ATAIS - Solution Design



Advanced Threat Analytics Implementation Services

Preparado para

Customer Name

9/26/2016

Versión 1 Draft

Preparado por

**[Update in doc Properties]**

[Type Author Position Here]

[Type Author Email Here]

Contribuidores

**[Type Contributors Here]**

Revisión y hoja de firmas

Control de Cambios

Tabla 1: Control de cambios

|  |  |  |  |
| --- | --- | --- | --- |
| Fecha | Autor | Versión | Refencia del cambio |
|  |  | 1 | Borrador inicial para revisión/discusión |
|  |  |  |  |
|  |  |  |  |

Reviewers

Table : Reviewers

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

Tabla de contenidos

[1 Solution Design Summary 0](#_Toc454807483)

[1.1 Audience 0](#_Toc454807484)

[2 Detailed Solutions Design 1](#_Toc454807485)

[2.1 Solutions Architecture Overview 1](#_Toc454807486)

[2.2 Active Directory Domain Services 1](#_Toc454807487)

[2.2.1 Solution Architecture—Domain Controllers 2](#_Toc454807488)

[2.3 Solution Sizing 3](#_Toc454807489)

[2.3.1 Sizing—ATA Center 3](#_Toc454807490)

[2.3.2 Sizing—ATA Gateways 4](#_Toc454807491)

[2.3.3 Domain Controller Analysis for Sizing 6](#_Toc454807492)

[2.3.4 ATA Components Required for Solution Design 6](#_Toc454807493)

[3 Solution Configuration 8](#_Toc454807494)

[3.1 Certificate Configuration 8](#_Toc454807495)

[3.2 ATA Center 8](#_Toc454807496)

[3.2.1 Hardware Configuration 8](#_Toc454807497)

[3.2.2 Network Ports 9](#_Toc454807498)

[3.3 ATA Lightweight Gateway 10](#_Toc454807499)

[3.3.1 Hardware Configuration 10](#_Toc454807500)

[3.3.2 Network Ports 11](#_Toc454807501)

[3.4 ATA Gateway 11](#_Toc454807502)

[3.4.1 Hardware Configuration 11](#_Toc454807503)

[3.4.2 Network Ports 12](#_Toc454807504)

[3.4.3 Port-Mirroring Considerations 13](#_Toc454807505)

[3.4.4 Port-Mirroring Configuration—Hyper-V 14](#_Toc454807506)

[3.5 ATA Configuration 15](#_Toc454807507)

[3.5.1 ATA General Configurations 15](#_Toc454807508)

[3.5.2 ATA Gateways Configuration 16](#_Toc454807509)

[3.5.3 ATA Detection Configurations 16](#_Toc454807510)

[3.5.4 Email Server Configuration 18](#_Toc454807511)

[3.5.5 Syslog Server Configurations 19](#_Toc454807512)

[3.5.6 Notification Settings 19](#_Toc454807513)

[3.6 Additional Network Configuration Information 20](#_Toc454807514)

[3.6.1 Endpoint or Device Firewall Configuration 20](#_Toc454807515)

[3.7 Event Collection 21](#_Toc454807516)

[3.7.1 Configuration of ATA Gateway to Listen for SIEM Events 21](#_Toc454807517)

[3.7.2 Configuration of Windows Event Forwarding 21](#_Toc454807518)

## Tablas

[Table 1: Change Record 3](#_Toc454807519)

[Table 2: Reviewers 3](#_Toc454807520)

[Table 3: Active Directory Configuration Items 2](#_Toc454807521)

[Table 4: Domain Controller Information 3](#_Toc454807522)

[Table 5: ATA Center Sizing 3](#_Toc454807523)

[Table 6: ATA Gateway Sizing 5](#_Toc454807524)

[Table 71: ATA Center Hardware for <type forest FQDN here> 9](#_Toc454807525)

[Table 82: Requirements—ATA Center Network Ports 10](#_Toc454807526)

[Table 93: Requirements—ATA Gateway Hardware 10](#_Toc454807527)

[Table 104: Requirements—ATA Lightweight Gateway Network Ports 11](#_Toc454807528)

[Table 115: Requirements—ATA Gateway Hardware 12](#_Toc454807529)

[Table 128: Port-Mirroring Configuration 15](#_Toc454807530)

[Table 13: ATA Center Configuration 15](#_Toc454807531)

[Table 14: ATA Console Configuration 15](#_Toc454807532)

[Table 15: ATA Gateway Configuration 16](#_Toc454807533)

[Table 16: ATA Gateway Configuration Details 16](#_Toc454807534)

[Table 179: Short-Term Lease Subnets 17](#_Toc454807535)

[Table 183: Email Alerting Configuration 18](#_Toc454807536)

[Table 19: Syslog server configuration 19](#_Toc454807537)

[Table 20: Email notifications configurations 19](#_Toc454807538)

[Table 21: Syslog notification settings 20](#_Toc454807539)

[Table 224: Endpoint Firewall Configuration 20](#_Toc454807540)

[Table 236: Windows Event Forwarding—Domain Controllers to Gateway 22](#_Toc454807541)

## Figuras

[Figure 1: High-Level ATA Design 1](#_Toc454807542)

**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. Resumen del diseño de la solución

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.

