ATAIS - Test Plan



Advanced Threat Analytics Implementation Services

Preparado para

[Type Customer Name Here]

Fecha

Versión 1 Draft

Preparado por

**[Update Author in Doc Properties]**

[Type Author Position Here]

[Type Author Email Here]

Contribuidores

**[Type Contributors Here]**

Revisión y hoja de firmas

Control de Cambios

|  |  |  |  |
| --- | --- | --- | --- |
| Fecha | Autor | Versión | Referencia del Cambio |
|  |  | 1 | Borrador inicial para revisión/comentarios |
|  |  |  |  |
|  |  |  |  |

Revisores

|  |  |  |  |
| --- | --- | --- | --- |
| Nombre | Versión Aprobada | Posición | Fecha |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Tabla de Contenidos

[1 Resumen de Casos de Prueba 1](#_Toc463389130)

[2 Enfoque de Casos de Prueba y Presunciones 3](#_Toc463389131)

[3 Especificación del Ambiente de los Casos de Prueba 4](#_Toc463389132)

[3.1 Planificación de los Casos de Prueba 4](#_Toc463389133)

[3.1.1 Alcance de Casos de Prueba 5](#_Toc463389134)

[3.1.2 Agendamiento 6](#_Toc463389135)

[3.2 Ambiente de Pruebas 7](#_Toc463389136)

[3.3 Requerimientos del Ambiente de Pruebas 7](#_Toc463389137)

[3.3.1 Requerimientos de Dimensionamiento 8](#_Toc463389138)

[3.3.2 Requerimientos de Hardware 9](#_Toc463389139)

[3.3.3 Requerimientos de Software 12](#_Toc463389140)

[3.3.4 Requerimientos de Pre Instalación 14](#_Toc463389141)

[3.4 Configuración del Ambiente de Pruebas 15](#_Toc463389142)

[3.4.1 Configuración de Red del Laboratorio 15](#_Toc463389143)

[3.4.2 Configuración del ATA Center 15](#_Toc463389144)

[3.4.3 Configuración del ATA Gateway 16](#_Toc463389145)

[4 Casos de Prueba y Resultados 18](#_Toc463389146)

[4.1 Casos de Prueba 18](#_Toc463389147)

[4.1.1 Caso de Prueba 1: Validar Port Mirroring 18](#_Toc463389148)

[4.1.2 Caso de Prueba 2: Validar Comunicaciones de Red Estables 19](#_Toc463389149)

[4.1.3 Caso de Prueba 3: Instalación de ATA Center 20](#_Toc463389150)

[4.1.4 Caso de Prueba 4: Configurar los Ajustes de Conectividad de Dominio de ATA Gateway 21](#_Toc463389151)

[4.1.5 Caso de Prueba 5: Descargar el Paquete de Instalación de ATA Gateway 22](#_Toc463389152)

[4.1.6 Caso de Prueba 6: Instalar el ATA Gateway 23](#_Toc463389153)

[4.1.7 Caso de Prueba 7: Configurar los Ajustes del ATA Gateway y Verificar que está Operacional 24](#_Toc463389154)

[4.1.8 Caso de Prueba 8: Configurar Subredes de Arriendo de Corto Plazo y Usuario Honeytoken 26](#_Toc463389155)

[4.1.9 Caso de Prueba 9: Alerta de ATA (Ajustes de Notificación) 27](#_Toc463389156)

[4.1.10 Caso de Prueba 10: Identificar y Trabajar con Alertas ATA y Actividades Sospechosas 28](#_Toc463389157)

[4.1.11 Caso de Prueba 11: Validar que ATA funciona adecuadamente 29](#_Toc463389158)

[4.1.12 Caso de Prueba 12: ATA Heath Center 31](#_Toc463389159)

[4.1.13 Caso de Prueba 13: Administración de la Base de datos 31](#_Toc463389160)

[4.2 Resumen de los Casos de Prueba 32](#_Toc463389161)

[5 Riesgos y Dependencias 35](#_Toc463389162)

[6 Incidentes Abiertos 36](#_Toc463389163)

Tablas

[Tabla 1: Elementos del alcance de los casos de prueba 5](#_Toc463389371)

[Tabla 2: Requerimientos – Dimensionamiento de ATA Center 8](#_Toc463389372)

[Tabla 3: Requerimientos – Dimensionamienot de ATA Lightweight Gateway 8](#_Toc463389373)

[Tabla 4: Requerimientos – Dimensionamiento ATA Gateway 9](#_Toc463389374)

[Table 5: ATA Center Configuration 9](#_Toc463389375)

[Tabla 6: Hardware de ATA Lightweight Gateway 10](#_Toc463389376)

[Tabla 7: Requerimientos—Hardware de ATA Gateway 11](#_Toc463389377)

[Tabla 8: Requerimientos—Software de ATA Center 12](#_Toc463389378)

[Tabla 9: Requerimientos—Software de ATA Gateway 13](#_Toc463389379)

[Tabla 10: Segmentos de Red del Laboratorio 15](#_Toc463389380)

[Tabla 11: Configuración del ATA Center 15](#_Toc463389381)

[Table 12: ATA Gateway Configuration 16](#_Toc463389382)

[Tabla 13: Caso de Prueba 1 18](#_Toc463389383)

[Tabla 14: Caso de Prueba 2 19](#_Toc463389384)

[Tabla 15: Caso de Prueba 3 20](#_Toc463389385)

[Tabla 16: Caso de Prueba 4 21](#_Toc463389386)

[Tabla 17: Caso de Prueba 5 22](#_Toc463389387)

[Tabla 18: Caso de Prueba 6 23](#_Toc463389388)

[Tabla 19: Caso de Prueba 7 24](#_Toc463389389)

[Tabla 20: Caso de Prueba 8 26](#_Toc463389390)

[Tabla 21: Caso de Prueba 9 27](#_Toc463389391)

[Tabla 22: Caso de Prueba 10 28](#_Toc463389392)

[Tabla 23: Caso de Prueba 11 29](#_Toc463389393)

[Tabla 23: Caso de Prueba 12 31](#_Toc463389394)

[Tabla 24: Caso de Prueba 13 31](#_Toc463389395)

[Tabla 25: Resultados de pruebas 33](#_Toc463389396)

[Tabla 26: Identificación de Riesgos 35](#_Toc463389397)

[Tabla 27: Indicentes Abiertos 36](#_Toc463389398)

Figuras

[Figura 1: Arquitectura a Alto Nivel 7](#_Toc463389416)

**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](http://office.microsoft.com/client/helppreview.aspx?AssetID=HA100375931033&QueryID=ALdFua2no0&respos=6&rt=2&ns=WINWORD&lcid=1033&pid=CH100487501033#3).

Template Guidance

Note there are samples of this document available. Please go to this [link](https://spsites.microsoft.com/sites/esaponline/Pages/Lessons_Learnt_Landing_Page.aspx?area=&discipline=&category=Deliverable%20Type%20%28SDM%29*&IsSubmitted=yes) to see a list.

The Test Plan template examines the processes as they exist in a live testing environment where the Planning > Defining > Performing/Executing > Reporting test flow is followed, keeping in mind that often you need to refine the test process as the product is constructed.

Description: The Test Plan describes the strategy and approach used to plan, organize and manage the project’s testing activities. It identifies testing objectives, methodologies and tools, expected results, responsibilities and resource requirements. This document is the primary plan for the testing team.

Justification: A Test Plan ensures that the testing process will be conducted in a thorough and organized manner that enables the team to determine the stability of the solution. A continuous understanding of the solution’s status builds confidence in team members and stakeholders as the solution is developed and stabilized.

Team Role Primary: Test is responsible for the creating the Test Plan. This plan outlines the strategy the team will take to test the solution. The test role is responsible for setting the quality expectations and incorporating those into the testing plan.

Team Role Secondary: Program Management participates in developing the test plan by ensuring that the solution requirements are met, the correct components are tested, and appropriate strategies are adopted for bug reporting and resolution. Development needs to understand how their work will be tested and how the bugs will be reported, assigned, resolved, and verified. User Experience verifies that the Test Plan contains the strategies and methods to test accessibility, usability and interface features.

