centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1610

Procedimiento de empleo seguro de
KATUA SDI Platform

Octubre de 2021

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 criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.10.14 12:02:52 +02'00'

NIPO: 083-21-189-X.

Fecha de Edición: octubre de 2021.

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. *Katua SDI Platform* es la solución hiperconvergente de KRC ESPAÑOLA que ofrece múltiples capacidades en una plataforma unificada:
    a) Despliegues de CPD virtuales.
    b) Despliegue de servicios *cloud*.
    c) Almacenamiento unificado.
    d) Escalabilidad.
    e) SDN.
    f) Capacidad *multi-tenant* en contextos de seguridad diferenciados.
2. **Esta solución ha sido cualificada e incluida en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) en la familia de "*Herramientas de hiperconvergencia*"**.
3. La solución de entrega en formato *appliance,* instalada en un *hardware* especialmente optimizado para este propósito y publicado en la guía STIC-CCN-104 de evaluación *Zoning (exp.* 2018-224).
4. Las características principales del *hardware* son:
    a) Procesador Intel Xeon
    b) Memoria RAM 32GB RAM ampliables
    c) Almacenamiento de base 1TB ampliable
    d) Sistema enrackable en 2U
    e) Fuentes de alimentación redundantes
5. Al estar diseñada siguiendo el principio de ***"Security by Design",*** la solución está securizada desde fábrica por lo que las actuaciones para una puesta en marcha segura son mínimas.

2. OBJETO Y ALCANCE

6. La presente guía recoge el procedimiento de puesta en marcha inicial del producto, primeros pasos, así como recomendaciones generales de configuración para garantizar el uso seguro del mismo.
7. Los procedimientos indicados en este documento se circunscriben a la **versión 1.0.6** del producto.
8. Determinadas operaciones por su complejidad y longitud sólo se referencian, remitiendo a los siguientes documentos para ver con detalle la operación:
    a) *Manual del usuario del dashboard.* [1]
    b) Manual del usuario CLI. [2]

3. ORGANIZACIÓN DEL DOCUMENTO

9. El documento se ha estructurado en los siguientes apartados:

Apartado 4. FASE DE DESPLIEGUE E INSTALACIÓN

En este apartado se describe el procedimiento de recepción del equipamiento y operaciones de verificación del embalaje, etiquetas, etc. De igual forma, se establecen las condiciones de instalación física y requisitos necesarios.

a) **Apartado 5. FASE DE CONFIGURACIÓN**

En este apartado se describen los procedimientos para realizar una configuración segura desde el inicio. Se detallan las diferentes opciones de inicio de sesión segura, conexión inicial a la infraestructura de red, configuración del administrador del producto, etc.

b) **Apartado 6. FASE DE OPERACIÓN**

En este apartado se describen las operaciones básicas de mantenimiento y verificación del sistema.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

10. *KATUA SDI Platform* se entrega en formato *appliance*, por lo que en el momento de recibir el producto se deberá verificar que:

    a) El embalaje perfectamente cerrado, sin roturas en las cintas de precinto marcadas con el anagrama de KRC Española.

    b) El producto no presenta signos de manipulación o deterioro de algún tipo.

    c) El etiquetado no ha sido manipulado ni presenta roturas, especialmente el sello de garantía identificado como tal en el equipo.

    d) El número de serie del producto a través del código de barras o QR de la misma.

    e) Los discos que conforman la solución están bloqueados y no se pueden extraer.

4.2 ENTORNO DE INSTALACIÓN SEGURO

11. La plataforma está diseñada para ser instalada en un Centro de Proceso de Datos (CPD), con acceso restringido y controlado. Es responsabilidad del cliente final garantizar esta seguridad física.

4.3 CONSIDERACIONES PREVIAS

12. La plataforma se ha diseñado para permitir su puesta en marcha de dos (2) formas diferentes:

    a) Sin conexión de red, para lo que será necesario conectar un monitor y teclado a la plataforma. En este modo la configuración inicial se puede llevar a cabo a través de la interfaz CLI disponible (ver Manual de Usuario CLI [2]).

    b) Con conexión de red, nodo *headless*, para lo que será necesario conectar la plataforma a una infraestructura de red existente y acceder a través de un equipo con navegador web compatible HTML 5. Para garantizar la máxima seguridad en la puesta en marcha, tanto la red existente como el equipo utilizado deberían estar convenientemente bastionados.

4.4 INSTALACIÓN

13. El producto viene preinstalado de fábrica, por lo que no se requieren actuaciones especiales para su instalación inicial.