Esta solución está diseñada para reunir los requerimientos u objetivos que fueron definidos en el documento de Visión y Alcances.

Los objetivos para el diseño de la solución incluyen:

**Instructions:** Please update the following goals to match your customer’s goals for the project. These should have been collected during the Envision phase and documented in the Vision and Scope document.

* Diseñar una solución que esté basada en una visión compartida y que reúna los requerimientos de Customer Name
* Crear un diseño que esté basado en los elementos de configuración que fueron acordados en el taller de diseño de la solución.
  1. Audiencia

Este documento de diseño de la solución está enfocado en los equipos de Customer Name que son responsables del diseño, implementación y operación de la solución Microsoft Advanced Threat Analytics (ATA).

1. Diseño Detallado de la Solución
   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.

Figura 1 ilustra la arquitectura del diseño de la solución.

Figura 1: Diseño de ATA a alto nivel

* 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.

La siguiente tabla indica la configuración de la infraestructura de Active Directory Domain Services (AD DS) de Customer Name para la que ATA proveerá servicios de detección.

Tabla 3: Elementos de configuración de Active Directory

|  |  |  |
| --- | --- | --- |
| Forest DOM\_BCI\_PROD.CL | | |
| Elemento | Detalles | Configuración |
| Número de controladores de dominio | El número de controladores de dominio que serán monitoreados con ATA. Ver requerimientos de Port Mirroring. | Domain Controllers |
| Sistema Operativo de los Domain Controller | Los sistemas operativos estándar de Customer Name en todos los Domain Controllers. | Escribir version/versiones OS aquí |
| Ubicación de los Domain Controller | Ubicación de los Domain Controllers de Customer Name donde se requiere que ATA entregue servicios de detección. | Escribir la ubicación del datacenter aquí |
| Usuario estándar | * Una cuenta de usuario y su contraseña de Active Directory que tenga el permiso de lectura a **todos los objetos** en el dominio a monitorear * Esta cuenta debería ser bloqueada de forma que no tenga permitido tener capacidades de logon interactivo sobre cualquier sistema dentro del forest. | Escribir nombre de usuario aquí. Dominio/nombredeusuario |
| Opcional:   * Usuario estándar   (solo lectura) – Contenedor Objetos Eliminados | Una cuenta de usuario de Active Directory (puede ser el mismo indicado anteriormente) que debería tener acceso de solo lectura al contenedor Objetos Eliminados. Esto permitirá que SATA detecte la eliminación masiva de objetos en el dominio además de actualizar a ATA sobre los objetos eliminados. | Escribir nombre de usuario aquí. Dominio/nombredeusuario |
| Opcional:   * Usuario estándar – Honey Token | Una cuenta de usuario que no tenga actividades en la red. Esta cuenta será configurada como el usuario de ATA Honey Token. Para configurar el usuario Honey Token, se necesitará el SID de la cuneta de usuario, no el nombre de usuario. | Escribir nombre de usuario aquí. Dominio/nombredeusuario  Ver la guía de operaciones para obtener el SID usando PowerShell |

* + 1. Arquitectura de Solución—Domain Controllers

Para entregar servicios de detección más confiables, ATA puede monitorear el tráfico desde y hacia los domain controllers (DC). La siguiente tabla entrega la información referente a los DC que ATA monitoreará, incluyendo la información de fully qualified domain name (FQDN) y la ubicación del datacenter.

**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.

Tabla 4: Información de los Domain Controller

|  |  |  |  |
| --- | --- | --- | --- |
| DC FQDN | Nombre del Forest | Nombre del Dominio | Ubicación del Datacenter |
| DC1.contoso.com | Contoso.Com | Contoso.Com | Contoso HQ |
|  |  |  |  |

* 1. Dimensionamiento de la Solución

**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.

La siguiente tabla describe el dimensionamiento de la solución.

* + 1. Dimensionamiento—ATA Center

La siguiente información entrega recomendaciones de dimensionamiento de sistemas para el ATA Center. El tamaño del ATA Center dependerá de cuanto tráfico de red basado en los DC se genere y en como muchas de las actividades sospechosas que ATA detecta son almacenadas en la base de datos. La siguiente tabla provee delineamientos generales que pueden ayudar a determinar el tamaño del ATA Center.

Se recomienda obtener datos por 30 días en el ATA Center para determinar el comportamiento normal de los usuarios y producir análisis de comportamiento. El espacio requerido por la base de datos de ATA (sobre la base de un DC) está definido en la siguiente tabla. Las recomendaciones están basadas en las estadísticas especificadas por Customer Name.