1. Resumen de Casos de Prueba

Provide an overall summary of the contents of this document.

Justification: Some readers may need to know only the highlights of the plan, and summarizing creates that user view. It also enables the full reader to know the essence of the document before they examine the details.

Cuando se planea este tipo de proyectos, a menudo los equipos del proyecto se enfocan en la implementación de Microsoft Advanced Threat Analytics (ATA), el cual entregará inmediatamente beneficios en base a sus resultados y la aparente satisfacción de [Type Customer Name Here]. Enfocarse en la implementación de ATA en primer lugar pone a tareas como la planeación y la pre implementación como secundarias en orden de importancia. Un número significante de esos proyectos fallan, no debido a problemas relacionados con la tecnología, sino porque falta el entendimiento de como operar la tecnología y como llevar a cabo una simulación de tecnología desplegada en un ambiente de producción simulado. Esto es imperativo para una solución viable.

Para evitar fallas, el equipo de proyecto necesita probar el ATA antes que la tecnología sea desplegada y operada en el ambiente de producción actual. Esto se hace para:

* Determinar como la solución trabaja e interactúa con el ambiente de producción.
* Verificar las restricciones y suposiciones sobre ATA.
* Asegurarse que los elementos del diseño de la solución reúnan requerimientos de negocio antes de proceder con el despliegue en producción.

Es en el ambiente de pruebas, no en el entorno de producción, que los equipos se asegurarán que la solución de ATA funcionará como se espera. Esto validará que equipo de soporte entienda como operará la solución y como validar el diseño técnico de la solución. Cuando se realiza en un ambiente de prueba que simula el ambiente de producción exacto de [Type Customer Name Here], las pruebas indicadas en este documento pueden ayudar a construir un alto grade de confianza en la solución y en las habilidades y capacidades de los involucrados.

Creando un plan de pruebas y realizando buenas pruebas durante todo el proceso de implementación de la solución de ATA, [Type Customer Name Here] podrá:

* Minimizar el riesgo.
* Proporcionar personal de apoyo con los conocimientos y experiencia necesaria.
* Reducir los costos asociados con soluciones o elementos de diseño débiles o pobres.

Sin afectar al usuario, en un ambiente de prueba, los miembros del equipo técnico deberán:

* Observar el diseño de la solución en operación.
* Cambiar los ajustes de la configuración.
* Ajustar el diseño para confirmar un rendimiento mejorado.

1. Enfoque de Casos de Prueba y Presunciones

Use this section to describe at a high level the approach, activities, and techniques (including techniques for designing tests) to be followed in testing the solution. If different approaches are required for the solution’s various components, this section should define which components would be tested by each approach.

This section also describes the processes (criteria and techniques) that will be used to verify that the testing approach chosen will effectively guarantee the required degree of test completeness. A process could be as simple as requiring all appropriate groups to review, comment and sign off on the document. A process could be more complex, requiring the use of tools to verify statement and path coverage.

Las pruebas se realizaron en un ambiente de laboratorio aislado que representa la arquitectura de [Type Customer Name Here] tan real como sea posible para realizar las pruebas de verificación.

Una combinación de recursos Físicos y virtuales fueron usados para construir y administrar el ambiente. Este documento se complementa con las Guías de Implementación y Operación que forman parte de esta iniciativa.

1. Especificación del Ambiente de los Casos de Prueba

Use this section to detail the test plan including Team Model, Scope of the Test, and to set standards and requirements for the documentation to be generated during the process.

Justification: The Testing Team must decide on what tool/process to use for reporting the results of testing. A computer-based tool allows the coordinator to monitor test results, develop result reports that can be passed on to the core team and other stakeholders, and track testing status. The test team should also specify tools needed to monitor operating effects of the new release on the computing environment.

Es importante para el equipo de pruebas estabilizar y mantener el ambiente de pruebas como si fuera el ambiente real de [Type Customer Name Here]. Las pruebas adecuadas de un diseño de solución de ATA pueden ser solo realizados en un ambiente de prueba muy cercano al ambiente real. Coordinar el establecimiento del ambiente de pruebas con el equipo ayuda a determinar los requerimientos para espejar el ambiente real.

* 1. Planificación de los Casos de Prueba

El equipo de pruebas es responsable de desarrollar un plan de pruebas completo que incluya lo siguiente para cada prueba individual que sea llevada a cabo:

* Alcance del caso de prueba
* Agendamiento
* Riesgo
* Diseño de la prueba
* Requerimientos de documentación
* Requerimientos de recursos
* Resolución de problemas e incidentes
  + 1. Alcance de Casos de Prueba

Describe what will and will not be covered in the testing activity. Emphasize the testing areas where potential problems pose the greatest risk to the organization or have the greatest probability of occurring. As the Testing Team develops the test designs and gains a better understanding of the time required performing them, they will further refine the testing scope.

Justification: the objectives section should clearly state the test objectives so that anyone reviewing the documentation can easily understand what the testing is intended to accomplish. Clear and meaningful objectives also help shed light on the importance of the service the Testing Team is providing through their testing efforts. Modify this table as appropriate. TS= TEST CODE

Los siguientes elementos del alcance de las pruebas serán verificados como parte de este plan de pruebas.

Tabla 1: Elementos del alcance de los casos de prueba

| Código de Identificación | Elemento de Prueba | Detalles |
| --- | --- | --- |
| TC1 | Validar port mirroring. | Este elemento es un requerimiento para la implementación y operación de la solución para proveer detección de datos. |
| TC2 | Validar comunicaciones de red estables entre el ATA Center y los servidores Gateway. | No se instalarán componentes ATA en este momento, solo las pruebas de comunicación. |
| TC3 | Instalar el ATA Center. | Instalar ATA Center permitirá que el resto de la solución sea implementada exitosamente, |
| TC4 | Configurar los ajustes de conectividad con el dominio de los ATA Gateway. | Esto asegurará que ATA pueda ser configurado exitosamente y que sea capaz de catalogar entidades como usuarios, grupos y objetos de computador desde AD DS. |
| TC5 | Descargar el paquete de instalación de ATA Gateway. | Este paquete prepara al usuario para la instalación del ATA Gateway. |
| TC6 | Instalar el ATA Gateway. | Instalar el ATA Gateway exitosamente permitirá a la solución iniciar la intercepción del tráfico de red para analizarlo y alertar. |
| TC7 | Configurar los ajustes de ATA Gateway. | La habilidad de manipular los elementos de configuración de ATA Gateway. |
| TC8 | Configurar subredes de arriendo a corto plazo y usuario honeytoken. | **Opcional si esta configuración en el documento de Diseño de la Solución:** La configuración de subredes de arriendo a corto plazo, como las VPN, Wi-Fi y otras y la configuración de la cuenta honeytoken a través de su SID. |
| TC9 | Configurar las alertas de ATA (ajustes de notificación). | La capacidad de configurar las alertas vía mail cuando ATA detecta actividades sospechosas. Las alertas son enviadas a una lista de distribución o a un administrador. |
| TC10 | Identificar y trabajar con las alertas de ATA y las actividades sospechosas. | Actualizar, resolver o desechar alertas en la consola ATA. |
| TC11 | Instalar el ATA Heath Center. | El ATA Health Center entrega una visión de la salud del ATA. Esto incluye el estado de las comunicaciones entre el ATA Center y el ATA Gateway. |
| TC12 | Instalar la administración de la base de datos. | La habilidad de respaldar, restaurar y administrar la base de datos de ATA MongoDB. |

* + 1. Agendamiento

Draft schedule, including all of the tests listed in the Test Design section of the Overall Test Plan, to show when each test will be performed and who will perform it. If the test environment is being used for more than one purpose, the schedule can help testers coordinate availability with other possible testing teams. You can provide the project plan timeline here for the stabilization phase of this project.

El siguiente agendamiento muestra la línea de tiempo que será seguida para iniciar y completar la fase de pruebas de este proyecto.

<<Paste timeline for the stabilization phase here from the master project plan>>

* 1. Ambiente de Pruebas

Identify the approach and procedures that will be used for the initial phase of the test. This approach should define the steps of the setup process. The setup process should include the staging requirements for the testing and the procedures to initialize the testing matrix. Update the diagram below to reflect your customer’s testing environment.

