centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1221

Procedimiento de empleo seguro
Stormshield Endpoint Security Evolution

Mayo 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.02.08 17:00:46 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-131-6.
Fecha de Edición: mayo 2023.

LIMITACIÓN DE RESPONSABILIDAD

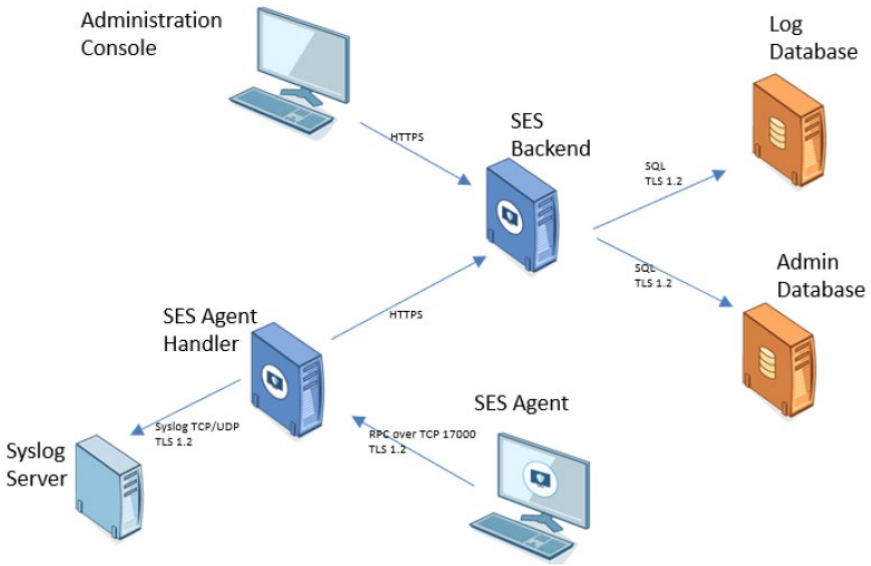
El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. ***SES Evolution*** es una solución de seguridad global que ofrece una protección completa de las estaciones de trabajo en organizaciones de todos los tamaños.
2. El agente SES Evolution se ejecuta en las estaciones de trabajo y las protege de ataques e intrusiones. El agente se configura en una consola de administración y está en contacto permanente con los gestores de agentes o agent handlers de SES Evolution que distribuyen las políticas de seguridad.
3. SES Evolution no trabaja con el reconocimiento de patrones ni de firmas de malware. Se centra en el análisis de comportamientos y procesos.
4. SES Evolution está compuesto por las siguientes componentes:
   - ***Agent Handler***. El gestor de agentes recibe datos y registros directamente de los agentes y actualiza la base de datos a través del backend.
   - ***Backend***. Servidor que centraliza todas las operaciones realizadas en el entorno de SES Evolution.
   - **Consola de administración**. Permite organizar, configurar y supervisar todos los agentes registrados. Además, se pueden establecer políticas de seguridad totalmente configurables, y los agentes se pueden segmentar en grupos para facilitar la administración. Con herramientas avanzadas que rastrean los registros y analizan los ataques, los administradores pueden supervisar el estado de sus agentes y rastrear el origen de los ataques detectados y bloqueados por los agentes de SES Evolution.
   - **Agente**. Software instalado en las estaciones de trabajo que proporciona protecciones de acuerdo a la política establecida por los administradores.



5. **Este producto ha sido cualificado e incluido en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) en la familia *Endpoint Detection and Response*. Consultar el CPSTIC para ver la versión que ha sido cualificada.**

2. OBJETO Y ALCANCE

6. El objetivo del presente documento es detallar las **configuraciones de seguridad del producto Stormshield Endpoint Security Evolution**, para su funcionamiento se realice de acuerdo con unas garantías de seguridad.
7. Stormshield Endpoint Security Evolution es un **producto *software*** cuya instalación se realiza en las estaciones de trabajo, mediante el uso de agentes y es administrado desde una consola de administración desplegada en el dominio.
8. Los requisitos mínimos necesarios para cada componente del producto mencionada en la sección inmediatamente anterior pueden ser consultados en la**[*Guía de instalación*]**.