Esta metodología será utilizada para determinar los requerimientos de hardware para el ATA Center. La información será documentada en la sección 2.4.1 de este documento.

Más información sobre dimensionamiento de ATA puede ser encontrada en el siguiente artículo de Technet “[ATA Capacity Planning](https://docs.microsoft.com/en-us/advanced-threat-analytics/plan-design/ata-capacity-planning)”.

Tabla 5: Dimensionamiento de ATA Center

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Paquetes por Segundo\* | CPU (Cores\*\*) | Memoria (GB) | Almacenamiento por día (GB) | Almacenamiento por mes (GB) | IOPS\*\*\* |
| 1,000 | 2 | 32 | 0.3 | 9 | 30 (100) |
| 10,000 | 4 | 48 | 3 | 90 | 200 (300) |
| 40,000 | 8 | 64 | 12 | 360 | 500 (1,000) |
| 100,000 | 12 | 96 | 30 | 900 | 1,000 (1,500) |
| 400,000 | 40 | 128 | 120 | 1,800 | 2,000 (2,500) |

\* Total diario en promedio de paquetes por segundo de todos los DC que serán monitoreados por todos los ATA Gateways

\*\* Esto incluye cores físicos, no hyper-threaded.

\*\*\* Número promedio (números peak)

**Notas:**

El ATA Center puede manejar un máximo de 400.000 frames por segundo (FPS) desde todos los DC monitoreados.

Los valores de almacenamiento indicados acá son valores netos, se debería considerar siempre el crecimiento futuro y asegurarse que el disco donde reside la base de datos tenga un 20% de espacio libre.

Si el espacio disponible alcanza un mínimo de 20% o 100GB, la colección de datos más antigua será eliminada. Esto continuará ocurriendo hasta que solo queden dos días de datos o el espacio disponible sea un de 5% o 50GB, en ese punto la recolección de datos se detendrá.

La latencia del storage para actividades de lectura y escritura debería ser inferior a 10ms.

El ratio entre las actividades de lectura y escritura es aproximadamente 1:3 bajo los 100.000 paquetes por segundo y 1:6 sobre los 100.000 paquetes por segundo.

* + 1. Dimensionamiento—ATA Gateways
       1. ATA Lightweight Gateway

Un ATA Lightweight Gateway se instala sobre un Domain Controller y monitorea su tráfico directamente. Se recomienda utilizar un ATA Lightweight Gateway en vez de un ATA Gateway cada vez que sea posible, mientras que los DC cumplan con la tabla de dimensionamiento listada más abajo. Un ATA Lightweight Gateway puede soportar el monitoreo de sólo un domain controller.

La siguiente tabla entrega algunas sugerencias a alto nivel referentes a como dimensionar los DC en base al monto de tráfico enviado y recibido. Más información sobre dimensionamiento de ATA puede ser encontrada en el artículo de TechNet “[ATA Capacity Planning](https://technet.microsoft.com/en-us/library/mt429323.aspx)”.

Tabla 7: Dimensionamiento de ATA Lightweight Gateway

|  |  |  |
| --- | --- | --- |
| Paquetes por segundo\* | CPU (Cores\*\*) | Memoria (GB) |
| 1,000 | 2 | 6 |
| 5,000 | 6 | 16 |
| 10,000 | 10 | 24 |

**\*** Total promedio de horas de trabajo del número de paquetes por segundos desde los domain controllers que serán monitoreados por el ATA Lightweight Gateway específico

**\*\*** Hyper-threading debe estar deshabilitado

* + - 1. ATA Gateway

Un ATA Gateway puede soportar el monitoreo de múltiples domain controllers dependiendo del monto del tráfico de red de los DC que serán monitoreados. La siguiente tabla entrega sugerencias a alto nivel respecto a cómo dimensionar el ATA Gateway basado en el monto de tráfico de red enviado y recibido. Más información sobre dimensionamiento de ATA puede ser encontrado en el siguiente artículo de Technet “[ATA Capacity Planning](https://docs.microsoft.com/en-us/advanced-threat-analytics/plan-design/ata-capacity-planning)”.

Tabla 6: Dimensionamiento de ATA Gateway

|  |  |  |
| --- | --- | --- |
| Paquetes por segundo\* | CPU (Cores\*\*) | Memoria (GB)\*\*\* |
| 1,000 | 1 | 6 |
| 5,000 | 2 | 10 |
| 10,000 | 3 | 12 |
| 20,000 | 6 | 24 |
| 50,000 | 16 | 48 |

**\*** Total promedio de horas de trabajo del número de paquetes por segundos desde los domain controllers que serán monitoreados por el ATA Gateway específico. Además, el monto total de DC con port mirroring no puede exceder la capacidad de la tarjeta de interfaz de red (NIC) del ATA Gateway

**\*\*** El monto total de cores no hyper-thrading que el DC tiene instalado. Aun cuando hyper-threading es aceptado para el ATA Lightweight Gateway, cuando se está planeando la capacidad, se deberían contar los cores actuales y no los cores hyper-threading

**\*\*\*** Monto total de memoria que tiene instalada el DC

* + 1. Análisis de Domain Controller para Dimensionamiento

Como se indicó previamente, el tamaño del ATA Center y el número y ubicación de los ATA Gateway o ATA Lightweight Gateway depende de cuánto tráfico de red reciba un DC. Este tráfico es enviado al ATA Gateway o recolectado localmente por el ATA Lightweight Gateway para su distribución al ATA Center.

