

DESCRIPCION DE LOS SERVICIOS OFRECIDOS

IMPLEMENTACION GFI EVENTS MANAGER

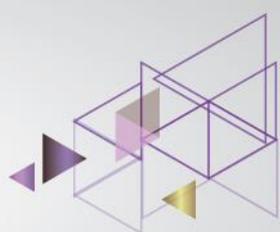
Modalidad de implementación

El objetivo de esta implementación es instalar la solución GFI Event Manager en la red del Banco Mariva, para recolección de eventos de servidores y dispositivos de red a los que se puede obtener.

Si el requerimiento es recolectar o recibir traps snmp de equipos, servidores o dispositivos ubicados en la DMZ, se deberá verificar en el firewall que los puertos que utiliza GFI Events Manager no estén bloqueados:

- Listado de Puertos utilizados por GFI EventsManager Server:
 - **Database Server Port: TCP 9292**
 - Puerto utilizado para conectar a la base de datos remota:
RPC Ports: TCP/UDP 7787-7788
 - Conexiones establecidas desde GFI EventsManager Server:
 - ❖ **HTTP Port: TCP 80**
 - ❖ **RPC Port: TCP/UDP 135**
 - ❖ **NetBIOS Port: TCP/UDP 139**
 - ❖ **SNMP Port: TCP/UDP 162**
 - ❖ **SMB Port: TCP 445**
 - ❖ **Syslog Port: TCP/UDP 514**
 - ❖ **SQL Port: TCP 1433**
 - ❖ **Oracle Port: TCP/UDP 1521**
 - ❖ **Ports: TCP/UDP 49153**

GFI - [Nota referencia fabricante](#)



DESCRIPCION DE LOS SERVICIOS OFRECIDOS

Alcance técnico - Tareas de implementación

- Instalación de una nueva instancia de GFI EventsManager.
- Instalación de una nueva base de datos local o remoto (SQL Server Client).
- Definición de credenciales para conectarse a las fuentes de logs remotas (Equipos Windows)
- Búsqueda de actualizaciones de la herramienta.
- Configuración de fuentes de eventos, logs y traps SNMP.
- Configuración de hasta 50 servidores/dispositivos para recolección de logs/envío de traps SNMP.
- Testeo de recolección de eventos, logs y traps SNMP.
- Clasificación de fuentes según tipo de servidor o dispositivo.
- Parametrización inicial de base de datos
- Optimización de base de datos para rotación programada automática.
- Testeo de generación de reportes predefinidos
- Configuración de 4 reportes personalizados
- Transferencia de conocimientos al administrador de la herramienta.

Limitaciones

- La implementación será realizada por uno de nuestros especialistas en horario laboral exceptuando días festivos oficiales.
- No se contempla instalación física, rackeo, cableado de red, ni conexión eléctrica del de ningún equipamiento.
- No se contempla la configuración de direccionamiento de traps SNMP y servicios syslog de dispositivos y o servidores, hacia la herramienta. Esta tarea debe ser ejecutada por el administrador del Banco.
- No se contempla verificaciones o modificaciones a firewalls, switches y dispositivos de red para asegurar la conectividad con la herramienta.

Requerimientos previos a la implementación

- Topología de red - incluyendo los firewalls que permiten acceso entre la red donde se encuentran los equipos afectados al presente proyecto.
- Listado validado de los equipos y/o dispositivos a monitorear con la herramienta.
- Asignación de personal técnico propio con teléfono y usuario de Skype



DESCRIPCION DE LOS SERVICIOS OFRECIDOS

Requerimientos de Hardware

Componente	Especificación
Procesador	2,5 GHz de 2 núcleos o superior
RAM	3 GB
Disco Duro	10 GB de espacio libre

Nota: el tamaño del disco duro depende de su entorno, el tamaño especificado en los requisitos es el mínimo requerido para instalar y archivar eventos.