3. ORGANIZACIÓN DEL DOCUMENTO

9. La organización del documento se compone de los siguientes apartados:

   - Apartado **4**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.
   - Apartado **5**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
   - Apartado **6**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.
   - Apartado **7**. En este apartado se incluye una lista de tareas a revisar para verificar que se han llevado a cabo cada una de las recomendaciones y configuraciones descritas en la presente guía de empleo seguro.
   - Apartado **8**. En este apartado se recogen las referencias utilizadas en la presente guía de empleo seguro.
   - Apartado **9**. En este apartado se recogen las abreviaturas utilizadas en la presente guía de empleo seguro.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

10. El producto es proporcionado por el fabricante desde el área de clientes *MyStormshield* en la sección *Downloads.* En dicha sección se puede descargar el *SES Evolution Installation Center* para la versión deseada.
11. Una vez descargado el instalador del producto, **se debe examinar la firma digital asociada al ejecutable y comprobar que está firmada por una entidad confiable**.

4.2 REGISTRO Y LICENCIAS

12. Las licencias determinan el número de agentes activos que se puede gestionar y tienen una fecha de caducidad. Se pueden importar varias licencias, en cuyo caso el número de agentes permitido es el número total de agentes de todas las licencias.
13. Las licencias se pueden importar desde la consola de administración en el menú *Licenses.*
14. En dicho menú, se debe hacer clic en *Add a license* y elegir los archivos proporcionados que se deseen importar.

4.3 CONSIDERACIONES PREVIAS

15. Las recomendaciones previas para una instalación estándar del producto son las descritas en este apartado.
16. Se recomienda hacer la instalación de forma acorde a la siguiente secuencia:
    - Instalación de las bases de datos.
    - Instalación del componente *backend.*
    - Instalación del componente *agent handler*.
    - Instalación de la consola de administración.
17. Las instalación y preparación del entorno de *Active Directory* y nombres de dominios debe ser preparada de forma previa a la instalación del producto.
18. Antes de instalar *SES Evolution*, se deben tener en cuenta las siguientes recomendaciones:
    - La consola, el componente *backend* y las bases de datos deben instalarse en hosts que pertenezcan al mismo dominio de *Active Directory*, o en dos dominios que tengan una relación de confianza.
    - SQL Server es necesario para instalar las bases de datos.
    - No se debe instalar el componente *backend* ni el *agent handler* en un controlador de dominio.
    - Se necesitan privilegios de administrador para instalar el producto.
    - Antes de instalar un servidor completo o el componente backend, se recomienda desactivar Windows Update y volver a activarlo después.

- En un componente *backend* o un *agent handler*, la carpeta "%PROGRAMDATA%\SES Evolution" debe excluirse del análisis antivirus en la estación de trabajo para optimizar el rendimiento. SES Evolution utiliza muchos archivos cab comprimidos que activan el análisis de antivirus.
- El agente de SES Evolution también puede instalarse en un componente backend o en un agent handler; una política de seguridad adecuada se proporciona por defecto para protegerlos.