Como parte de las sesiones de diseño, el análisis fue completado para determinar cuántos paquetes en cada DC dentro del alcance se manejarían. La siguiente tabla entrega esta información.

**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://technet.microsoft.com/en-us/library/mt429323.aspx> to assist you with this process.

Table 8: Analyzed Packets per Second

|  |  |  |
| --- | --- | --- |
| Domain Controller FQDN | Paquetes por Segundo analizados | Comentarios |
| DC FQDN | #### |  |

* + 1. Componentes ATA requeridos para el diseño de la solución

El diseño de ATA, como se puede notar, esta principalmente basado en cuánto tráfico de red es generado desde y hacia los DC dentro del alcance. Haciendo uso de la información que fue obtenido durante el workshop de diseño, los componentes ATA requeridos para Customer Name son los siguientes.

**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.

Tabla 9: Componentes ATA del diseño de la solución

|  |  |  |  |
| --- | --- | --- | --- |
| Componente | Número | Ubicación | Detalles |
| ATA Center | 1 | Primary Datacenter | One ATA Center will be deployed to provide detection services for the contoso.com forest. |
| ATA Gateway | 2 | 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. |
| ATA Lightweight Gateway | 2 | 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 |

1. Configuración de la Solución

**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. Configuración de Certificados

La siguiente tabla resume la configuración de certificados que serán usados para el ATA Center y Gateway. Esos certificados serán emitidos por la autoridad internas de certificados de Customer Name.

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

Tabla 10: Configuración de certificados de ATA

|  |  |  |
| --- | --- | --- |
| Rol | Configuración del certificado | Detalles del certificado |
| Center | El ATA Center requiere certificados para los siguientes servicios:  Internet Information Services (IIS) – Certificado Web server – Certificado Client, Server authentication  ATA Center Service – Certificado Server authentication | Certificado Web server:  Enter in the ATA Portal FQDN:  e.g. ATAportal.contoso.com  Servicio ATA Center:  Enter the ATA Center Service URL. e.g. ATAservername.contoso.com |
| Gateway | Se requiere un certificado que soporte **Server Authentication** para instalarlo en el almacén computador del ATA Gateway (y ATA Lightweight Gateway) n en el almacenamiento Local Computer. Este certificado debe ser de confianza del ATA Center. | Enter in the specific URL for this certificate. |

**Note:** Certificados auto-firmados solo deberían ser usado para ambientes de laboratorio o de pruebas únicamente.

* 1. ATA Center

Esta sección detalla la configuración específica que es requerida por la implementación del ATA Center.

* + 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.

La siguiente sección muestra la configuración de hardware del ATA Center y Gateway.

**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.

La siguiente tabla entrega información sobre los recursos computacionales que serán necesarios para soportar la implementación de ATA Center.

Tabla 71: Hardware de ATA Center para <type forest FQDN here>

|  |  |  |
| --- | --- | --- |
| Componente | Detalles de Hardware de ATA Center | Configuración |
| Procesador | Ver sección dimensionamiento de ATA Center (tabla 5: dimensionamiento de ATA Center). | Update based on sizing exercise here |
| Memoria | Ver sección dimensionamiento de ATA Center (tabla 5: dimensionamiento de ATA Center). | Update based on sizing exercise here |
| Espacio en disco disponible  Almacenamiento de base de datos | Ver sección dimensionamiento de ATA Center (tabla 5: dimensionamiento de ATA Center). | Enter based on sizing exercise here  Record Database location here. Review operations and implementation guides for further requirements. Its recommended to move the database to dedicated disks and drive |
| Red | Un adaptador de red, dos direcciones IP:   * ATA service * ATA management (IIS) | 2 IP Addresses are required. Enter both IP addresses that will be used here:  ATA Service IP: x.x.x.x  ATA Management IP (IIS): x.x.x.x |
| Máquina virtual  Computador físico | La instalación del ATA Center como una máquina virtual es soportada.  <<Update this section to reflect choice reasoning>> | Physical or Virtual |
| BIOS | La base de datos de ATA requiere que Customer Name DESHABILITE nonuniform memory access (NUMA) en el BIOS. | Confirm Disabled (Y, N) and add commentary if the answer is “N”. |

* + 1. Puertos de red

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

La siguiente tabla indica los puertos de red mínimo requeridos por el ATA Center.