El siguiente diagrama muestra la arquitectura a alto nivel implementada en un ambiente de laboratorio. Un mínimo de dos DC serán requeridos para este ambiente.

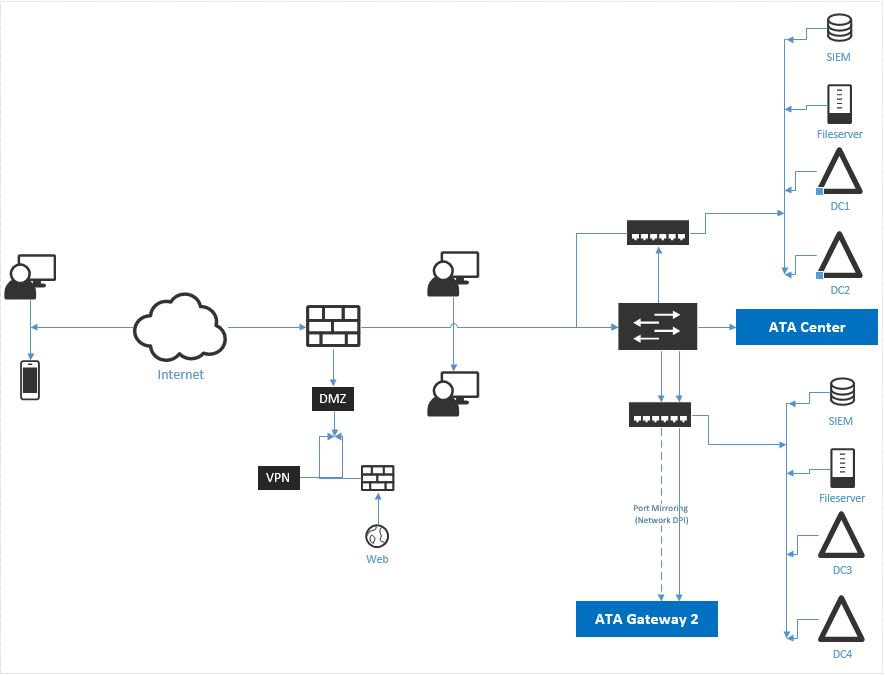


Figura 1: Arquitectura a Alto Nivel

* 1. Requerimientos del Ambiente de Pruebas

Update this section to reflect the relevant sizing of the testing environment.

* + 1. Requerimientos de Dimensionamiento
       1. ATA Center

Tabla 2: Requerimientos – 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)

* + - 1. ATA Gateway

Tabla 3: Requerimientos – Dimensionamienot 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 controladores de dominio 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

Tabla 4: Requerimientos – Dimensionamiento 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 controladores de dominio que serán monitoreados por el ATA Lightweight Gateway específico

\*\* Hyper-threading debe estar deshabilitado

* + 1. Requerimientos de Hardware
       1. ATA Center

La siguiente tabla muestra los requerimientos de hardware base para el ATA Center.

Table 5: ATA Center Configuration

| Componente | Requerimientos de hardware para ATA Center |
| --- | --- |
| Procesador | Revisar los requerimientos de dimensionamiento. |
| Memoria | Revisar los requerimientos de dimensionamiento. |
| Espacio disponible de disco  Almacenamiento de Base de Datos | Revisar los requerimientos de dimensionamiento. |
| Red | La comunicación entre el ATA Center y el ATA Gateway es encriptado por medio de SSL sobre el puerto 443. Adicionalmente, la consola de administración de ATA se ejecuta sobre IIS y es asegurada usando SSL sobre el puerto 443. **Dos direcciones IP** se requieren. El servicio de ATA Center asociará el puerto 443 a la primera dirección IP y el IIS asociará el puerto 443 a la segunda dirección IP. También se deben revisar los requerimientos de Puerto de Red en la siguiente tabla.  **Nota:** Se debe confirmar una conexión de red estable y efectiva entre el ATA Center y el Gateway, Ver los requerimientos de memoria del ATA Gateway.  **Nota:** Subredes de arriendo de corto plazo  Identificar las subredes en las cuales las direcciones IP son reasignadas entre dispositivos con un periodo de tiempo muy corto (segundos o minutos). ATA reduce el tiempo de vida del cache para las direcciones IP en esas subredes para acomodar la reasignación rápida entre dispositivos. Las redes VPN o inalámbricas son ejemplos comunes de subredes de arriendo de corto plazo. |
| Virtualización | La instalación del ATA Center en una máquina virtual está soportada. |
| BIOS | La base de datos de ATA requiere que [Type Customer Name Here] DESHABILITE NUMA en la BIOS. Algunos sistemas podrían referirse a NUMA como node interleaving. En ese caso, se debería HABILITAR node interleaving. |

* + - 1. ATA Lightweight Gateway

Tabla : Hardware de ATA Lightweight Gateway

| Componente | Requerimiento de Hardware de ATA Lightweight Gateway |
| --- | --- |
| Procesador | Revisar los requerimientos de dimensionamiento. |
| Memoria | Revisar los requerimientos de dimensionamiento. |
| Red | **Nota:** El ATA Lightweight Gateway monitorea el tráfico local sobre todos los adaptadores de red del controlador de dominio. Después de la implementación, se puede utilizar la consola de ATA si se quiere modificar cuales adaptadores serán monitoreados.  **Nota:** Como parte del proceso de resolución realizada por el ATA Lightweight Gateway, los siguientes puertos necesitan ser abiertos inbound sobre los dispositivos de la red desde el ATA Lightweight Gateway.   * NTLM over RPC * NetBIOS |
| Virtualización | La instalación del ATA Lightweight Gateway en una máquina virtual es soportada sobre Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 Standard Datacenter. EL Lightweight Gateway *no es soportado en Server Core*. El controlador de dominio puede ser un RODC. |

* + - 1. ATA Gateway

Un ATA Gateway puede soportar el monitoreo de múltiples controladores de dominio (dependiendo del monto de tráfico de red desde y hacia los DC), o un solo DC, donde ATA Lightweight Gateway está instalado.

Tabla 7: Requerimientos—Hardware de ATA Gateway

| Componente | Requerimientos de Hardware de ATA Gateway |
| --- | --- |
| Procesador | Revisar los requerimientos de dimensionamiento. |
| Memoria | Revisar los requerimientos de dimensionamiento.  **Nota:** El ATA Gateway usa la memoria para almacenar los datos capturados y enviarlos al ATA Center. Hay una configuración por defecto de 1.000.000 de entidades y es configurable. Dependiendo de la carga del DC conectado al ATA Gateway, la carga que se genere puede ser enorme.  **Precaución:** Si la comunicación entre el ATA Center y el ATA Gateway es interrumpida, el ATA Gateway almacenará en memoria 1.000.000 de entidades que pueden tomar hasta 5 GB de memoria. Una vez que el límite es alcanzado, se detendrá la colecta de tráfico de red hasta que la comunicación sea restaurada con el ATA Center. Dependiendo de la carga de DC, esto puede ser horas o minutos. |
| Red | El ATA Gateway requiere dos o más adaptadores de red.  **Adaptador de Administración:** Sera utilizado para comunicaciones sobre la red de la compañía. Este adaptador debería ser configurado con lo siguiente:   * Una dirección IP estática, incluyendo un default gateway. * DNS servers preferido y alternativo. * “DNS suffix for this connection” debería ser el nombre del DNS del dominio que está siendo monitoreado.   **Adaptador de captura:** Será usado para capturar el tráfico desde y hacia el DC:   * Configurar port mirroring en este adaptador como destino del tráfico de red del DC. * Configurar una dirección IP estática no ruteable en el ambiente sin default gateway y sin dirección de servidor DNS. Por ejemplo, 1.1.1.1/8. * Esto asegurará que el adaptador de captura de red pueda capturar el monto máximo de tráfico y que el adaptador de red de administración sea usado para enviar y recibir el tráfico de red requerido.   **Nota:** Subredes de arriendo de corto plazo  Identificar las subredes en las cuales las direcciones IP son reasignadas entre dispositivos dentro de un periodo de tiempo muy corto (segundos o minutos). ATA reduce el tiempo de vida de almacenamiento de esas direcciones IP en esas subredes para acomodar la reasignación rápida entre dispositivos. Las VPN o redes Wi-Fi son ejemplos comunes de subredes de arriendo de corto plazo. |
| Virtualización | La instalación del ATA Gateway en una máquina virtual es soportado cuando los DC que serán monitoreados también son ejecutados en máquinas virtuales en el mismo host.  **Importante:** No instale el KB 3047154 en el host de virtualización. Esto podría causar que el port mirroring no funcione adecuadamente. |

* + 1. Requerimientos de Software
       1. ATA Center

Esta sección proporciona los requerimientos de software para el ATA Center.