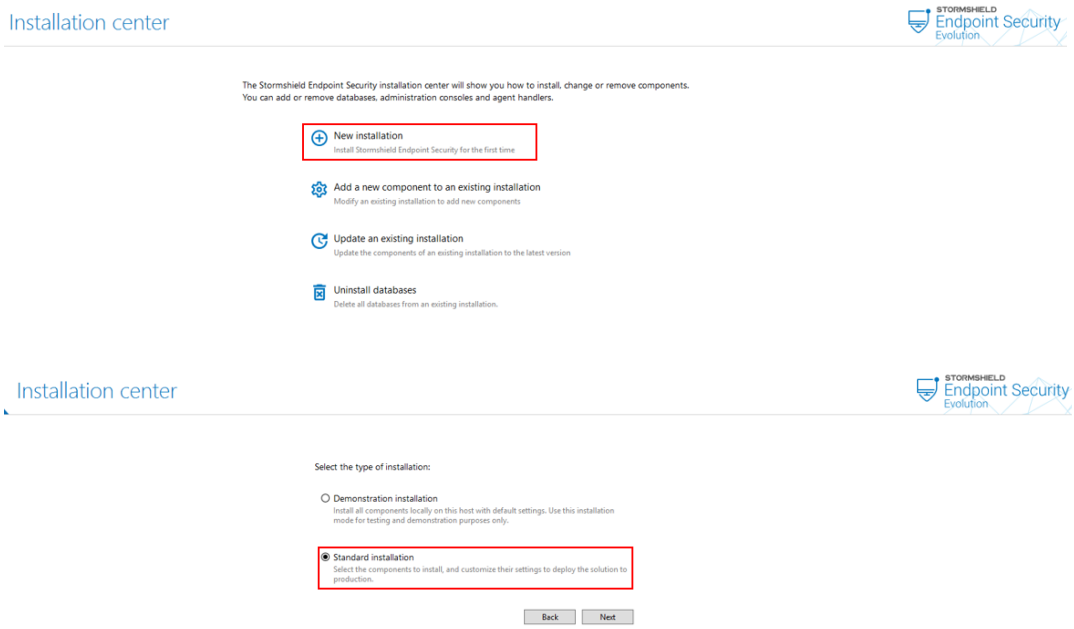
19. Los componentes de la solución pueden instalarse en la misma máquina o en máquinas separadas.
20. Para contrarrestar ciertas amenazas, será necesario importar las políticas con la versión de política 2204c o superior, para ello, se deberán seguir los pasos siguientes:
    - Abrir la consola de Stormshield SES.
    - Ir al menú Políticas y hacer clic en Importar.
    - Seleccionar los archivos de políticas a importar y hacer clic en Abrir.
    - Si algún agente ya está desplegado, ir al menú Entorno y desplegar el entorno.
21. En caso de no disponer de dichas políticas o consultas relacionadas, contactar con el soporte del fabricante.
22. Los siguientes recursos están disponibles en el sitio web de *Stormshield Technical* o en el sitio web del Instituto Stormshield. Se sugiere que se base en estos recursos para una mejor aplicación de todas las características de esta versión, así como el uso de las siguientes guías (ver apartado **8 REFERENCIAS**):
    a) [Guía de instalación]
    b) [Guía de administración]
    c) [Recomendaciones SQL Server]

4.4 INSTALACIÓN ESTÁNDAR

23. Las instalaciones estándar permiten utilizar *SES Evolution* en un entorno de producción. Se pueden instalar todos los componentes del producto en la misma máquina o repartirlos en varias máquinas, es importante tener en cuenta que tanto el componente *backend* como el componente *agent handler,* no pueden ser instaladas en un controlador de dominio, para más información respecto a requisitos de despliegue, consultar [Guía de instalación].
24. Para añadir uno o varios componentes de *backend,* consolas de administración y *agent handlers* posteriormente en otras máquinas, es necesario ejecutar el *SES Evolution Installation Center* en cada máquina y modificar la instalación existente añadiendo cada componente. Los equipos en los que se instalan las consolas de administración y los *agent handlers* deben ser capaces de comunicarse con el *backend*. El *backend* también debe poder comunicarse con las bases de datos.
25. Para realizar la instalación inicial del producto se deberá llevar a cabo el proceso descrito en lo que resta de sección.
26. En primer lugar, se deberá iniciar sesión en el equipo deseado con una cuenta de usuario Windows con las siguientes características:

- La cuenta de usuario debe pertenecer al dominio.
- Debe poseer privilegios de administrador.
- La cuenta de usuario debe tener el rol sysadmin en la instancia de la base de datos.

27. Una vez iniciada la sesión, se deberá hacer doble clic sobre el ejecutable del ***SES Evolution Installation Center.***
28. Una vez iniciado el instalador, se deberá hacer clic en la opción ***New installation*** y seleccionar ***Standard installation***.



29. En el siguiente menú, se deben indicar los parámetros de la base de datos, nombre de la instancia y el usuario para acceder a la base de datos. Seleccionando Windows como opción de autenticación se usará el usuario actual para llevar a cabo la conexión con la base de datos.
30. Además, se deberá configurar la base de datos de logs. Se puede indicar la misma instancia que para la base de datos de administración. En este menú se podrán configurar parámetros relacionados con la retención de logs. Es recomendable indicar un valor igual o superior a un mes, estos valores se pueden modificar posteriormente desde la consola de administración.
31. Se deben indicar además las contraseñas usadas para cifrar las claves privadas usadas para la generación de los certificados usados por el producto. Se recomienda hacer uso de contraseñas robustas con un mínimo de longitud de 12 caracteres que contenga caracteres alfanuméricos y símbolos especiales.
32. La cuenta de dominio con la que ha iniciado sesión se introduce por defecto como cuenta de superadministrador. El superadministrador es el usuario de la consola que permite crear otros usuarios. Debe pertenecer al mismo dominio de Active Directory que el servidor SQL, las distintas instancias de base de datos de *SES Evolution* y la consola de administración. Si no es así, debe establecerse una relación de confianza entre los dominios.