Tabla 82: Requirements—ATA Center Network Ports

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Protocolo | Transporte | Puerto | Desde o hacia | Dirección | Dirección IP |
| SSL (ATA communications) | TCP | 443 | ATA Gateway | Inbound | ATA Center Service IP Address: x.x.x.x |
| HTTP | TCP | 80 | Red Customer Name | Inbound | Management IP (IIS) Address: x.x.x.x |
| HTTPS | TCP | 443 | Red Customer Name y ATA Gateway | Inbound | Management IP (IIS) Address: x.x.x.x |
| SMTP (optional) | TCP | 25 | SMTP server | Outbound | Management IP (IIS) Address: x.x.x.x |
| SMTPS (optional) | TCP | 465 | SMTP server | Outbound | Management IP (IIS) Address: x.x.x.x |
| Syslog (optional) | TCP | 514 | Syslog server | Outbound | Management IP (IIS) Address: x.x.x.x |

* 1. ATA Lightweight Gateway
     1. Configuración de Hardware

**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 effected, 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.

Un ATA Lightweight Gateway soportará y monitoreará son lo el DC donde está instalado. La siguiente tabla detalla el domain controller donde se instalará el ATA Lightweight Gateway.

Tabla 93: Requerimientos—Hardware de ATA Gateway

|  |  |  |  |
| --- | --- | --- | --- |
| Nombre Domain Controller | Paquetes por segundo | CPU (Cores) | Memoria (GB) |
| DCName | X,xxx | CPU Cores | Installed Memory |

* + 1. Puertos de Red

Tabla 104: Requerimientos—Puertos de red de ATA Lightweight Gateway

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Protocolo | Transporte | Puerto | Desde o hacia | Dirección |
| DNS | TCP y UDP | 53 | DNS Servers | Outbound |
| NTLM over RPC | TCP | 135 | Todos los dispositivos en la red | Outbound |
| NetBIOS | UDP | 137 | Todos los dispositivos en la red | Outbound |
| SSL | TCP | 443 | Update this cell to include the ATA Center service IP address and the ATA Console IP address.  ATA Center:  Dirección IP Center Service  Dirección IP IIS | Outbound |
| Syslog (opcional) | UDP | 514 | Servidor SIEM | Inbound |

**Nota:** Como parte del proceso de resolución realizado por el ATA Lightweight Gateway, los siguientes puertos necesitan ser abiertos inbound para los dispositivos de red desde los ATA Lightweight Gateways:  
 NTLM sobre RPC  
 NetBIOS

* 1. ATA Gateway
     1. Configuración de Hardware

**Instruction: i**f 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.

Un ATA Gateway soportará múltiples domain controllers y está basado en el monto de tráfico de red que los DC envíen y reciban, La siguiente configuración se definió.

Table 115: Requerimientos—Hardware de ATA Gateway

|  |  |  |
| --- | --- | --- |
| Componente | Detalles de Hardware de ATA Gateway | Configuración |
| Procesador | Ver sección de dimensionamiento de ATA Gateway (tabla 6: Dimensionamiento ATA Gateway). | Update based on sizing exercise here |
| Memoria | Ver sección de dimensionamiento de ATA Gateway (tabla 6: Dimensionamiento ATA Gateway). | Update based on sizing exercise here |
| Red | El ATA Gateway requiere dos o más adaptadores de red:   * Un **adaptador de administración** que será utilizado para comunicaciones con la red de la compañía. * Un **adaptador de captura** que será usado para capturar el tráfico desde y hacia los DC, | **Administración:**  Este adaptador será configurado de la siguiente forma:  Management IP: 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  **Captura:**  Este adaptador será configurado de la siguiente forma:  Dirección IP de captura: 1.1.1.1  Subred de captura: 255.255.255.255  Configurar el port mirroring para el adaptador de captura como el destino del tráfico de red del DC. |
| Máquina virtual  Computador físico | Update this section to reflect choice reasoning  La instalación del ATA Gateway en una máquina virtual es soportada si el DC que está siendo monitoreado también está siendo ejecutado en una máquina virtual en el mismo host de virtualización. | Type in “Physical” or “Virtual” depending on customer’s choice. If virtual, list the virtualization platform. |

* + 1. Puertos de Red

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

La siguiente tabla indica los requerimientos mínimos de Puerto que ATA Gateway requiere que sean configurados para el adaptador de administración.