Tabla 8: Requerimientos—Software de ATA Center

| Componente | Requerimientos de Software de ATA Center |
| --- | --- |
| Certificados | ATA Center requiere certificados para los siguientes servicios:   * IIS, el que es un certificado de web server * ATA Center service, el que es un certificado de server authentication |
| Sistema Operativo | Use Windows Server 2012 R2 Standard o Datacenter  El ATA Center **NO PUEDE** ser instalado sobre un controlador de dominio. |
| Membresía de Dominio o Workgroup | El ATA Center puede ser instalado en un servidor que es miembro de un dominio o un workgroup. |
| Cuenta de Usuario | **Administrador local (no unida al dominio)**  **Cuanta de usuario estándar (unido al dominio)**—agregada a admin locales, ATA Administrators |
| Componentes | Los siguientes componentes son instalados y configurados durante la instalación del ATA Center:   * IIS * MongoDB * ATA Center service y Management IIS site * Data Collection set personalizados de Windows Performance Monitor * Certificados X.509 serán recomendaos y emitidos por una infraestructura interna de public key. Self-signed son solo recomendados para effects de prueba. |
| Soporte de Browser | El acceso a la consola de administración de ATA es por medio de un browser. Los siguientes browsers son soportados:   * Internet Explorer version 10 * Google Chrome 40 * La resolución mínima del ancho de pantalla es de 1700 pixeles |
| Microsoft Updates | Se debe asegurar que las últimas actualizaciones hayan sido instaladas en el servidor. |

* + - 1. ATA Gateway

Esta sección entrega información de los requerimientos de software para el ATA Gateway.

Tabla 9: Requerimientos—Software de ATA Gateway

| Componente | Requerimientos de Software de ATA Gateway |
| --- | --- |
| Certificados | El ATA Gateway requiere certificados para los siguientes servicios:   * Un certificado que soporte **Server Authentication** es requerido que se instale en el ATA Gateway en el almacenamiento de computador local. Este certificado debe ser confiable para el ATA Center. |
| Sistema Operativo | Windows Server 2012 R2 Standard o Datacenter si se está usando ATA Gateway.  Sólo el ATA Lightweight Gateway puede ser instalado sobre controladores de dominio Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 Standard o Datacenter. *Server Core no es soportado.* |
| Membresía de Dominio o Workgroup | El ATA Gateway puede ser instalado sobre un servidor que sea miembro de un dominio o un workgroup. The ATA Lightweight Gateway *debe* ser instalado sobre un DC. RODC están soportados. |
| Cuentas de usuarios | **Administrador Local (unido al dominio)**  **Cuenta de usuario estándar (unido al dominio)**—Agregado al Admin local, ATA Administrators.  **Cuenta de Servicio Estándar**—Usada para consultar el Active Directory para indexación y catalogación de objetos o entidades. (Conectividad del Dominio)  **Cuenta Honeytoken**—SID a ser usado (opcional). Una cuenta de usuario de un que no tenga actividades de red. Esta cuenta será configurada como el usuario ATA honeytoken. Para configurar el usuario honeytoken, se necesitará el SID de la cuenta, no el nombre de usuario.  **Opcional:** La cuenta estándar de servicios debería tener siempre permisos de solo-lectura sobre el contenedor de Objetos Eliminados. Esto permitirá que ATA detecte eliminación masiva de objetos en el dominio. Para información sobre la configuración de permisos de solo-lectura sobre el contenedor de Objetos Eliminados, revise la sección **Changing permissions on a deleted object container** en el artículo TechNet [View or Set Permissions on a Directory Object](https://technet.microsoft.com/library/cc816824(v=ws.10).aspx). |
| Componentes | Los siguientes componentes son instalados y configurados durante la instalación del ATA Gateway:   * KB 3047154 (No instale KB 3047154 sobre el host de virtualización. Esto puede causar que el port mirroring deje de funcionar.) * ATA Gateway service * Microsoft Visual C++ 2013 Redistributable * .NET Framework 4.6.1 * Data Collection set personalizados de Windows Performance Monitor |
| Microsoft Updates | Ejecutar Windows Update y asegurar que las últimas actualizaciones hayan sido instaladas antes de la instalación del ATA Gateway o ATA Lightweight Gateway. |
| Software de Seguimiento de Red | No instalar Microsoft Message Analyzer, Wireshark, u otro software de captura de red sobre el ATA Gateway. Si se necesita capturar tráfico de red, se debe instalar y usar Microsoft Network Monitor 3.4. |

* + 1. Requerimientos de Pre Instalación

1. Sobre el ATA Gateway, se debe asegurar que el [KB 2919355](http://support.microsoft.com/kb/2919355/) haya sido instalado. Para revisar si está instalado el hotfix, ejecutar el siguiente comando PowerShell: Get-HotFix -Id kb2919355.
2. Ver el apéndice de este documento para información adicional sobre la configuración de port mirroring. La sección de instalación de este documento asume que el port mirroring está configurado y está operativo.
3. Para validar port mirroring, se debe revisar la Guía de Operaciones de ATAIS como parte de este proyecto.
   1. Configuración del Ambiente de Pruebas
      1. Configuración de Red del Laboratorio

Tabla 10: Segmentos de Red del Laboratorio

|  |  |
| --- | --- |
| Nombre del Segmento de Red | Dirección IPv4 |
| Red de Laboratorio | <<10.0.0.0/24>> |
| Subredes de arriendo a corto plazo |  |
| Otras subredes |  |

* + 1. Configuración del ATA Center

Tabla 11: Configuración del ATA Center

| Componente | Detalles del Hardware del ATA Center | Configuración |
| --- | --- | --- |
| Procesador | Ver sección de dimensionamiento de ATA Center. | <<Basado en el dimensionamiento. Escribir acá>> |
| Memoria | Ver sección de dimensionamiento de ATA Center. | <<Basado en el dimensionamiento. Escribir acá>> |
| Espacio en disco disponible  Almacenamiento de base de datos | Ver sección de dimensionamiento de ATA Center. | <<Basado en el dimensionamiento. Escribir acá>>  <<Escribir la ubicación de la base de datos acá. Revisar las guías de implementación y operación para los requerimientos. Es recomendado mover la base de datos a un disco y unidad dedicada.>> |
| Red | Un adaptador de red, dos direcciones IP:  ATA Center service  ATA Management (IIS) | <<IP1>>  <<IP2>> |
| Máquina Virtual  Máquina Física | La instalación del ATA Center sobre una máquina virtual está soportado.  <<Actualizar esta sección para incluir una justificación razonable.>> | <<Virtual or Física>> |
| BIOS | La base de datos de ATA requiere que [Type Customer Name Here] DESHABILITE NUMA en el BIOS. | <<Confirmar que se deshabilite>> |