33. Si cambia el nombre de la cuenta de dominio que es superadministrador de *SES Evolution*, asegúrese de haber creado antes un usuario con el nuevo nombre en la consola de administración de *SES Evolution*. De lo contrario, no podrá iniciar sesión en la consola.
34. Seleccione *Backend* si desea instalar un componente *backend*. El *backend* centraliza todas las operaciones realizadas en el entorno, y es el núcleo de la instalación. Es necesario especificar los siguientes parámetros:
    - El nombre de dominio que se va a usar para referirse a la máquina donde se instala el *backend*.
    - El nombre de host del clúster. Es obligatorio. Si desea implementar balanceo de carga o redundancia con varios *backends* (recomendado para más de 50.000 agentes), esta es la dirección que los *agent handlers* y la consola usarán para conectarse al el *backend*. El nombre DNS debe ser diferente del primer nombre de host y ambos nombres DNS no pueden cambiarse posteriormente. Si no desea configurar un clúster *backend*, deberá declarar una entrada DNS (CNAME) con un nombre específico cuya dirección IP apuntará a la dirección de la máquina en la que está instalado el *backend*.
35. Seleccione el tipo de cuenta que se utilizará como identidad para los procesos del servidor IIS e indique su usuario y contraseña.
36. Si se desea instalar componentes adicionales en la misma máquina que el *backend,* seleccione *agent handler* y la consola de administración de *Stormshield Endpoint Security Evolution*. Introduzca la dirección de contacto (nombre de domino) del *agent handler* que utilizarán los agentes para ponerse en contacto con él.
37. Cargar la licencia del producto obtenida y haga clic en *Install*.
38. Tras esto, se deberá mover el ratón de forma aleatoria para generar números aleatorios que serán usados durante la generación de los certificados usados por el producto.
39. Una vez haya finalizado la instalación podrá salir del Centro de Instalación.

4.4.1 AÑADIR UNA CONSOLA, *BACKEND* O *AGENT HANDLER*

40. En el caso de que se haya decidido instalar las componentes en diferentes máquinas, el centro de instalación permite realizar la instalación de forma individual.
41. Para ello se deberán seguir los siguientes pasos.
    - En primer lugar, se deberá iniciar sesión en el equipo deseado con una cuenta de usuario Windows con las siguientes características:
        - La cuenta de usuario debe pertenecer al dominio.
        - Debe poseer privilegios de administrador.
        - La cuenta de usuario debe tener el rol *sysadmin* en la instancia de la base de datos.
    - Ejecutar el archivo para el centro de instalación:

    SES_Evolution_Installation_Center.exe.

    - Hacer clic en *Add a new component to an existing installation.*

- Seleccionar el componente deseado a instalar. Si está añadiendo un componente *backend*, introduzca la dirección de la instancia de la base de datos de administración y las credenciales de inicio de sesión de la cuenta de superadministrador en la base de datos. Si va a añadir una consola o un *agent handler*, introduzca la dirección del componente *backend.*
- Indicar los parámetros de configuración necesarios.
- Aplicar los cambios y continuar con el proceso hasta que quede completado.

5. FASE DE CONFIGURACIÓN

5.1 ACTUALIZACIÓN DE SES EVOLUTION

42. Para actualizar los componentes de *SES Evolution*, hay que obtener un *Installation Center* en la versión deseada del área de cliente MyStormshield, en la sección Descargas y ejecutar desde un host en el que se haya instalado un componente de la solución. Todos los componentes se actualizarán automáticamente.

    - Iniciar sesión en el equipo utilizando su cuenta de dominio.
    - Hacer doble clic en el archivo SES_Evolution_Installation_Center.exe.
    - Hacer clic en Update an existing installation.
    - Introduzca la dirección de la instancia de la base de datos de administración y las credenciales de inicio de sesión de la cuenta de superadministrador en la base de datos.
    - En la ventana siguiente, el *Installation Center* detecta automáticamente los componentes que deben actualizarse. Hacer clic en *Start Update.*

43. Si la consola de administración requiere una actualización, el *Installation Center* muestra la lista de usuarios conectados a la consola y los nombres de sus estaciones de trabajo. Aparece un banner rojo en todas las consolas abiertas, pidiendo a los usuarios que guarden sus cambios y salgan de la consola. La actualización se inicia cuando se cierran todas las consolas.