5. FASE DE CONFIGURACIÓN

5.1 AUTENTICACIÓN

14. En lo concerniente a la autenticación de los usuarios, la plataforma implementa su propio modelo de autenticación basado en credenciales locales.
15. Todos los componentes internos se comunican haciendo uso de certificados. La plataforma implementa su propia PKI para la generación y gestión de certificados de los diferentes componentes. Para más información, consultar 5.5 GESTIÓN DE CERTIFICADOS.
16. La conexión de usuarios a través de CLI requiere autenticación en dos pasos: acceso local al sistema operativo (por consola o *ssh*), y autenticación adicional para el acceso a la gestión de la plataforma. Esto permite distinguir el usuario administrador de la plataforma, del usuario con acceso *root* del sistema operativo.
17. El proceso de conexión y autenticación está descrito en el *Manual de Usuario del dashboard* [1], apartado 3.

5.2 ADMINISTRACIÓN DEL PRODUCTO

5.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

18. La plataforma admite la administración de forma local, a través del uso de la consola, o de forma remota a través de conexión *ssh* o *https*.
19. Para realizar la **administración local** es necesario una autenticación en dos (2) fases:
    a) Identificación del usuario del sistema operativo (cuenta local)
    b) Identificación ante la plataforma que ofrece su propia línea de comandos (ver Manual de Usuario CLI)
20. La **administración remota** se puede realizar de dos (2) formas, utilizando siempre y de forma obligatoria canales seguros. Sólo se admite el uso de *SSH* y *HTTPS*.
    a) CLI: Conexión vía *SSH* y autenticación del usuario del sistema operativo (cuenta local), y posteriormente autenticación ante la plataforma.
    b) DASHBOARD: Conexión vía *HTTPS* y autenticación ante la plataforma.
21. El sistema NO permite el uso de canales o servicios no seguros, como telnet.
22. La plataforma no permite la transferencia de archivos a/desde la misma utilizando el servicio *FTP*. Sólo es posible realizar transferencia mediante el uso de *SCP*.

5.2.2 CONFIGURACIÓN DE ADMINISTRADORES

23. Los usuarios administradores pueden crear y asociar permisos a usuarios definiendo los privilegios de actuación sobre los diferentes aspectos de la plataforma. Los tipos de permisos son agrupados en los siguientes bloques:
    a) Permisos globales de la plataforma.
    b) Permisos sobre *tenants.*
        i. Permisos delegados de administración sobre el *tenant.*
        ii. Permisos "*readonly*" para monitorización.
    c) Permisos sobre APIs.
24. Los usuarios y roles existentes, así como su asociación se puede consultar a través del *dashboard*, en la opción *Identity*.
25. La plataforma controla la política de contraseñas, así como los parámetros de *timeout y* sesiones. Los valores de estos parámetros están establecidos desde fábrica por defecto. El usuario *root* tiene la capacidad de cambiar los mismos mediante la edición de los ficheros de configuración correspondientes.
26. Los ajustes en relación con la política segura de contraseñas se pueden efectuar modificando los ficheros */etc/login.defs* y */etc/security/pwquality.conf* para la configuración de acceso vía *ssh/consola* y el fichero */etc/keystone/keystone.conf* para la configuración de acceso vía dashboard.
27. Los ajustes en relación con la configuración de *timeouts* y bloqueos se pueden efectuar modificando los ficheros */etc/ssh/sshd_config* y */etc/pam.d/password-auth* para accesos vía *ssh/consola* y el fichero */etc/keystone/keystone.conf* para accesos vía dashboard.
28. Los valores por defecto se han establecido de la siguiente forma:
    a) Configuración de la política segura de contraseñas:
        i. Longitud mínima de 11 caracteres para el servicio *SSH* y 12 para el *dashboard*.
        ii. Se debe incluir al menos una letra minúscula
        iii. Se debe incluir al menos una letra mayúscula
        iv. Se debe incluir al menos un número
        v. Se debe incluir al menos un carácter especial
    b) Configuración de parámetros de sesión:
        i. *Timeout* de sesión para la CLI de 300 segundos y para el *dashboard* 1800.
        ii. El sistema bloquea la interfaz web durante 1800 segundos tras 6 intentos fallidos.

iii. Los usuarios del sistema operativo se bloquean indefinidamente tras 8 intentos (no *root*).

iv. El usuario *root* será el encargado de realizar el desbloqueo de las cuentas de forma manual.

v. Los accesos por *SSH* bloquean la IP de los clientes que realicen 6 intentos en un corto periodo de tiempo durante 1 hora.

29. La gestión de las cuentas de usuario debe ser realiza de acuerdo a la política de seguridad de la organización, que debe ir alineada con las siguientes buenas prácticas:

    a) Las nuevas contraseñas no deben coincidir con al menos 10 de los valores anteriores.

    b) No deberá utilizarse la misma contraseña para acceder a distintos sistemas o equipos.

    c) Las contraseñas por defecto deben actualizarse lo antes posible.

    d) No deberá realizarse un cambio de contraseña en los 4 días posteriores al último cambio.

    e) Se debe evitar la utilización de palabras de diccionario, caracteres repetitivos o secuenciales (Ej: "*aaaaaa*" o "*1234abc*"), patrones de teclado (Ej: "*qazwsx*" o "*qwertyuiop*") o nombres propios específicos de contexto, nombres de usuario, nombre del host del sistema.

5.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

30. La plataforma se entrega con una de las interfaces configurada para la administración y gestión de la plataforma a través de *CLI* o *dashboard*.

31. El *appliance* dispone de una interfaz de red *IPMI 2* para la conexión remota a la consola. Por seguridad, desde fábrica se entrega desactivada, siendo responsabilidad del cliente su activación posterior.

32. En la ilustración 1 se identifican las diferentes interfaces de red en la configuración *hardware* predeterminada:

Ilustración 1. Interfaces de red del producto

5.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

33. Todos los protocolos de red en la plataforma se entregan preconfigurados para garantizar la seguridad desde el primer instante.
34. Las comunicaciones hacen uso de *TLS v1.2* configurado por defecto. **Cualquier versión de *SSL* o *TLS* previa debe estar deshabilitada.**
35. El servicio *HTTP* está deshabilitado en el portal de administración y así debe permanecer, debiendo hacer uso de *HTTPS*. El navegador debe soportar el uso de *TLSv1.2* o superior. En caso contrario se rechazará la conexión.
36. Las conexiones a través de *SSH* de realizan utilizando el protocolo *SSHv2*.
37. La plataforma se entrega configurada para hacer uso exclusivamente de *Ciphers* admitidos en la guía CCN-STIC-807. **No se recomienda alterar esta configuración**, pero en caso necesario, se puede realizar editando los ficheros */etc/ssh/sshd_config* para las conexiones *SSH* y */etc/httpd/conf.d/ssl.conf* para las conexiones *HTTPS*.

5.5 GESTIÓN DE CERTIFICADOS

38. La plataforma implementa su propia infraestructura PKI para la generación de certificados digitales de uso interno. En el Manual de Usuario del dashboard [1], apartado 2.4 se describe el procedimiento para regenerar todos los certificados.
39. Recomendamos la generación de certificados usando longitudes de bits lo más amplias posibles con una duración en general no superior a 4 años.

5.6 ACTUALIZACIONES

40. La plataforma hace uso del sistema de gestión de paquetes *rpm* del sistema operativo para las actualizaciones.
41. Los paquetes se deberán descargar desde la web de soporte de KRC Española para el producto.
42. Se recomienda el uso de un equipo seguro tipo aduana para la descarga de los paquetes, evitando la conexión directa de la plataforma a Internet.
43. Los paquetes descargados en el equipo seguro, se podrán subir a la plataforma haciendo uso de *scp.*
44. Los paquetes de actualización se entregan firmados digitalmente y el usuario deberá verificar si la firma es correcta. Esta verificación se puede realizar desde la consola CLI ejecutar el comando *rpm -K <NombrePaquete>*.
45. Una vez verificada la firma, se podrá realizar la instalación de los paquetes con Nombre Paquete *rpm -i <NombrePaquete>.*
46. Esta operación sólo está disponible para el usuario *root* del sistema.

5.7 AUTO-CHEQUEOS

47. La plataforma no realiza autochequeos programados. Al reiniciar, se realiza un *check* de integridad de almacenamiento, memoria, CPU, como parte del *POST* del equipo y del sistema operativo.
48. Todos los paquetes están firmados, tanto los correspondientes al sistema operativo de base, como los propios de la plataforma. Se puede verificar la integridad de los paquetes utilizando *rpm –qaV,* una vez identificado como *root* en el sistema operativo.