* + 1. Configuración del ATA Gateway

Table 12: ATA Gateway Configuration

| Componente | Detalles de Hardware de ATA Gateway | Configuración |
| --- | --- | --- |
| Processor | Ver sección de dimensionamiento de ATA Gateway. | <<Basado en el dimensionamiento. Escribir acá>> |
| Memory | Ver sección de dimensionamiento de ATA Gateway. | <<Basado en el dimensionamiento. Escribir acá>> |
| Available Disk Space | Ver sección de dimensionamiento de ATA Gateway. | <<Basado en el dimensionamiento. Escribir acá>> |
| Gateway Type | ATA Lightweight Gateway o ATA Gateway | <<Basado en el dimensionamiento. Escribir acá>> |
| Red | El ATA Gateway requiere dos o más adaptadores de red.  **Adaptador de Administración**: Será usado para comunicaciones sobre la red de la compañía.  **Adaptador de captura**: Será usado para capturar tráfico desde y hacia los controladores de dominio.  **Si se usa ATA Lightweight Gateway (preferido), se debe asegurar los requerimientos de hardware y dimensionamiento se cumplan.** | **Administración:**  Este adaptador será configurado de la siguiente manera:   * <<IP estática>> * <<Servidores DNS preferidos y alternativos >> * << “DNS suffix for this connection” debería ser el nombre del dominio monitoreado.>>   **Captura:**  Este adaptador será configurado de la siguiente manera:   * Configurar port mirroring para adaptador de captura como el destino del tráfico de red del controlador de dominio. * <<Configurar una dirección IP estática, no ruteable para el ambiente sin default gateway sin direcciones DNS. Por ejemplo, 1.1.1.1 /0.>> |
| Máquina Virtual  Máquina Física | La instalación del ATA Gateway sobre una máquina virtual está soportado siembre y cuando los DC que esté monitoreando sean máquinas virtuales sobre el mismo host de virtualización  <<Actualizar esta sección para incluir una justificación razonable.>> | <<Virtual or Física>> |

1. Casos de Prueba y Resultados

Use this section to provide a general description of the steps the tests will go through to ensure quality tests. Describe the detailed steps to be followed by testers during the testing cycle. Include a description of points where testing is suspended for documentation of results, expectations on re-initialization of the environment, and tests that are to be performed in sequence. Update the table below as the stages progress.

Remember, the customer will be signing and accepting this document so make sure you record your results thoroughly.

Esta sección muestra los pasos y resultados de las pruebas realizadas cuando se implementó ATA en un ambiente de laboratorio.

* 1. Casos de Prueba
     1. Caso de Prueba 1: Validar Port Mirroring

Tabla : Caso de Prueba 1

| Caso de Prueba 1: Validar Port Mirroring | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Descripción | El proceso para validar que port mirroring está configurado y funcionando apropiadamente. Este caso de Prueba no es requerido si se está usando ATA Lightweight Gateway. | | | | | |
| Pasos de la prueba | 1. Instalar [Microsoft Network Monitor 3.4](https://www.microsoft.com/download/details.aspx?id=4865) en el sistema ATA Gateway. 2. Ingresar el siguiente filtro: **Internet Control Message Protocol** (**ICMP),** y hacer clic en **Apply**. 3. Clic en **Start** para iniciar la sesión de captura. 4. Desde otro host en la red que esta el controlador de dominio, un ATA Center o ATA Gateway, iniciar la ventana de Consola de Comandos. 5. Ping (si ICMP está permitido) sobre el primer controlador de dominio que el ATA Gateway monitoreará continuamente por lo menos cinco minutos usando **ping <hostname or IP> -t.** 6. Cambiarse al ATA Gateway. 7. En el ATA Gateway, en el Network Monitor, validar que se pueda ver el requerimiento de ping que se está haciendo al controlador de dominio. 8. En el ATA Gateway, en el Network Monitor, validar que se puede ver la respuesta de ICMP que se envía desde el controlador de dominio al host que inició el proceso. | | | | | |
| Escenario de uso | Port mirroring esta operacional y configurado correctamente sobre los controladores de dominio. Si el port mirroring no funciona, se debe revisar la configuracíon de la red o el host virtual. | | | | | |
| Elementos de validación de los casos de prueba | **ID** | **Paso de Validación** | | **Resultado Esperado** | | **Resultado Actual** |
| 1.1 | Selecciones solo el adaptador de red de **Captura** o el adaptador de red que está conectado al puerto del switch que está configurado como el destino del port mirroring. | | Es importante asegurar que el administrador vea el tráfico desde y hacia los controladores de dominio que el ATA Gateway monitoreará. | |  |
| Resultados de la prueba | **Fecha de Prueba** | | **Probado por** | | **Resultado** | |
|  | |  | |  | |
| Comentarios |  | | | | | |

* + 1. Caso de Prueba 2: Validar Comunicaciones de Red Estables

Tabla : Caso de Prueba 2

| Caso de Prueba 2: Validar Comunicaciones de Red Estables | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Descripción | Esto es para asegurar que las comunicaciones entre el ATA Center y el ATA Gateway son estables sin tiempos de espera o con una latencia mínima. | | | | | |
| Pasos de la prueba | 1. Instalar [Microsoft Network Monitor 3.4](https://www.microsoft.com/download/details.aspx?id=4865) sobre el ATA Gateway. 2. Iniciar una venta de Consola de Comandos. 3. Ping (si el ICMP está permitido) sobre el primer controlador de dominio que el ATA Gateway monitoreará continuamente por lo menos cinco minutos usando **ping <hostname or IP> -t.** | | | | | |
| Escenario de uso | Revisar que las comunicaciones de red sean estables entre el primer DC, el ATA Center y el ATA Gateway. | | | | | |
| Elementos de validación de los casos de prueba | **ID** | **Paso de Validación** | | **Resultado Esperado** | | **Resultado Actual** |
| 2.1 | Ping | | Sin tiempo de espera de red con un 0% de paquetes perdidos. | |  |
| Resultado de la prueba | **Fecha de Prueba** | | **Probado por** | | **Resultado** | |
|  | |  | |  | |
|  | |  | |  | |
| Comentarios |  | | | | | |

* + 1. Caso de Prueba 3: Instalación de ATA Center

Tabla : Caso de Prueba 3

| Caso de Prueba 3: Instalación de ATA Center | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Descripción | Esto asegurará que el ATA Center ha sido instalado exitosamente y que la consola de ATA pueda ser accedida con éxito en la preparación de la configuración del ATA Gateway. | | | | | |
| Pasos de la prueba | 1. Iniciar sesión en el servidor de ATA Center con un usuario que sea miembro del grupo de administradores locales. 2. Desde una Consola de Comandos con privilegios de administrador, ejecutar el Microsoft ATA Center Setup.exe y seguir el asistente de instalación. 3. En la página **Welcome**, seleccionar el idioma y hace clic en **Next**. 4. Leer el End User License Agreement y, si se acepta, hacer clic en **Next**. 5. Sobre la página de configuración del ATA Center, ingrese la configuración basada en el documento de diseño de la solución. 6. Clic **Install** para instalar ATA y sus componentes y crear la conexión entre el ATA Center y la consola de ATA. 7. Después que la instalación se complete, hacer clic en **Launch** para conectar a la consola ATA. | | | | | |
| Escenario de uso | Instalación del ATA Center y verificación del éxito de la instalación. | | | | | |
| Elementos de validación de los casos de prueba | **ID** | **Paso de Validación** | | **Resultado Esperado** | | **Resultado Actual** |
| 3.1 | Verificar que el Servicio de ATA Center este ejecutándose escribiendo **Services.msc** sobre el menú Run del menú de inicio de Windows. | | Que el servicio de ATA Center se encuentre en un estado de ejecución | |  |
| 3.2 | Iniciar sesión con las mismas credenciales del usuario que se usó para instalar ATA Center. | | La primera ver que se inició sesión en la consola de ATA se pondrá automáticamente en la página **Domain connectivity settings** para continuar la configuración e instalación del ATA Gateway. | |  |
| 3.3 | Revisar el archivo de registro **Microsoft.Tri.Center-Errors.log**, el cual puede ser encontrado en la siguiente ubicación: %programfiles%\Microsoft Advanced Threat Analytics\Center\Logs. | | No debería haber errores en este archivo de registro. | |  |
| Resultados de la prueba | **Fecha de Prueba** | | **Probado por** | | **Resultado** | |
|  | |  | |  | |
|  | |  | |  | |
| Comentarios |  | | | | | |

* + 1. Caso de Prueba 4: Configurar los Ajustes de Conectividad de Dominio de ATA Gateway