44. Si aún quedan consolas abiertas:

    - Hacer clic en *Force Update* para cerrar las consolas remotamente y proceder con la actualización. Utilizar esta opción sólo asegurándose de que no hay cambios que guardar, por ejemplo, si el usuario de la consola está ausente.
    - Hacer clic en *Cancel Update* si se prefiere posponer la actualización.

45. Será necesario un certificado *VeriSign Universal Root Certification Authority* instalado para verificar la autenticidad de las actualizaciones de *SES Evolution*.

46. Este certificado debe instalarse en el almacén de certificados Autoridades de certificación raíz de confianza o Autoridades de certificación raíz de terceros.

5.1.1 ACTUALIZACIÓN DE AGENTES

47. Cuando haya actualizado *SES Evolution* desde el *Installation Center*, puede aplicar esta versión a uno o varios grupos de agentes a través de la consola de administración. Si algunos agentes no están conectados a gestores de agentes, *Agent Handlers*, aplique la nueva versión manualmente a estos agentes.

48. Es recomendable realizar primero una actualización a un grupo de agentes de prueba para probar la versión antes de realizarla a los grupos en producción.

49. Para bajar a los agentes a una versión de *software* anterior de *SES Evolution*, se debe asegurar de que la opción Permitir bajar a una versión anterior está activada en Elegir configuración de actualización de agentes en el menú de Agentes.

50. El privilegio *Agent groups – Modify* es necesario para actualizar los agentes.

51. Para verificar la autenticidad de las actualizaciones de *SES Evolution* será necesario tener instalado un Certificado *VeriSign Universal Root Certification Authority*.
52. Debe instalarse en el almacén de certificados Autoridades de certificación raíz de confianza o Autoridades de certificación raíz de terceros.

5.2 DESINSTALACIÓN DE *SES EVOLUTION*

53. Para desinstalar completamente *SES Evolution*, los diversos componentes de *SES Evolution* deben desinstalarse en el siguiente orden:
    - Agentes de SES Evolution. Para más información, consultar Desinstalación de agentes en *[Guía de administración].*
    - Consolas de administración.
    - *Agent handlers*.
    - Servidores *backend.*
    - Bases de datos.
54. Se requieren privilegios de administrador.

5.2.1 DESINSTALACIÓN DE CONSOLAS, *AGENT HANDLERS* Y SERVIDORES *BACKEND*

55. Para desinstalar consolas, *agent handlers* y *backends* desplegados se deben seguir los siguientes pasos:
    - Iniciar sesión en el equipo que aloja el componente *SES Evolution* utilizando la propia cuenta de dominio.
    - En *Programs and Features* en el panel de control de Windows, seleccionar el componente deseado y hacer clic en *Uninstall*.
    - Introducir la información solicitada en el desinstalador de *SES Evolution* que se abre: *Backend host name* para la consola y el gestor de agentes, y *Database instance* para el servidor *backend.*
    - Hacer clic en *Uninstall.*
    - Reiniciar el ordenador una vez desinstalados los componentes.

5.2.2 DESINSTALACIÓN DE BASES DE DATOS

56. Para llevar a cabo la desinstalación y borrado de las bases de datos se deben seguir los siguientes pasos:
    - Iniciar sesión en el host utilizando la propia cuenta de dominio.
    - Hacer doble clic en el archivo *SES_Evolution_Installation_Center.exe.*
    - Hacer clic en *Uninstall database*.
    - Rellenar la información necesaria para conectarse a la instancia de base de datos y hacer clic en *Connect.*

- En la siguiente pantalla, hacer clic en *Uninstall database*.
- Salir del Centro de Instalación una vez desinstaladas las bases de datos.

