centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1223

Procedimiento de empleo seguro
MONSE

Febrero de 2024

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.03.01 11:18:50 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-098-1.
Fecha de Edición: febrero de 2024.

ÍNDICE

1. INTRODUCCIÓN

1. MONSE (MONitorización de la SEguridad) es una solución SIEM para recopilar y correlacionar de forma centralizada múltiples fuentes de eventos de seguridad. La solución facilita analizar eventos basados en logs, procesos, comportamiento e IOCs. Dispone de técnicas de Inteligencia Artificial que facilitan la detección de anomalías, integración de fuentes de inteligencia de amenazas, posibilidad de definir reglas de alerta adaptadas a la particularidad de cada organización, así como la posibilidad de crear cuadros de mando personalizables.
2. La plataforma permite un despliegue modular en función del tipo de madurez de la organización. Dispone de múltiples funcionalidades orientadas a la mejora en el cumplimiento del Esquema Nacional de Seguridad.
3. MONSE ha sido cualificada e incluida en el Catálgo de Productos y Servicios de Seguridad TIC del Centro Criptológico Nacional (CPSTIC) en la familia **"Sistema de gestión de eventos de deguridad (SIEM)**. Se recomienda consultar el Catálogo para conocer la versión cualificada en cada momento.

2. OBJETO Y ALCANCE

4. El objeto del presente documento es facilitar la instalación y configuración segura del producto **Monse con la versión de software v1.0 y empleando el Agente con versión v8.3.2**, junto con el aseguramiento del entorno en el que se despliega.
5. El despliegue del *probe* MONSE puede ser en formato *Appliance* físico o virtual para su despliegue en *VMware ESXi*.

3. ORGANIZACIÓN DEL DOCUMENTO

6. Este documento se compone de los siguientes apartados:

a) Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado **5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado **6**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

d) Apartado **7**: Checklist de las tareas a realizar y el estado de cada una de ellas.

e) Apartado **8**: Referencias.

f) Apartado **9**: Abreviaturas usadas en este documento.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. Para cada una de las opciones de instalación del *probe* (*Appliance* físico o virtual) se deben realizar las comprobaciones correspondientes:
   - *Appliance* físico: comprobar que la caja no llegue golpeada y el precinto con el logotipo de **Grupo CIES** esté intacto.
   - OVA (*appliance* virtual): comparar el **hash sha512** del OVA con el suministrado por correo. Para realizar la comprobación, se puede ejecutar el siguiente comando en una consola de *powershell* (sin comillas): *"Get-FileHash -Algorithm sha512 .\monse.ova | Format-List"*
8. En el caso del Agente, el técnico de Grupo CIES proporcionará un enlace de descarga del mismo. En dicho enlace, se puede descargar también el hash sha512 del fichero. Una vez descargado, deberá verificarse que coincide al realizar el hash del fichero.

4.2 ENTORNO DE INSTALACIÓN SEGURO

9. El *probe* en formato *appliance* físico se instalará en el CPD de la organización, cumpliendo sus políticas de seguridad. Como mínimo debe garantizarse el control y restricción de acceso físico y lógico a la sonda y/o al hipervisor que la aloje.

4.3 REGISTRO Y LICENCIAS

10. No es necesario un registro de licencia, esta se activa automáticamente durante el proceso de despliegue.

4.4 CONSIDERACIONES PREVIAS

11. Para el correcto funcionamiento, ha de permitirse previamente la siguiente conexión hacia WAN en el firewall de la organización:
    - Origen: sonda.
    - Destino: Monse Central.
    - Puerto: 33900.
    - Servicio: opnvpn.
12. En caso de desplegar el *probe* a partir de OVA, comprobar que la versión mínima de ESXi sea superior a 6.5.
13. Para la instalación del *probe* como *appliance* físico se ha de aprovisionar lo siguiente:
    - 1 puerto RJ45 en la electrónica de red configurado en modo acceso en la VLAN correspondiente.
    - 1 conexión a la red eléctrica protegida por SAI.
    - 1 U en armario de comunicaciones/servidores.

5. FASE DE INSTALACIÓN

14. El *probe* como *appliance* físico es *plug and play*. Una vez conectado a la red, se avisará al técnico de Grupo CIES designado para la comprobación del correcto funcionamiento.

15. Para la instalación del *probe* como *appliance* virtual, se desplegará la OVA en un ESXi siguiendo los siguientes pasos:

    a) En el ESXi, seleccionar en Crear/Registrar máquina virtual.