Tabla : Caso de Prueba 4

| Caso de Prueba 4: Configurar los Ajustes de Conectividad de Dominio de ATA Gateway | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Descripción | Las configuraciones en la sesión de ajustes de conectividad de dominio aplican a los ATA Gateways administrados por el ATA Center. | | | | | |
| Pasos de la prueba | 1. Abrir la consola de ATA e iniciar sesión. 2. La primera vez que se inicia sesión en la consola ATA después de la instalación, automáticamente se redirigirá a la página de configuración del ATA Gateway. Si se necesita modificar las configuraciones posteriormente, hacer clic en Configuraciones y seleccionar **Configuration.** | | | | | |
| Escenario de uso | La habilidad para configurar los ajustes de conectividad de dominio en preparación a la instalación de los paquetes del ATA Gateway. | | | | | |
| Elementos de validación de los casos de prueba | **ID** | **Paso de Validación** | | **Resultado Esperado** | | **Resultado Actual** |
| 4.1 | En la página **Gateways**, haga clic sobre **Domain connectivity settings**, ingrese los elementos de configuración especificados en el diseño de la solución y haga clic en **Save**. | | Los ajustes de configuración deberían ser aceptados haciendo clic en **Save**. | |  |
| Resultados de la prueba | **Fecha de Prueba** | | **Probado por** | | **Resultado** | |
|  | |  | |  | |
|  | |  | |  | |
| Comentarios |  | | | | | |

* + 1. Caso de Prueba 5: Descargar el Paquete de Instalación de ATA Gateway

Tabla : Caso de Prueba 5

| Caso de Prueba 5: Descargar el Paquete de Instalación de ATA Gateway | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Descripción | Después de configurar los ajustes de conectividad de dominio, el administrador puede decargar el paquete de instalación de ATA Gateway. | | | | | |
| Pasos de la prueba | 1. Iniciar la sesión sobre el servidor de ATA Gateway. 2. Sobre la máquina ATA Gateway, abrir un browser e ingresar la dirección IP que se configuró en el ATA Center para la consola ATA. Cuando se inicie la consola ATA, haga clic en la opción **Settings** y seleccione **Configuration**. 3. En la pestaña **ATA Gateways**, haga clic **Download ATA Gateway Setup**. 4. Guardar el paquete localmente. | | | | | |
| Escenario de uso | Descargar el paquete ZIP exitosamente para configurar los servidores ATA Gateway. | | | | | |
| Elementos de validación de los casos de prueba | **ID** | **Paso de Validación** | | **Resultado Esperado** | | **Resultado Actual** |
| 5.1 | Descargar el paquete ZIP | | El paquete ZIP debería ser descargado exitosamente e incluir lo siguiente:   * Instalador de ATA Gateway * Ajustes de archivos de configuración con la información requerida para conectarse al ATA Center | |  |
| Resultados de la prueba | **Fecha de Prueba** | | **Probado por** | | **Resultado** | |
|  | |  | |  | |
|  | |  | |  | |
| Comentarios |  | | | | | |

* + 1. Caso de Prueba 6: Instalar el ATA Gateway

Tabla : Caso de Prueba 6

| Caso de Prueba 6: Instalar el ATA Gateway | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Descripción | Este caso de prueba confirma la instalación exitosa del ATA Gateway o ATA Lightweight Gateway. | | | | | |
| Pasos de la prueba | 1. Extraer los archivos desde el archivo ZIP. 2. Desde una Consola de comandos con privilegios de administrador, ejecutar el Microsoft ATA Gateway Setup.exe y seguir el asistente de instalación. 3. En la página **Welcome**, seleccione el idioma y haga clic en **Next**. 4. Bajo **ATA Gateway deployment type**, seleccione la configuración basada en el documento de diseño de la solución. | | | | | |
| Escenario de uso | Installation of the ATA Gateway or Lightweight Gateway and verifying access to the Gateway Console. | | | | | |
| Elementos de validación de los casos de prueba | **ID** | **Paso de Validación** | | **Resultado Esperado** | | **Resultado Actual** |
| 6.1 | Después de que la instalación se complete, haga clic en **Launch** para abrir el browser e iniciar sesión en la consola ATA. | | Inicie sesión con las mismas credenciales que se usaron para instalar el ATA Gateway. | |  |
| Resultados de la prueba | **Fecha de Prueba** | | **Probado por** | | **Resultado** | |
|  | |  | |  | |
|  | |  | |  | |
| Comentarios |  | | | | | |

* + 1. Caso de Prueba 7: Configurar los Ajustes del ATA Gateway y Verificar que está Operacional

Tabla : Caso de Prueba 7

| Caso de Prueba 7: Configurar los Ajustes del ATA Gateway y Verificar que está Operacional | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Descripción | Una vez que ATA Gateway está instalado, debe establecerse la configuración para el ATA Gateway y se necesita verificar la instalación. | | | | | |
| Pasos de la prueba | 1. Sobre la máquina con ATA Gateway, en la consola ATA, haga clic sobre **Configuration** y seleccione la página **ATA Gateways**. 2. Ingrese la configuración según el documento de diseño de soluciones. 3. Haga clic en **Save**. 4. Inicie sesión en la consola ATA y abra **Performance Monitor**. 5. En el árbol Performance, haga clic sobre **Performance Monitor,** luego clic en el signo más y **Add a Counter**. Expanda **Microsoft ATA Gateway** y se debe bajar hasta encontrar **Network Listener Captured Messages per Second** y agregarlo. | | | | | |
| Escenario de uso |  | | | | | |
| Elementos de validación de los casos de prueba | **ID** | **Paso de Validación** | | **Resultado Esperado** | | **Resultado Actual** |
| 7.1 | Al menos un DC en la lista debe ser servidor de catálogo global. Esto activará que ATA pueda resolver objetos de usuario y computador en otros dominios del forest. | | Los cambios en la configuración serán aplicados al ATA Gateway en la siguiente sincronización agendada entre el ATA Gateway y el ATA Center. | |  |
| 7.2 | Asegurarse que el primer DC **no** sea un RODC. | | RODC deberían ser agregados solamente después que se complete la sincronización inicial. | |  |
| 7.3 | Revisar que el servicio ATA Gateway este ejecutándose escribiendo **Services.msc** desde el menú de inicio de Windows y seleccionando **Run**. | | El servicio de ATA Gateway está ejecutándose.  Después que se hayan guardado los ajustes de ATA Gateway, podrían pasar algunos minutos para que el servicio se inicie la primera vez debido a que construye el caché de los analizadores de captura de red usados por el ATA Gateway. | |  |
| 7.4 | Revisar el archivo “Microsoft.Tri.Gateway-Errors.log” ubicado en la siguiente carpeta: “%programfiles%\Microsoft Advanced Threat Analytics\Gateway\Logs”. | | Buscar las entradas con “transfer” o “service start.” | |  |
| 7.5 | Revisar el siguiente contador de performance de Microsoft ATA Gateway. | | **NetworkListener PEF Parser Messages/Sec**: Este contador sigue cuantos mensajes están siendo capturados por el ATA por segundos. El valor debería desde cientos a miles dependiendo del número de DC monitoreados y que tan ocupado esta cada DC. Valores de un dígito o dos podrían indicar un problema con la configuración de port mirroring. | |  |
| 7.6 | Revisar el siguiente contador de performance de Microsoft ATA Gateway | | **EntityResolver Activity**: Este valor debería estar en el rango de unos pocos cientos, cada pocos segundos. | |  |
| 7.7 | Verificar que el dominio, objetos del forest y catálogo de entidades se esté llevando a cabo. | | Se debería ver una lista de **Entities Recently Learned** en la barra de notificación en el lado derecho de la consola. | |  |
| 7.8 | Buscar un objeto en la barra de búsqueda. | | Como un usuario o un grupo en el dominio. Se debería resolver exitosamente. | |  |
| 7.9 | Performance monitor | | Se debe ver actividad en el gráfico. Se deben seguir los pasos del punto 5 de esta sección. | |  |
| Resultados de la prueba | **Fecha de Prueba** | | **Probado por** | | **Resultado** | |
|  | |  | |  | |
|  | |  | |  | |
| Comentarios |  | | | | | |