5.3 SERVIDORES DE AUTENTICACIÓN

57. Durante el proceso de instalación se deberá realizar la integración con Active Directory.
58. Si hay varios dominios de Active Directory en la infraestructura, se podrán instalar gestores de agentes, *Agent Handlers*, en equipos que pertenezcan a dominios distintos de aquel en el que se encuentra ubicado el componente *backend.* Las comunicaciones entre el *backend* y los agentes se protegen mediante autenticación mutua basada en certificados.
59. Así los distintos dominios de Active Directory deberán poder comunicarse entre sí.
60. Los pasos que se indican a continuación serán necesarios para instalar un gestor de agentes, *Agent Handlers*, en un dominio distinto de aquél en el que se encuentra el componente *backend*:
    - Utilizando un servidor que pertenezca al dominio 1 de Active Directory, realice una instalación avanzada instalación en el Centro de instalación y seleccione la instalación del componente *backend.*
    - Utilizando un servidor que pertenezca al dominio 2 de Active Directory, haga clic en *Modify an existing installation* en el Centro de instalación y haga clic en *Stormshield Endpoint Security Evolution Agent handlers.*
    - Introducir los valores de los parámetros y hacer clic en *Install.*
    - Si se van a instalar varios gestores de agentes, *Agent Handlers*, repetir la operación en cada equipo que aloje controladores de agentes.

5.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

61. **La configuración TLS debe realizarse de la siguiente manera**:
62. Utilizar el parámetro de directiva de grupo *Computer Configuration → Policies → Administrative Templates → Network → SSL Configuration Settings → SSL Cipher Suite Order* para mantener únicamente las suites de cifrado deseadas (y, opcionalmente, cambiar el orden), y aplicar dicha directiva a todos los dispositivos en los que estén instalados la consola, el *agent handler*, el agente y el *backend* del TOE.
63. Las suites de cifrado deseadas son las siguientes:
    - *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
    - *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
    - *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
    - *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*
    - *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P521*
    - *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384*
    - *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256*
    - *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P521*

- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384*

64. Será necesario un certificado ***VeriSign Universal Root Certification Authority*** instalado para verificar la autenticidad de las actualizaciones de ***SES Evolution***.

65. Este certificado debe instalarse en el almacén de certificados Autoridades de certificación raíz de confianza o Autoridades de certificación raíz de terceros.

5.5 AUDITORÍA

5.5.1 CONFIGURACIÓN DE LA GESTIÓN DE REGISTROS

66. El agente genera logs cada vez que se bloquean acciones del usuario o cuando el agente realiza una acción de auditoría. En función de su gravedad, estos registros se podrán enviar a tres destinos diferentes. Los distintos ajustes de este proceso se podrán definir en la configuración de los grupos de agentes.

67. Además, para cada regla de seguridad que se cree, se podrá especificar:

    - La gravedad de los eventos registrados,
    - Los destinos de estos registros.

5.5.2 RECOMENDACIONES

68. La gravedad de los eventos registrados por una regla podrá ajustarse en los siguientes casos:

    - Si existen aplicaciones muy sensibles, aumentará la gravedad de los registros. Los registros de Emergencia y Alerta tendrán prioridad sobre otros registros enviados a los gestores de agentes, y se enviarán con mayor frecuencia (cada 30 segundos por defecto, cada hora para otros niveles de registro),
    - Si una regla de seguridad genera demasiados registros irrelevantes, será necesario reducir la gravedad.

5.5.3 CONFIGURACIÓN DE REGISTROS EN UNA REGLA DE SEGURIDAD

69. Para llevar a cabo la configuración de los registros para reglas o políticas de seguridad

    - Seleccionar la política de seguridad en la pestaña *Policies* de la consola de administración y, a continuación, seleccionar el conjunto de reglas. Aparecerá la página principal del conjunto de reglas.
    - Hacer clic en la pestaña de la regla que se desea modificar.
    - Si está en modo de sólo lectura, hacer clic en *Edit* en el banner superior.
    - En el banner de la parte superior de la regla, hacer clic en  . Aparecerá la ventana *Log settings.*
    - En el campo *Log severity*, asignar el nivel a los registros generados por esta regla.
        - *Inherit*: se aplica el comportamiento general definido para el grupo de agentes. En el ejemplo anterior los logs se pueden ver en el agente porque este es el caso para los logs de todos los niveles a partir de *Notice.*

- *Never*: los logs nunca pueden verse en el agente independientemente del comportamiento general.
- *Always*: los logs siempre se pueden ver en el agente independientemente del comportamiento general.

- En el campo *Show on agent*, elegir si los logs de esta regla se pueden ver en la consola de administración.
- En el campo *Send to Syslog*, elegir si se desea enviar los registros de esta regla al servidor *Syslog* si se ha configurado uno.
- Hacer clic en *Confirm*.
- Guardar los cambios realizados.