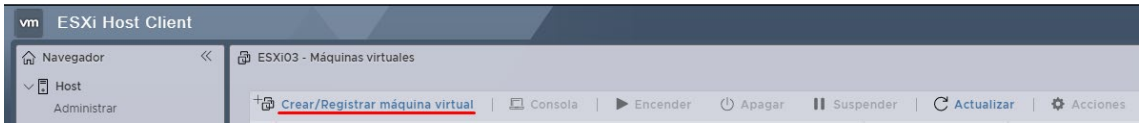

Ilustración 1. Crear máquina virtual (I).

    b) Seleccionar Implementar una máquina virtual a partir de un archivo OVF u OVA:

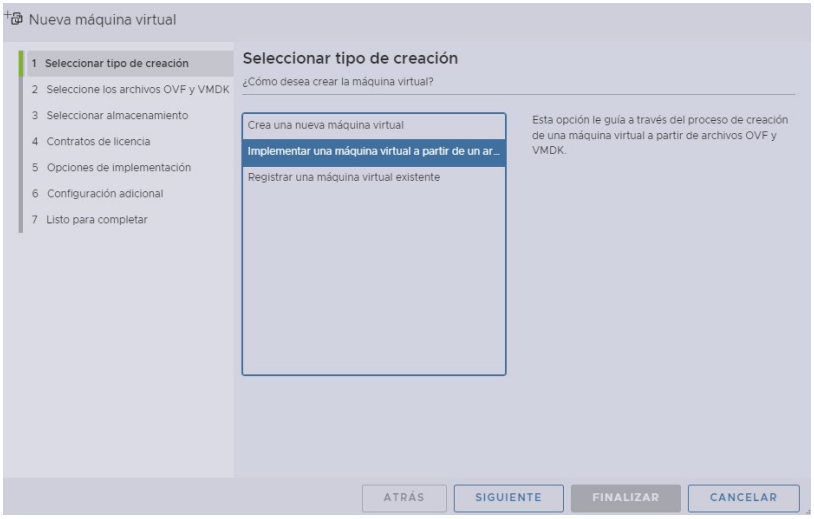

Ilustración 2. Crear máquina virtual (II).

    c) Poner un nombre y seleccionar el OVA suministrado:

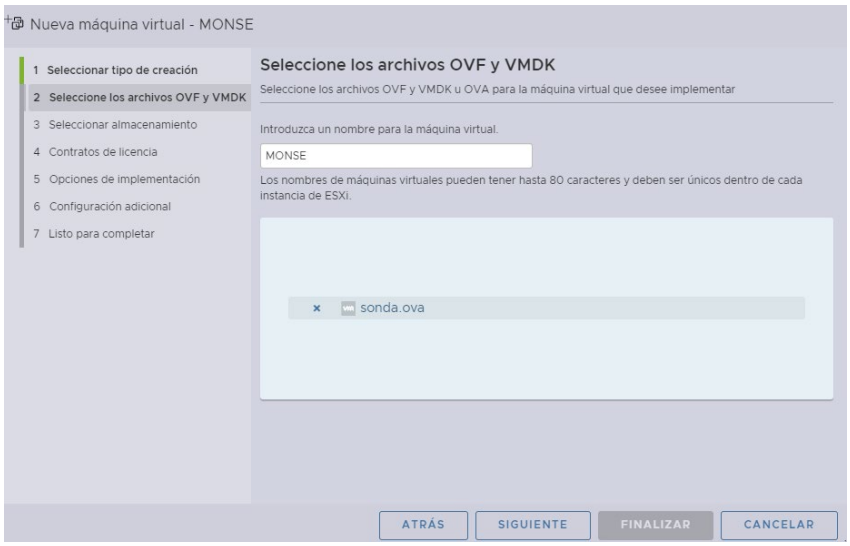

Ilustración 3. Crear máquina virtual (III).

d) Seleccionar el *datastore* de destino:

Ilustración 4. Crear máquina virtual (IV).

e) Seleccionar la red de destino, aprovisionamiento fino y marcar el encendido automático:

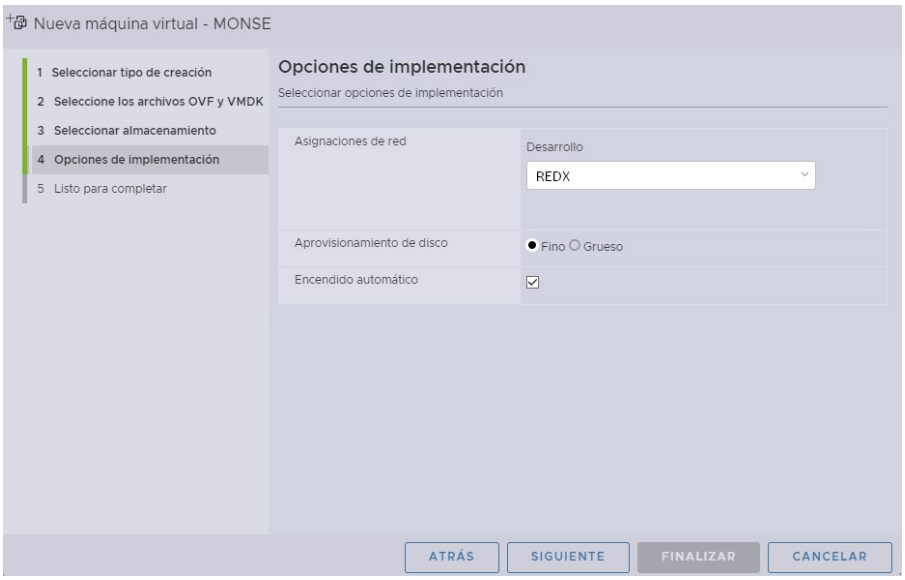

Ilustración 5. Crear máquina virtual (V).

f) Pasar a la pantalla de revisión y finalizar.

g) Asegurarse de que la casilla “Sincronizar hora de invitado con el host” está desmarcada:

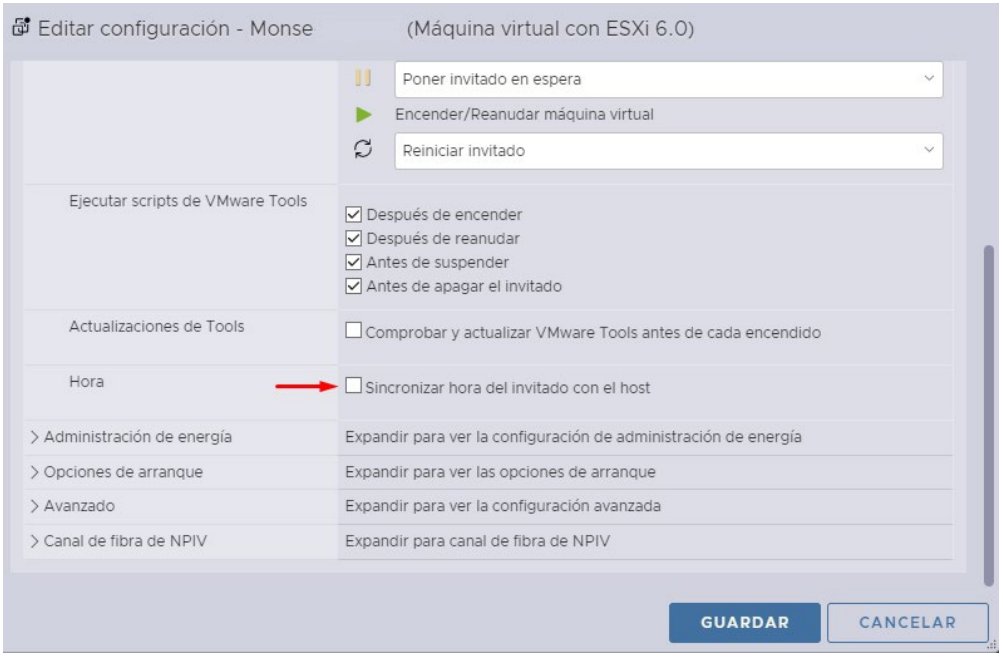

Ilustración 6. Crear máquina virtual (VI).

h) Marcar “Forzar configuración de BIOS”:

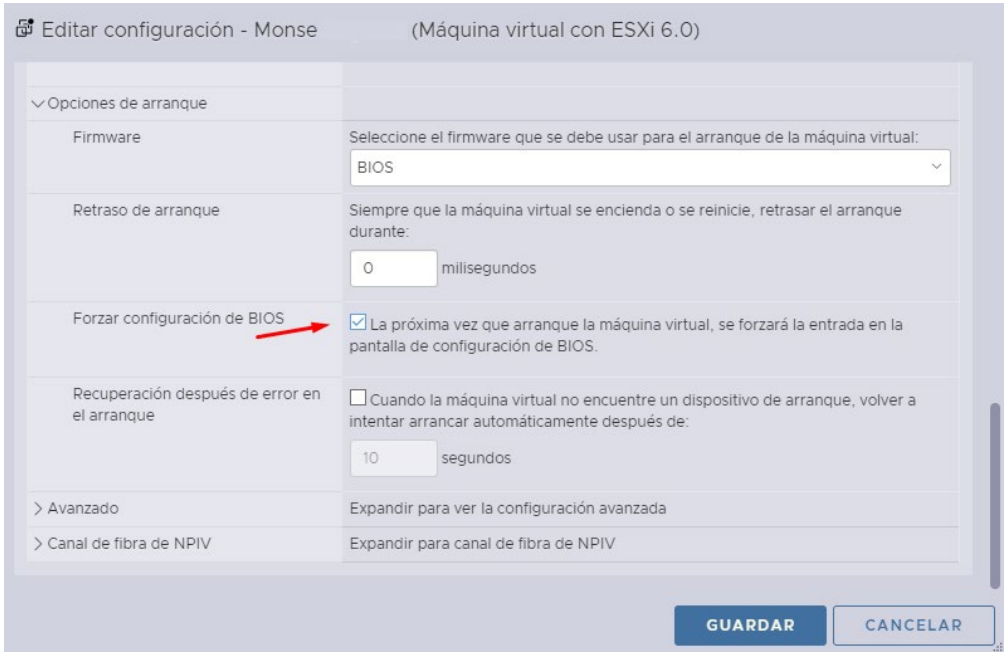

Ilustración 7. Crear máquina virtual (VII).

i) Arrancar la máquina y esperar a que entre en BIOS

j) En *Advanced I/O Device configuration*, deshabilitar las 4 opciones:

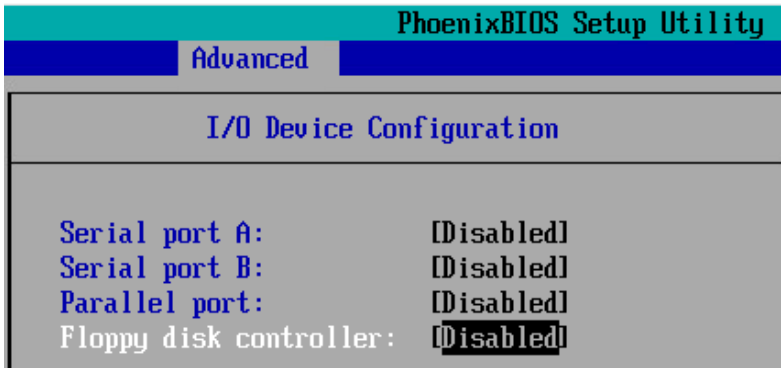

Ilustración 8. Configuración BIOS (I).

k) Establecer contraseña de BIOS:

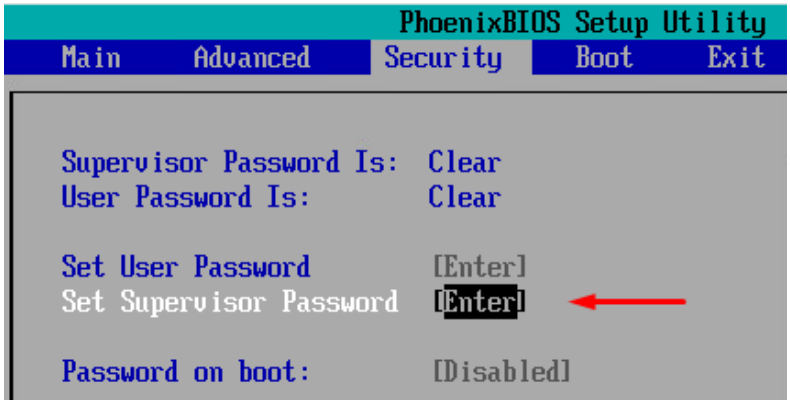

Ilustración 9. Configuración BIOS (II).

l) En *Boot*, establecer el disco como primer dispositivo de arranque:

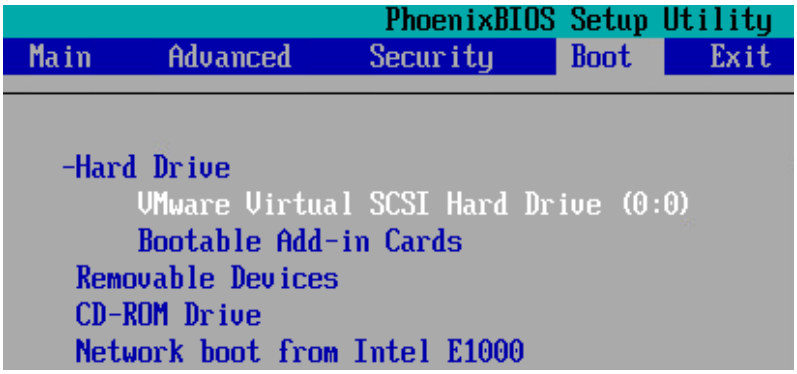

Ilustración 10. Configuración BIOS (III).

m) Guardar cambios, arrancar la máquina e informar al técnico de Grupo CIES asignado.