* + 1. Caso de Prueba 8: Configurar Subredes de Arriendo de Corto Plazo y Usuario Honeytoken

Tabla : Caso de Prueba 8

| Caso de Prueba 8: Configurar Subredes de Arriendo de Corto Plazo y Usuario Honeytoken | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Descripción | Subredes de arriendo de corto plazo son subredes en las cuáles la asignación de direcciones IP cambia rápidamente, dentro de segundos o minutos. Por ejemplo, direcciones IP usadas por la VPN o direcciones IP Wi-Fi.  Cuenta de usuarios Honeytoken son cuentas de Active Directory que son utilizadas para atraer atacantes al pensar que la cuenta es de valor entonces ellos se centran en la cuenta honeytoken cuando intentan robar credenciales. Si un atacante intenta usarla, ATA detectará la actividad sospechosa. | | | | | |
| Pasos de la prueba | 1. Desde la consola ATA, sobre la máquina del ATA Gateway, haga clic en el ícono de configuraciones y seleccione **Configuration**. 2. Bajo **Detection**, agregue las subredes de arriendo de corto plazo. Ingrese las subredes usando el formato de notación slash, por ejemplo: 192.168.0.0/24 y haga clic en el signo más. 3. Configurar exclusiones: Se pueden configurar las direcciones IP que serán excluidas de actividades sospechosas específicas. 4. Para encontrar un SID para un usuario, se debe ejecutar el siguiente comando Windows PowerShell -> Get-ADUser UserName –Properties. 5. Para el SID de la cuenta honeytoken, ingrese el SID para la cuenta de usuario que no tendrá actividad de red y haga clic en el signo más. Por ejemplo: S-1-5-21-72081277-1610778489-2625714895-10511. | | | | | |
| Escenario de uso | Configurar y guardar los ajustes de detección para subredes de arriendo de corto plazo y usuario honeytoken. | | | | | |
| Elementos de validación de los casos de prueba | **ID** | **Paso de Validación** | | **Resultado Esperado** | | **Resultado Actual** |
| 8.1 | Guardar las subredes de arriendo de corto plazo. | | La configuración debería ser guardada exitosamente después de los pasos 1-3. | |  |
| 8.2 | Enumerar el SID para el usuario honeytoken. | | Para encontrar el SID para un usuario, ejecutar el siguiente comando Windows PowerShell -> Get-ADUser UserName –Properties. | |  |
| 8.3 | Poblar el usuario honeytoken bajo la configuración de detección. | | El SID es aceptado exitosamente en la consola y guardado. Pasos 4-5. | |  |
| Resultados de la prueba | **Fecha de Prueba** | | **Probado por** | | **Resultado** | |
|  | |  | |  | |
|  | |  | |  | |
| Comentarios |  | | | | | |

* + 1. Caso de Prueba 9: Alerta de ATA (Ajustes de Notificación)

Tabla : Caso de Prueba 9

| Caso de Prueba 9: Alerta de ATA (Ajustes de Notificación) | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Descripción | ATA puede alertar al administrador cuando detecte una actividad sospechosa, incidente de salud o una actualización disponible por correo electrónico con un buen nivel de información de la alerta (frecuencia y detalles). Las pruebas de Syslog están fuera de alcance. | | | | | |
| Pasos de la prueba | 1. Sobre el servidor de ATA Center, haga clic en el ícono del escritorio **Microsoft Advanced Threat Analytics Management**. 2. Ingrese el nombre de usuario y la contraseña y haga clic en **Log in**. 3. Selecciones la opción de ajuste en la barra de herramientas y seleccionar **Configuration**. 4. Seleccionar **Notifications**. 5. Haga clic en **Email server settings** para activar las alertas por mail e ingresar la configuración especificada en el diseño de la solución. | | | | | |
| Escenario de uso | Configurar los ajustes para mail y tipo de notificación. ATA puede alertar al administrador cuando detecta una actividad sospechosa, incidente de salud, o actualización de software disponible. Pruebas de Syslog están fuera de alcance. Microsoft no pueden generar un escenario de “hackeo” para generar alertas. | | | | | |
| Elementos de validación de los casos de prueba | **ID** | **Paso de Validación** | | **Resultado Esperado** | | **Resultado Actual** |
| 9.1 | Configuración de Alertas | | La configuración de las alertas exitosamente guardadas. | |  |
| 9.2 | Alerta recibida por mail | | Una vez que ATA detectó una actividad sospechosa, incidente de salud o una actualización de software, debería ser recibida una alerta por el administrador. Se debe asegurar que el servidor Simple Mail Transfer Protocol (SMTP) tenga activo el relay para las direcciones IP del ATA Center y ATA Gateway. | |  |
| 9.2 | Tipo de notificación | | Se debe asegurar que el mail es recibido basada en el tipo de notificación previsto. | |  |
| Resultados de la Prueba | **Fecha de Prueba** | | **Probado por** | | **Resultado** | |
|  |  | |  | |  | |
|  | |  | |  | |
| Comentarios |  | | | | | |

* + 1. Caso de Prueba 10: Identificar y Trabajar con Alertas ATA y Actividades Sospechosas

Tabla : Caso de Prueba 10

| Caso de Prueba 10: Identificar y Trabajar con Alertas ATA y Actividades Sospechosas | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Descripción | Las actividades sospechosas son listadas en orden cronológico, con las actividades sospechosas en lo más alto de la línea de tiempo. | | | | | |
| Pasos de la prueba | 1. Después de iniciar sesión en la consola ATA, el administrador es automáticamente llevado a la pantalla **Suspicious Activities Time Line**. 2. El panel **Filter by** ubicado en el lado izquierdo de la pantalla, seleccionar uno de los siguientes: **All**, **Open**, **Resolved**, o **Dismissed**. 3. Para filtrar aún más la lista, seleccionar **High**, **Medium,** o **Low**. 4. Para actividades sospechosas que activan a [Type Customer Name Here] que entregue información, Las preguntas son abiertas automáticamente. 5. Sin embargo, si la respuesta del administrador es si, la actividad sospechosa podría ser descartada y las actividades futuras de este tipo desde el mismo computador podrían no generar una actividad sospechosa o generaran una actividad que sea descartada automáticamente. 6. Si el administrador de ATA no está seguro, haga clic en **Cancel** y se deberá hacer seguimiento con el dueño de la entidad. 7. El administrador puede cambiar el estado de una actividad sospechosa activamente haciendo clic en el estado actual de la actividad sospechosa y seleccionando uno de los siguientes estados: **Open**, **Resolved** o **Dismissed**. | | | | | |
| Escenario de uso | Activar ATA para aprender de la red de [Type Customer Name Here] y algunas actividades sospechosas (Reconocimiento DNS, Pass the Ticket, comportamiento anormal y ejecución anormal), requerir información para mejorar la detección de las actividades sospechosas detectadas. | | | | | |
| Elementos de validación de los casos de prueba | **ID** | **Paso de Validación** | | **Resultado Esperado** | | **Resultado Actual** |
| 10.1 | Actualizar la actividad | | El administrador puede actualizar exitosamente y proveer información dentro de una actividad. | |  |
| Resultados de la Prueba | **Fecha de Prueba** | | **Probado por** | | **Resultado** | |
|  | |  | |  | |
|  | |  | |  | |
| Comentarios |  | | | | | |