5.6 AUTOPROTECCIÓN DE CONSOLA, AGENT HANDLER Y BACKEND

70. Para proporcionar protecciones a los componentes de la solución, en este caso la consola de administración, los *agent handlers* y el *backend*, se recomienda instalar un agente en los equipos donde estén instalados dichos componentes y aplicar una política de seguridad que contenga las siguientes *Shared RuleSets*, en función de los componentes que estén instalados en dicho equipo:
    - *Stormshield - Administration console protection* para equipos en los que esté instalado la consola de administración.
    - *Stormshield - Agents Handler protection* para equipos en los que esté instalado el componente *agent handler*.
    - *Stormshield - Backend protection* para equipos en los que esté instalado el componente *backend*.
71. Los agentes SES Evolution en sí están equipados con un mecanismo de autoprotección implementado por un conjunto de reglas transparentes para administradores y usuarios, con el propósito de proteger a los agentes de ataques externos o de usuarios malintencionados que puedan intentar desactivarlos o desinstalarlos.
72. Cuando se activa el modo de mantenimiento en la consola de administración, el agente sigue proporcionando protecciones al sistema en el que está instalado detectando amenazas porque la política de seguridad sigue activada. Sin embargo, este modo debe ser utilizado con precaución y por usuarios de confianza ya que se desactivará el modo de autoprotección en el agente.

6. FASE DE OPERACIÓN

6.1 GESTIÓN DE USUARIOS EN LA CONSOLA DE ADMINISTRACIÓN DE SES EVOLUTION

73. Los usuarios accederán a la consola con sus cuentas de Microsoft Windows que deberán estar en el mismo Active Directory que el componente *backend*. De no ser así, deberá establecerse una relación de confianza entre los dominios.
74. Por defecto, sólo el superadministrador especificado durante la instalación podrá acceder a la consola de administración. Este administrador podrá crear otros usuarios que también podrán iniciar sesión.
75. A cada usuario se le asignará un rol que define su perfil y restringe las funciones disponibles en la consola de administración. Hay tres roles disponibles por defecto: *Audit, Helpdesk y Administration.*
76. También se podrán crear y personalizar nuevos roles.
77. Varios usuarios podrán conectarse simultáneamente a las consolas que gestionan el mismo pool.

6.1.1 CREACIÓN DE ROLES PERSONALIZADOS

78. Se deberá tener el privilegio *Users-write* para poder crear roles.
    - Seleccionar el menú *Users* y, a continuación, la pestaña Roles.
    - Hacer clic en *Create a rol.*
    - Introducir un nombre para el rol y su descripción si es necesario.
    - Pulse *OK*. El nuevo rol aparecerá en la lista. Por defecto se aplican los privilegios más restrictivos.
    - Para cada privilegio, elegir el tipo de acceso que se desea conceder. Cada privilegio corresponde a un panel de la consola de administración. Por defecto, sólo los paneles *Environment, Dashboard y Licenses* son accesibles.
79. El privilegio *Lock* permitirá romper los bloqueos establecidos por otros usuarios en los paneles de la consola.

6.1.2 AÑADIR USUARIOS EN LA CONSOLA DE ADMINISTRACIÓN

80. Deberá tener el privilegio *Users-Modify* para poder añadir usuarios.
    - Seleccionar el menú *Users* y, a continuación, la pestaña *Users.*
    - Hacer clic en *Create a user.*
    - Seleccionar el rol que se desea asignar a este usuario: *Audit*, *Help desk*, *Administration, Custom role*.
    - Introducir el ID de la cuenta Windows en formato *domain_name\user_name*. Asegurarse de que el ID sea correcto, ya que no se realizarán comprobaciones cuando

se introduzca el ID. Cualquier error en la cuenta sólo se detectará cuando el usuario intente iniciar sesión.

- Hacer clic en *Create a user*.