Table 16: Requirements—Gateway Network Ports

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Protocolo | Transporte | Puerto | Desde o hacia | Direccción |
| LDAP | TCP y 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 y UDP | 88 | Domain controllers | Outbound |
| Netlogon | TCP y UDP | 445 | Domain controllers | Outbound |
| Windows Time | UDP | 123 | Domain controllers | Outbound |
| DNS | TCP y UDP | 53 | DNS Servers | Outbound |
| NTLM over RPC | TCP | 135 | Todos los dispositivos en la red | Outbound |
| NetBIOS | UDP | 137 | Todos los dispositivos en la red | Outbound |
| SSL | TCP | 443 | Update this cell to include the ATA Center service IP address and the ATA Console IP address.  ATA Center:  Dirección IP Center Service  Dirección IP IIS | Outbound |
| Syslog (opcional) | UDP | 514 | Servidor SIEM | Inbound |

* + 1. Consideraciones de Port-Mirroring

La principal Fuente de datos que ATA usa viene de la inspección en profundidad del tráfico de red desde y hacia los domain controllers. El port mirroring necesita ser configurado antes que ATA pueda acceder al tráfico de red. Port mirroring copia el tráfico desde el puerto origen al puerto destino. ATA funciona con la mayoría de las soluciones que puedes espejar el tráfico – si el port mirroring puede ser configurado para ATA, este puede ser usado para analizar amenazas al sistema.

La siguiente tabla muestra las consideraciones de ATA Gateway para port mirroring en escenarios de computadores físicos o máquinas virtuales.

Tabla 17: Consideraciones de Port-Mirroring

|  |  |  |
| --- | --- | --- |
| ATA Gateway | Domain Controller | Consideraciones |
| Virtual | Virtual sobre el mismo host | * El switch virtual necesita soportar port mirroring. * Mover una de las máquinas virtuales a otro host por sí mismo podrías causar que el port mirroring dejara de funcionar. |
| Virtual | Virtual sobre diferente hosts | Confirmar que el virtual switch soporte este escenario. |
| Virtual | Física | Se requiere un adaptador de red dedicado. De otra manera, ATA verá que el tráfico que va y viene del host, incluyendo el tráfico que se envíe al ATA Center. |
| Física | Virtual | Confirmar que el virtual switch soporte este escenario y que la configuración de port mirrroring de los switch físicos están basados en ese escenario.   * Si el host virtual está en el mismo switch físico, se necesitará configurar switch-level span. * Si el host virtual está en un switch físico diferente, se necesitará configurar un RSPAN o un ERSPAN\*. |
| Física | Física en el mismo switch | El switch físico debe soportar SPAN o port mirroring. |
| Física | Física en diferente switch | Esto requiere que el switch físico soporte RSPAN o ERSPAN\*. |

**\*** ERSPAN esta solo soportado cuando la desencapsulación está realizada antes que el tráfico sea analizado por ATA

Los ATA Gateway virtuales son requeridos para cada host de virtualización sobre el cual un domain controller virtual está ejecutándose.

Para configurar port mirroring, Customer Name necesitará referirse a la documentación del fabricante.

* + 1. Configuracíon Port-Mirroring—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.

La siguiente tabla muestra la configuración de Hyper-V que se utilizará en esta solución:

Tabla 8: Configuración Port-Mirroring

|  |  |  |  |
| --- | --- | --- | --- |
| Rol | Tipo | Nombre máquina virtual | Host de máquina virtual |
| Center | Destino | Enter VM Name | Enter Host Name |
| Gateway | Origen | Enter VM Name | Enter Host Name |

**Nota:** Esta es una característica del switch Microsoft Hyper-V que fue agregada en Windows Server 2012. Por este motivo, el host de virtualización necesita ejecutar (al menos) Windows Server 2012.

* 1. Configuración de ATA

La información en esta sección está configurada por medio del portal de ATA (esto es, la interfaz de administración) y ayudar a configurar ATA para verificar que está capturando información del ambiente de una manera eficiente.

* + 1. Configuraciones Generales de ATA

**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. These items are located under the “ATA General” section of the “Configuration” window.

* + - 1. ATA Center

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

Tabla 13: Configuración de ATA Center

|  |  |  |
| --- | --- | --- |
| Configuración | Valor | Comentarios |
| Dirección IP y Puerto de ATA Center |  |  |
| Certificado |  |  |
| Idioma |  |  |

* + - 1. Consola ATA

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

Tabla 14: Configuración de Consola ATA

|  |  |  |
| --- | --- | --- |
| Configuración | Valor | Comentarios |
| URL Consola ATA |  |  |

* + - 1. ATA Gateways

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

Tabla 15: Configuración ATA Gateway

|  |  |  |
| --- | --- | --- |
| Configuración | Valor | Comentarios |
| Conectividad del Dominio | Nombre de Usuario:  Dominio: |  |
| Actualización automática de ATA Gateways |  |  |

* + 1. Configuración de ATA Gateways

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

Tabla 16: Detalles de configuración de ATA Gateway

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nombre Gateway | Tipo Gateway | DC Monitoreados | Candidato a sincronizador del Dominio (Si/No) | Listener Syslog (Si/No) | Colector de Windows Event Forwarding (Si/No) | Comentarios |
| 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. |

* + 1. Configuraciones de Detección de ATA
       1. Subredes de arriendo a corto plazo

**Instruction:** Identify the subnets in which IP addresses are reassigned between devices within a very short period of time (seconds or minutes) and update the following table with appropriate information for each subnet.