* + 1. Caso de Prueba 11: Validar que ATA funciona adecuadamente

Tabla : Caso de Prueba 11

| Caso de Prueba 11: Validar que ATA funciona adecuadamente | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Descripción | Correr una prueba simple para validar que ATA está recibiendo un evento sospechoso y marca una actividad sospechosa como resuelta. | | | | | |
| Pasos de la prueba | 1. Iniciar sesión en otro cliente (no en el ATA Gateway, Center o DC). 2. Ejecutar cmd.exe. 3. Escribir nslookup y presionar **Enter**. 4. Escribir ls domain.com donde domain.com es el nombre del dominio en su ambiente y presionar **Enter**. Esto desencadenará una actividad sospechosa de DNS, reconocimiento del uso de DNS en la **Suspicious Activities Time Line**. 5. Iniciar sesión en la consola de ATA. El administrador automáticamente será llevado a **Suspicious Activities Time Line**. 6. Validar que hay una actividad de **Reconnaissance using DNS** en la línea de tiempo. 7. Haga clic en **Details** para este evento sospechoso. 8. Haga clic en **Note** y escriba *Prueba:* *Validando la funcionalidad ATA.* Haga clic en **Save**. 9. Seleccionar **Open** y marcar la actividad sospechosa como **Resolved**. | | | | | |
| Escenario de uso | Para validar la red de [Type Customer Name Here] con una prueba simple de actividad sospechosa y seguir el proceso de agregar una nota y marcar como resuelta. | | | | | |
| Elementos de validación de los casos de prueba | **ID** | **Paso de Validación** | | **Resultado Esperado** | | **Resultado Actual** |
| 11.1 | Iniciar sesión en un cliente/servidor y ejecutar nslookup con las opciones indicadas. | | El administrador puede iniciar sesión exitosamente a un Sistema y ejecutar nslookup para realizar pruebas. | |  |
|  | 11.2 | Validar resultados en la consola ATA. | | Reconocimiento de actividad sospechosa usando DNS esta presente en la línea de tempo de las actividades. | |  |
|  | 11.3 | Agregar una nota y marcar el evento como resuelto. | | El evento debería estar marcado como resuelto. | |  |
| Resultadoos de la Prueba | **Fecha de Prueba** | | **Probado por** | | **Resultado** | |
|  | |  | |  | |
|  | |  | |  | |
| Comentarios |  | | | | | |

* + 1. Caso de Prueba 12: ATA Health Center

Tabla : Caso de Prueba 12

| Caso de Prueba 12: ATA Health Center | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Descripción | Informe sobre la salud general de la infraestructura ATA. | | | | | |
| Pasos de la Prueba | 1. Para comprobar la salud general del sistema, hacer clic en el ícono **Health Center icon en** en la barra de menú. 2. En la alerta, haga clic en **Open** y seleccione **Resolved** o **Dismissed**. | | | | | |
| Escenario de uso | El ATA Health Center le permite al administrador saber que existe un problema al levantar una alerta. | | | | | |
| Elementos de validación de los casos de prueba | **ID** | **Paso de Validación** | | **Resultado Esperado** | | **Resultado Actual** |
| 11.1 | Heath Center | | Le administrador debería ver exitosamente el Health Center y actualizar las alertas registradas en él, si las hay. | |  |
| Resultados de la prueba | **Fecha de Prueba** | | **Probado por** | | **Resultado** | |
|  | |  | |  | |
|  | |  | |  | |
| Comentarios |  | | | | | |

* + 1. Caso de Prueba 13: Administración de la Base de datos

**Instruction:** We recommend at minimum to test the backup procedure. Restore should only be done in a lab or isolated environment for testing and process refinement. Management – Robomongo is used to view the database.

Tabla : Caso de Prueba 13

| Caso de Prueba 13: Administración de la Base de datos | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Descripción | ATA utiliza una base de datos open-source con los acuerdos pertinentes como parte de la instalación de ATA. Esta base de datos es llamada MongoDB. MongoDB no entrega ninguna interfaz de administración (solo líneas de comando). **Nota:** Microsoft no soporta la modificación de la base de datos ATA. | | | | | |
| Pasos de la prueba | Respaldo o recuperación—referirse a [relevant MongoDB documentation](http://docs.mongodb.org/manual/administration/backup/).  Administración—referirse a [relevant Robomongo documentation](https://robomongo.org/). | | | | | |
| Escenario de uso | Respaldo, recuperación, administración (según se requiera) | | | | | |
| Elementos de validación de los casos de prueba | **ID** | **Paso de Validación** | | **Resultado Esperado** | | **Resultado Actual** |
| 12.1 | Respaldo | | El respaldo es existoso | |  |
| 12.2 | Restauración | | La restauración es exitosa y los servicios de ATA Center y ATA Gateway están ejecutándose. | |  |
| 12.3 | Administración | | La base de datos es accesible a través de Robomongo. | |  |
| Resultados de la prueba | **Fecha de Prueba** | | **Probado por** | | **Resultado** | |
|  | |  | |  | |
|  | |  | |  | |
| Comentarios |  | | | | | |

* 1. Resumen de los Casos de Prueba

TR = Test Results = Success/Failure,

Summary Comments = Summarize on the test case results as notes for the production deployment e.g. Challenges, failures, notes.

If port mirroring as example is on a pure virtual environment in a lab, but production will be a combination of virtual and physical port mirroring requirements, make a note here of your result during testing, but also make a note in the risk section later in this document.

Referirse a las guías de implementación y operación de ATAIS para los pasos detallados y verificar los elementos discutidos en esta sección.

Tabla 25: Resultados de pruebas

| Código de Identificación | Elemento de Prueba | Resultado de Prueba | Resumen de Comentarios |
| --- | --- | --- | --- |
| TR1 | Validar port mirroring. |  |  |
| TR2 | Validar que hay una comunicación de red estable entre los servidores ATA Center y Gateway. |  |  |
| TR3 | Instalar el ATA Center. |  |  |
| TR4 | Configurar los ajustes de conectividad del dominio de ATA Gateway. |  |  |
| TR5 | Descargar el paquete de instalación de ATA Gateway. |  |  |
| TR6 | Instalar el ATA Gateway. |  |  |
| TR7 | Configurar los ajustes del ATA Gateway. |  |  |
| TR8 | Configurar las subredes de arriendo de corto plazo y un usuario honeytoken. |  |  |
| TR9 | Configurar alertas de ATA (ajustes de notificación). |  |  |
| TR10 | Identificar y trabajar con las alertas de ATA y actividades sospechosas. |  |  |
| TR11 | Validar que ATA esté funcionando adecuadamente. |  |  |
| TR12 | Instalar el ATA Health Center. |  |  |
| TR13 | Instalar la herramienta de admnistración de base de datos |  | Esto es una prueba con terceras partes con procesos definidos con MongoDB y Robomongo. |

1. Riesgos y Dependencias

Use this section to identify three items: assumptions, risks, and dependencies. The assumptions are those that have been made while developing the test plan. The risks are those that arise from either the assumptions or they are anticipated during the testing process. For each risk, indicate the probable impact if the assumption turns out to be incorrect, and the measures employed to correct the situation. Dependencies include things such as the Development Plan and Functional Specification that will help create details for the test plan procedures. There is an example in the table below. Please modify or remove.

Justification: Identifying risks early enables the team to begin managing those risks. Some potential risks include:

* Problems with establishing a comprehensive test environment (that is, hardware)
* Inability to obtain the resources necessary to perform all tests adequately
* Inadequate time to perform detailed tests
* Changes not being made in a timely manner when errors are detected
* Poor designs
* Unplanned schedule changes
* RC = Risk Code

La siguiente tabla muestra los riesgos identificados como resultado de las pruebas realizadas por la solución ATA para [Type Customer Name Here].

Tabla 26: Identificación de Riesgos

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Código de Identificación | Elemento de Riesgo | Plan de Mitigación | Fecha de término de la mitigación | Impacto de la producción |
| RC1 | Port mirroring: Solamente redes virtuales en laboratorio. Producción requerirá una configuración de switch físico para port mirroring con redes virtuales. | [Type Customer Name Here] veriticará y probará la configuración de port mirroring. Los resultados serán compartidos para la aceptación del documento del plan de pruebas. | <dd/MM/yyyy> | [Type Customer Name Here] acepta este elemento como un riesgo en el ambiente de producción. |

1. Incidentes Abiertos

Use this section to identify any key concerns and tasks that need to be followed up on in order to ensure the plan’s completeness. OC=Open Issue Code

La siguiente tabla muestra los incidentes que continuarán abiertos a través de la implementación del producto y su efecto en el ambiente de producción.

Tabla : Indicentes Abiertos

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Código de Identificación | Elemento de Incidente Abierto | Plan de Mitigación (si existe) | Fech de Término de la Mitigación | Impacto en Producción |
| OC1 |  |  |  |  |