6.1.3 GESTIÓN DE LA CONEXIÓN SIMULTÁNEA DE USUARIOS A CONSOLAS QUE GESTIONAN EL MISMO POOL

81. Varios usuarios podrán gestionar simultáneamente el mismo pool desde *hosts* diferentes.
82. Cuando un usuario modifique cualquiera de los siguientes recursos, éstos se bloquearán automáticamente y ningún otro usuario podrá modificarlos:
    - Grupos de agentes,
    - Políticas,
    - Grupos de *agent handlers.*
83. A continuación, se bloqueará todo el panel, es decir, todos los grupos de agentes, todos los grupos de manejadores de agentes, todas las políticas o todos los usuarios. Por ejemplo, el usuario 1 no puede modificar la política A mientras que el usuario 2 modifica la política B.
84. Tampoco se podrán añadir nuevos grupos o nuevas políticas cuando un panel está bloqueado.
85. Cuando un usuario guarda o cancela los cambios, el panel se desbloqueará automáticamente si no hay más objetos siendo editados en este panel.
86. Si un usuario intenta modificar un panel bloqueado, aparecerá un mensaje en el banner superior indicando qué usuario bloqueó el panel y desde cuándo. Por lo tanto, el usuario no podrá modificar nada.
87. Sin embargo, si el rol del usuario incluye el privilegio *Lock - Unlock*, el usuario podrá romper el bloqueo del panel utilizando el botón *Break the lock* que se sitúa en el banner superior. Esta función resulta especialmente útil cuando, por ejemplo, un recurso permanece accidentalmente en modo de edición.
88. Como esta operación libera el panel y anula los cambios en curso del otro usuario, deberá utilizarse con cuidado. En este caso, el usuario que primero mantuvo el bloqueo será avisado cuando intente guardar los cambios.
89. Para romper el bloqueo de un panel si tiene el privilegio:
    - Hacer clic en *Break the lock* en el banner superior.
    - Confirmar la operación en la ventana que aparece.

6.2 GESTIÓN DE LICENCIAS DE SES EVOLUTION

90. Se registra una licencia mientras se instala el entorno *SES Evolution.*
91. Las licencias determinarán el número de agentes *SES Evolution* activos que se pueden gestionar con la solución, y tienen una fecha de caducidad.
92. Se podrán importar varias licencias, en cuyo caso, el número de agentes permitidos es el número total de agentes para todas las licencias.

6.2.1 IMPORTAR LICENCIAS EN SES EVOLUTION

93. Se deberá tener el privilegio *Licenses-Modify* para poder importar licencias.
    - En el cuadro de mandos de la consola de administración, hacer clic en Licencias.
    - Hacer clic en Add una licencia y seleccionar el archivo de licencia (por ejemplo, SES-JCCA-WE9T-Q5RA.lic). El campo Capacidad representa el número de agentes activos de SES Evolution y el número total de agentes permitidos por licencia.

6.2.2 LECTURA DE LA INFORMACIÓN DE LA LICENCIA

94. Se deberá tener el privilegio *Licenses-Display* para poder leer la información de la licencia.
95. La sección Licencias en el panel de la consola de administración muestra el número de agentes activos y la proporción comparada con el número de agentes permitidos. Un agente se considera activo si se ha conectado al *agent handler* en los últimos 10 días.
96. El gráfico será verde cuando el número de agentes activos está por debajo del 90% de la capacidad total de la licencia, naranja cuando está entre el 90% y el 110%, y rojo cuando se ha superado el umbral tolerado del 110%.
97. La información sobre las licencias se actualizará cada hora y cada vez que se accede al cuadro de mandos.

7. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Preparación del entorno de operación	☐	☐	
Obtención Licencias	☐	☐	
Instalación servidor de bases de datos	☐	☐	
Instalación servidor *backend*	☐	☐	
Instalación servidor *agent handler*	☐	☐	
Instalación de consola de administración	☐	☐	
Despliegue de agentes	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Configuración de protocolos seguros	☐	☐	
Recomendaciones registros auditoría	☐	☐	

8. REFERENCIAS

98. Los manuales del producto son facilitados a la organización tras la adquisición del producto.

[*Guía de instalación*]	Installation Guide - Stormshield Endpoint Security Evolution v2.2
[*Guía de administración*]	Administration Guide - Stormshield Endpoint Security Evolution v2.2
[*Recomendaciones SQL Server*]	SQL Server recommendations Guide for Stormshield Endpoint Security Evolution v2.2

9. ABREVIATURAS

DNS	*Domain Name System*
IIS	*Internet Information Services*
IP	*Internet Protocol*
SES	*Stormshield Endpoint Security*
SQL	*Structured Query Language*
TLS	*Transport Layer Security*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL