is **optional**. The scope of the default offer does not include SIEM integration. If your deliver has included it, please leverage this section for configuration specific details for your delivery. If not, please delete this section.

Modify this section to record the customer’s specific configuration needs for this solution. Remove or configure optional configuration items. If not relevant to the design, please remove this section. Note: Configuration of the SIEM servers is the customer’s responsibility.

To enhance the detection of Pass-the-Hash malicious hacking attempts, ATA requires the following Windows Event Log IDs: 4776, 4732, 4733, 4728, 4729, 4756, and 4757. The following table provides information about each Windows Event Log ID and a link for further information.

|  |  |  |
| --- | --- | --- |
| Windows Event Log ID | Description | Link for further information |
| 4776 | The computer attempted to validate the credentials for an account. | <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4776> |
| 4732 | A member was added to a security-enabled local group. | <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4732> |
| 4733 | A member was removed from a security-enabled local group. | <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4733> |
| 4728 | A member was added to a security-enabled global group. | <https://social.technet.microsoft.com/wiki/contents/articles/17049.event-id-when-a-user-is-added-or-removed-from-security-enabled-global-group-such-as-domain-admins-or-group-policy-creator-owners.aspx> |
| 4729 | A member was removed from a security-enabled global group. |
| 4756 | A member was added to a security-enabled universal group. | https://social.technet.microsoft.com/wiki/contents/articles/17051.event-id-when-a-user-is-added-or-removed-from-security-enabled-universal-group-such-as-enterprise-admins.aspx |
| 4757 | A member was removed from a security-enabled universal group. |

Table 31: Windows Event Log IDs

This can be forwarded to the ATA Gateway in either by configuring the ATA Gateway to monitor SIEM events or by using Windows event forwarding to capture specific Windows events that are logged and captured within the domain controllers event logs.

Important

The Event Collection steps are not required for ATA Lightweight Gateways, as these can read events locally, without the need to configure event forwarding.

* + 1. Configuration of ATA Gateway to Listen for SIEM Events

**Instruction:** Update the following table with specific information.

|  |  |  |
| --- | --- | --- |
| Listening IP Address (Gateway) | Port Type | Port (Default) |
| <<EnterIPHere>> | UDP | 514 |

Table 32: SIEM Configuration—Gateway

* + 1. Configuration of Windows Event Forwarding

**Instructions:** If the customer does not have a SIEM server you can configure your domain controllers to forward Windows Event ID 4776 directly to one of your ATA Gateways. This is out of scope for this engagement by default. Customer needs to configure WEF on the Domain Controllers. This is a pure record if the customer configures WEF.

Customer Name can collect events from remote computers and store them in logs on a local computer. The following section contains the configuration for Customer Name related to specific events that are to be collected through the creation of a subscription.

The following table lists ’s domain controllers that will be used to forward Windows Event IDs: 4776, 4732, 4733, 4728, 4729, 4756, and 4757, to the ATA Gateways.

**Instruction:** Update the following table with specific information for Windows Event Forwarding for your customer’s deployment. If you are configuring multiple listeners for multiple forests, please add a subsection for each forest name and copy/paste the sample table provided.

|  |  |  |
| --- | --- | --- |
| Configuration Item | Computers | Details |
| Source | Enter DomainControllerFQDN | Source domain controllers |
| Collector | Enter ATAGateway FQDN | ATA Gateway |
| Subscription name | Enter Subscription Name | Created on the collector |
| Event log readers group | Enter Source Computers FQDN | Created on the collector |

Table 33: Windows Event Forwarding—Domain Controllers to Gateway