ATA reduces the cache lifetime for all IP addresses in these subnets to accommodate the fast reassignment between devices. VPN or Wi-Fi networks are common examples of short-term lease subnets.

Subredes arrendadas a corto plazo son en las que las asignaciones de direcciones IP cambian dentro de segundos o minutos. Esto incluye las direcciones IP que están siendo usadas para VPN o redes Wireless. Es importante configurar ATA para reconocer esas subredes para evitar la posibilidad de que ATA marque actividades legítimas de esos dispositivos como sospechosas. Esto puede ayudar a que ATA no emita advertencias sobre actividades que son esperadas (esto es llamado identificación falso positivo).

ATA será configurado para considerar las siguientes subredes arrendadas a corto plazo.

**Instruction:** Update the following table with specific information about network subnets that ATA will exclude using the short-term lease configuration option.

Table 179: Short-Term Lease Subnets

|  |  |  |
| --- | --- | --- |
| Función de arriendo | Detalles | Rando Subnet/Bit |
| Enter Subnet ID/Name | Provide details about subnet | Enter Subnet Range and Bit Mask Info:  e.g. 1.2.3.4/24 |

* + - 1. Configuración Honey Token

Una cuenta honey token es una cuenta de usuario que ha sido creada para atraer a un atacante potencial. Esta cuenta es configurada típicamente para que parezca una cuenta con alto nivel de acceso pero que está configurada con mínimas capacidades y máximo monitoreo. Esta cuenta debería tener un nombre que sea atractivo, pero debe ser fuertemente bloqueada, por lo que, si llega a usar, no pueda hacer nada en el ambiente. Si se utiliza este tipo de cuenta, se debe verificar que la cuenta no tenga la posibilidad de iniciar sesión interactivamente o que pueda ser usada para enumerar el directorio.

ATA tiene la habilidad de monitorear la cuenta y alertar si está siendo usada. La siguiente tabla provee información acerca del usuario honey token que se configurará para que ATA la monitoree:

**Instructions:** Update the following table with the information of the honey token account that will be used for your customer’s ATA deployment. If monitoring more than one forest, please add additional rows.

Tabla 21: Configuración de Honey Token

|  |  |  |  |
| --- | --- | --- | --- |
| Nombre de cuenta | SID | Ubicación en Forest AD | Explicación |
| IMADomanAdmin | S-1-5-21-3557858698-2536648719-2954018678-1141 | Contoso.com | This account is located in the 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. |

* + - 1. Exclusiones de Reconocimiento de DNS

ATA puede determinar cuando alguien está intentando (como una posible táctica de ataque) capturar información del DNS. Este ataque a menudo consiste del intento de completar la transferencia de zona para obtener la información desde una zona DNS con el objetivo de obtener información valiosa sobre la red y sus dispositivos.

Este ataque podría ser confundido con una transferencia de zona legítima de un DNS a otro en el ambiente. Para evitar esta identificación inadecuada, ATA puede ser configurado para excluir direcciones como por ejemplo DNS Servers. No se debería generar una alerta si, o cuando, las actualizaciones son realizados a las zonas de bases de datos. La siguiente tabla muestra los sistemas que la configuración de ATA excluirá desde las actividades de reconocimiento del DNS.

**Instruction:** update the following table with a list of DNS servers that ATA will be configured to exclude from DNS reconnaissance reviews.

Tabla 20: Exclusiones DNS Server de Customer Name

|  |  |
| --- | --- |
| Nombre DNS Server | Direcciónes IP |
|  |  |

* + - 1. Exclusiones de Direcciones IP de Pass-the-ticket

**Instruction:** If the customer has Pass-the-ticket exclusions, please fill out this section. Otherwise remove the last sentence, delete the table and type a statement stating that the customer does not have any Pass-the-ticket exclusions.

Algunas aplicaciones pueden realizar autenticación de una forma que ATA determina que es una actividad sospechosa de Pass-the-ticket. Si después de la investigación, se determina que la aplicación está funcionando adecuadamente, se debería considerar excluirla desde la detección Pass-the-ticket. Para hacer esto, se debería agregar la dirección IP al listado de exclusión de la regla de detección de Pass-the-ticket. Para hacer esto, se debería agregar a la lista de exclusión de Pass-the-ticket la dirección IP del host donde la aplicación está ejecutándose. La siguiente tabla ilustra cuales áreas serán excluidas:

|  |  |
| --- | --- |
| Nombre de Servidor | Dirección IP |
|  |  |

* + 1. Configuración Mail Server

La siguiente tabla contiene la configuración de alerta de mail.