16. Una vez desplegada la sonda (*probe*), se proporcionará acceso al técnico de Grupo CIES a cargo del despliegue para realizar la instalación de los agentes en los *endpoints*. Para ello, se recomienda proporcionar un acceso nominal seguro (VPN, CITRIX…) protegido mediante MFA al técnico, así como un usuario nominal del dominio/*endpoint* con permisos para instalar software en los dispositivos objeto del servicio.

17. En caso de necesitar realizar la instalación del Agente posteriormente en otros dispositivos, y tras descargarlo del enlace facilitado por el técnico de Grupo CIES (ver apartado 4.1 ENTREGA SEGURA DEL PRODUCTO), seguir los siguientes pasos:

    - Deberán seguirse primero las acciones indicadas en la guía "MONSE Agentes Windows" la cual será facilitada por el técnico del Grupo CIES.
    - Una vez realizadas dichas tareas, se deberá instalar descomprimiendo el ZIP y copiando en el directorio extraído el archivo "elastic-agent.yml", sobrescribiendo el existente.
    - Ejecutar el siguiente comando con permisos de administrador: .*elastic-agent.exe install*
    - Se preguntará si lo queremos enrolar en *fleet*, seleccionar NO.
    - Comprobar que se produce la conexión sin errores en la consola de PowerShell. Debería aparecer un mensaje informando lo siguiente: "Elastic Agent has been succesfully installed".
    - En caso de error, contactar con el técnico del grupo CIES.

6. FASE DE CONFIGURACIÓN

6.1 ADMINISTRACIÓN

18. Todas las tareas de administración del producto quedan a cargo del grupo CIES. El producto no requiere ninguna acción administrativa por parte de la organización.

6.2 GESTIÓN DE USUARIOS

19. Para la creación de nuevos usuarios, deberá ponerse en contacto con el técnico de Grupo CIES.
20. Se recomienda exigir a los usuarios, de manera procedural, modificar su contraseña cada 60 días.
21. Los usuarios pueden llevar a cabo el cambio de contraseña desde el botón de perfil, haciendo clic en *Profile*. Introduciendo los valores en los campos *Current password, New password* y *Confirm new password*.
22. Dicha contraseña deberá cumplir con la Política de contraseñas existente, no configurable:
    - Longitud mínima: 12 caracteres.
    - Vigencia máxima: 90 días.
    - Vigencia mínima: 2 días.
    - No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres iguales consecutivos
    - Incluir caracteres de tres de las siguientes categorías:
        - Mayúsculas.
        - Minúsculas.
        - Números.
        - Caracteres no alfanuméricos.

6.3 ACTUALIZACIONES

23. La actualización del *probe* queda a cargo del personal de Grupo CIES, la organización no deberá llevar a cabo ninguna acción.
24. La actualización de los Agentes, se llevará a cabo de forma periódica según indicaciones de Grupo CIES. Será necesario verificar que las máquinas donde se quieran actualizar los Agentes tengan conectividad con el dominio *https://artifacts.elastic.co*
25. El comando concreto de actualización será facilitado por Grupo CIES en el momento.

6.4 AUDITORÍA

26. El producto genera registros de auditoría de forma transparente para la organización. Estos son solo visibles para el Grupo CIES.

6.5 SINCRONIZACIÓN

27. Tanto el *probe* en modalidad *Appliance* físico, como virtual sincronizan la hora con el servidor horario de MONSE, que a su vez sincroniza con el Real Instituto y Observatorio de la Armada. Esta sincronización viene preconfigurada tanto en el *appliance* físico como en el OVA y no requiere configuración.

6.6 ALTA DISPONIBILIDAD

28. En el caso de desplegar el *probe* a partir de un OVA, **se recomienda que la máquina esté en un cluster de VMware**.

7. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la integridad del paquete	☐	☐	
Instalación de la sonda	☐	☐	
CONFIGURACIÓN			
Gestión de usuarios			
Modificación de contraseñas	☐	☐	

8. REFERENCIAS

29. La guía referenciada será facilitada por Grupo CIES tras la adquisición del producto.

REF1 *Guía MONSE Agentes Windows*

9. ABREVIATURAS

BIOS	Basic Input Output System
CPD	Centro de Procesamiento de Datos
ENS	Esquema Nacional de Seguridad.
IOC	Indicator Of Compromise
MFA	Multi Factor Authentication
SAI	Sistema de Alimentación Ininterrumpida
SIEM	Security Information and Event Management
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

PUBLICACIONES DE DEFENSA

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