Requerimientos de Software

1. Sistemas operativos admitidos (32 y 64 bits)

- Windows® Server 2012 - Foundation, Essentials, Standard o Datacenter
- Windows® Server 2008 - Standard o Enterprise
- Windows® Server 2008 R2 – Standard o Enterprise
- Windows® Server 2003 SP2 - Standard o Enterprise
- Windows® 8 - Standard, Professional o Enterprise
- Windows® 7 - Enterprise, Professional o Ultimate
- Windows® Vista SP1 - Enterprise, Business o Ultimate
- GFI EventsManager 2 Instalación de GFI EventsManager | 33
- Windows® XP Professional SP3
- Windows® SBS 2008
- Windows® SBS 2003

2. Otros componentes de software (Recomendado)

- Microsoft® .NET framework 4.0
- Microsoft® Data Access Components (MDAC) 2.8 o posterior
- Un servidor de correo (cuando se requieren alertas por correo electrónico)

Requisitos de almacenamiento

Los requisitos de almacenamiento a continuación están basados en el tamaño medio de un registro de eventos, que es de 535 bytes por evento:

Espacio Disco Duro	Número de eventos
Eventos almacenados por 1GB de espacio de almacenamiento	2 006 994
Eventos almacenados por 500 MB de espacio de almacenamiento	1 003 497 032



DESCRIPCION DE LOS SERVICIOS OFRECIDOS

Puertos y Protocolos de Firewall

La siguiente tabla contiene los puertos y protocolos que deben habilitarse en el firewall del host de GFI EventsManager:

Puerto	Protocolos	Descripción
135	UDP y TCP	Los equipos de destino utilizan este puerto para publicar información sobre los puertos dinámicos disponibles. GFI EventsManager utiliza esta información para poder comunicarse con los equipos destino.
139 y 445	UDP y TCP	GFI EventsManager lo utiliza para recuperar las descripciones del registro de eventos de las máquinas de destino.
162	UDP y TCP	GFI EventsManager lo utiliza para recibir capturas SNMAP. Asegúrese de que este puerto esté abierto en el equipo donde está instalado GFI EventsManager
514	UDP y TCP	GFI lo utiliza para recibir mensajes Syslog
1433	UDP y TCP	GFI EventsManager lo utiliza para comunicarse con el back-end de base de datos de SQL Server. Asegúrese de que este puerto esté habilitado en Microsoft SQL Server y en el equipo donde está instalado GFI EventsManager.

Puerto	Protocolos	Descripción
1521	UDP y TCP	Se utiliza para recopilar los registros de auditoría de Oracle Server. El puerto 1521 es el puerto predeterminado para esta conexión. Si el puerto se cambia manualmente en la configuración de Oracle Listener, ajuste la configuración del firewall según correspondencia.
49153	UDP y TCP	Utilizado por GFI EventsManager para recopilar eventos de orígenes de eventos con Microsoft Windows Vista o Microsoft Windows 7.

Excepciones del antivirus

- El tráfico no esté bloqueado en los puertos que usa GFI EventsManager
- **esmui.exe** y **esmproc.exe** tengan acceso permitido a través del firewall
- Las carpetas de GFI EventsManager se excluyan del análisis antivirus en tiempo real



DESCRIPCION DE LOS SERVICIOS OFRECIDOS

LIMITACIONES

- La implementación inicial será realizada de forma on-site.
- La implementación se realizara en días laborales de lunes a viernes de 9 a 18 Hs., horario de Argentina exceptuando días feriados nacionales.
- No incluye instalación de los sistemas operativos y aplicación de parches requeridos.
- Las configuraciones mencionadas en el presente alcance estarán limitadas a la cantidad de equipos mencionados en esta oferta.

TIEMPOS DE IMPLEMENTACION

Una vez cumplidos los requisitos iniciales, y necesarios para comenzar el proyecto se estiman para la presente propuesta hasta **5 (cinco)** días hábiles de trabajo on-site / remoto, según corresponda.

ENTREGABLES

ETAPA	DESCRIPCIÓN
INICIO DEL PROYECTO	Este documento será redactado al cierre de proyecto y servirá para validación y aprobación de las tareas realizadas durante la implementación. El mismo estará basado en el documento "Inicio de proyecto". Una vez consensuado y aprobado este documento se dará por finalizado el proyecto
CIERRE DEL PROYECTO	Este documento será redactado al cierre de proyecto y servirá para validación y aprobación de las tareas realizadas durante la implementación. El mismo estará basado en el documento "Inicio de proyecto". Una vez consensuado y aprobado este documento se dará por finalizado el proyecto

IMPORTANTE: Pasados 30 (treinta) días de la presentación y aprobación del documento "cierre de proyecto" no se aceptaran requerimientos o reclamos sobre los servicios realizados.

En los casos donde la contratación de servicios incluyera soporte técnico brindado por Nextvision S.R.L., los nuevos requerimientos serán interpretados como utilización del servicio de soporte técnico.