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

Tabla 183: Configuración de alerta de mail

|  |  |  |
| --- | --- | --- |
| Campo | Descripción | Valor |
| Servidor SMTP (requerido) | El FQDN del servidor SMTP. | For example: smtp.contoso.com |
| SSL | Indicar SSL si el servidor SMTP requiere SSL.   |  | | --- | | **System_CAPS_noteNota** | | **Si el administrador habilita SSL, Customer Name también necesitará cambiar el número de puerto.** | | Default is disabled |
| Autenticación | Habilitar si el servidor SMTP requiere autenticación.   |  | | --- | | **System_CAPS_noteNota** | | **Si Customer Name habilita la autenticación, el administrador debe entregar el nombre de usuario y la contraseña de una cuenta de correo que tenga permisos para conectarse al servidor SMTP.** | | Default is disabled |
| Enviar desde (requerido) | La dirección de correo desde donde se enviará la alerta. | For example: ATA@contoso.com |

* + 1. Configuraciones de Servidor Syslog

ATA puede ser configurado para reenviar información sobre actividades sospechosas detectadas a los sistemas SIEM. ATA puede enviar información usando dos formatos RFC específicos: 5424 y 3164. Esas configuraciones son específicas del sistema SIEM que tiene el cliente. La siguiente tabla lista las configuraciones para la integración del SIEM de Customer Name:

**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:

Tabla 19: Configuración servidor Syslog

|  |  |  |  |
| --- | --- | --- | --- |
| Servidor Syslog | Puerto | Transporte | Formato |
| Syslog.contoso.com | 514 | UDP | RFC5424 |

* + 1. Configuraciones de Notification
       1. Notificaciones de Correo

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

Esta sección indica la configuración de correo que será usada para la implementación de ATA en Customer Name. Utilizando esta configuración, ATA enviará alertas de correo usando las siguientes configuraciones:

Tabla 20: Configuraciones de notificación de Correo

|  |  |
| --- | --- |
| Valor | Configuración |
| Nueva detección de actividad sospechosa | Enabled |
| Nueva detección de incidente de salud |  |
| Nueva actualización esta disponible |  |
| Recipientes de correo |  |

* + - 1. Notificaciones de Syslog

**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.

Esta sección indica que la configuración de notificación de syslog que será usada para la implementación de ATA en Customer Name. Usando esta configuración, ATA enviará información a los servidores syslog usando las siguientes configuraciones:

Table : Syslog notification settings

|  |  |
| --- | --- |
| Valor | Configuración |
| Nueva detección de actividad sospechosa | Enabled |
| Actualización de actividad sospechosa existente |  |
| Nueva detección de incidente de salud |  |

* 1. Información Adicional de Configuración de Red

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

Esta sección entrega información de la configuración de red que puede ayudar con la implementación de la solución ATA para Customer Name.

* + 1. Endpoint o Configuración de Dispositivos de Firewall

Para proveer adecuadamente servicios de detección, ATA necesita acceso a la información sobre los dispositivos que existen en la red. Para hacer esto, una serie de puerto de red deben ser abiertos entre los ATA Gateways y los dispositivos que están ubicados en el ambiente que ATA está revisando. La siguiente tabla ilustra los puertos que deben ser abiertos si existen firewall entre el ATA Gateway y los dispositivos en el ambiente de red.

Tabla 224: Configuración de Endpoint Firewall

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nombre de puerto | Tipo | Puerto | Entidades | Dirección |
| NetBIOS | UDP | 137 | Todos los dispositivos sobre la red | Inbound |
| NTLM sobre RPC | TCP | 135 | Todos los dispositivos sobre la red | Inbound |

* 1. Colección de Eventos

**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.

Para mejorar la detección de ATA del intento de Pass-the-Hash, ATA requiere el evento de Windows con el ID 4776. Esto puede ser reenviado al ATA Gateway en una de dos vías, configurando el ATA Gateway para monitorear los eventos de SIEM o usando Windows Event Forwarding para capturar eventos Windows específicos que son registrados y capturados dentro de los registros de eventos de los domain controllers.

* + 1. Configuración de ATA Gateway para Escuchar Eventos de SIEM

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

Table 25: Configuración SIEM—Gateway

|  |  |  |
| --- | --- | --- |
| Dirección IP de escucha (Gateway) | Tipo de Puerto | Puerto (Por defecto) |
| <<EnterIPHere>> | UDP | 514 |

* + 1. Configuración de 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 puede colectar eventos desde computadores remotos y almacenarlos en registros de un computador local. La siguiente sección contiene la configuración para Customer Name relacionados con eventos específicos que han sido capturados a través de la creación de la subscripción.

La siguiente tabla lista los domain controller de Customer Name que serán usados para reenviar el ID de evento Windows 4776 a los ATA Gateway.

**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.

Table 236: Windows Event Forwarding—Domain Controllers to Gateway

|  |  |  |
| --- | --- | --- |
| Ítem de configuración | Computadores | Detalles |
| Origen | Enter DomainControllerFQDN | Domain controllers de origen |
| Colector | Enter ATAGateway FQDN | ATA Gateway |
| Nombre de la subscription | Enter Subscription Name | Creada sobre el colector |
| Registro de evento del grupo de lectura | Enter Source Computers FQDN | Creada sobre el colector |