5.8 AUDITORÍA

5.8.1 REGISTRO DE EVENTOS

49. La plataforma define dos (2) niveles de log:
    a) Nivel de sistema operativo: Registra información del sistema operativo, tales como inicios/cierres de sesión, servicios propios necesarios para el funcionamiento de la plataforma, mensajes de componentes del sistema, etc.
    b) Nivel de componentes HCI: Registra los logs de los diferentes componentes de la plataforma HCI: mensajes de la capa de computación, *storage*, images, etc.
50. De forma general, se auditan eventos de:
    a) Conexión/Desconexión.
    b) Cambios de contraseñas y permisos de usuarios.
    c) Cambios en la configuración del sistema.
    d) Eventos que afecten a la funcionalidad del sistema, como son creación de volúmenes, conexión/desconexión de interfaces de red, eventos de *kernel y* escalado de privilegios.
51. El formato de los logs y eventos se almacenan en texto, dentro de la carpeta del sistema operativo */var/log.*
52. Es posible modificar los eventos objeto de auditoría, así como las políticas de retención de los ficheros de log generados. Para efectuar estos cambios es necesario editar el fichero */etc/audit/rules.d/audit.rules.*
53. Sólo el usuario *root* tiene capacidad para visualizar el contenido de los ficheros de log.
54. Ningún usuario (incluyendo el *root*), tiene la capacidad de modificación de los ficheros de log.

5.8.2 ALMACENAMIENTO LOCAL

55. Todo el almacenamiento de los logs se realiza de forma local.
56. Las políticas definidas de contención de los logs son las siguientes:
    a) Sistema *Audit* del sistema operativo:
        i. Máximo 12 archivos de logs.
        ii. Tamaño del log generado: 12MB.
        iii. Rotación automática al alcanzar estos límites.
    b) Resto de componentes:
        i. Rotación semanal.
        ii. Mantiene 4 (14 en el caso de algunos componentes de la capa hiperconvergente) archivos de log.
        iii. Los archivos de log se sobreescriben para evitar el llenado del espacio de almacenamiento.
57. Las políticas se pueden modificar editando, una vez autenticado en el sistema como *root* mediante la edición de los ficheros */etc/audit/auditd.conf* y */etc/logrotate.conf*

5.8.3 ALMACENAMIENTO REMOTO

58. Esta versión del producto no permite el almacenamiento remoto de eventos de auditoría.

5.9 *BACKUP*

59. El sistema permite la generación de *snapshots* que pueden ser exportados para su extracción a través de canal seguro (*SSH)*. En el *Manual de Usuario del dashboard* [1], apartado 9, se describe el procedimiento para la generación de instantáneas.
60. Se recomienda el uso de *scp* para la extracción como método óptimo, dado el tamaño que pueden ocupar los *snapshots* de las instancias.
61. Para realizar un *backup* de la configuración existente, basta con realizar una copia del directorio */etc* del sistema, donde se almacena la configuración para su posterior restauración en otro *appliance*.
62. La periodicidad de la realización de *snapshots* y *backups* dependerá en gran medida de la volatilidad de la información almacenada y de los cambios en la configuración de la plataforma. De forma general, se recomienda realizar un *snapshot* previo a cambios en la configuración de las instancias y posteriormente, una vez verificada su funcionalidad.
63. Para el *backup* de la configuración existente, dado que no es una operación habitual realizar cambios a este nivel, se recomienda realizar un *backup* previo a

cualquier cambio en los ficheros de configuración, y una vez verificado el funcionamiento correcto realizar un nuevo *backup*.

5.10 SERVICIOS DE SEGURIDAD

64. El sistema implementa herramientas para prevenir posibles ataques. Los servicios asociados a las herramientas de prevención se entregan habilitados y configurados por lo que no es necesaria ninguna actuación para su activación.

65. Los servicios implementados son:

    a) Implementación de *firewall* de sistema operativo.

    b) Implementación de políticas de contraseña fuerte con detección de ataques de fuerza bruta.

    c) Implementación de políticas contra ataques *DoS* o *DDoS*.

    d) Implementación de contextos de seguridad SELinux por cada instancia.

6. FASE DE OPERACIÓN

66. Se recomienda realizar periódicamente una revisión de la plataforma para verificar el correcto funcionamiento y el nivel de vulnerabilidad siguiendo esta guía:

    a) Con un usuario identificado a nivel de sistema operativo como *root* comprobar:

    - Ficheros de log de la auditoría con el objetivo de localizar cambios en ficheros del sistema o en los servicios activos. Los ficheros de auditoría están ubicados en */var/log/audit.*
    - Fichero de registro de mensajes del sistema. Localizar posibles errores con *cat /var/log/messages | grep -i error*.
    - Ficheros log de la plataforma. Verificar los diferentes ficheros de log en busca de posibles errores de la plataforma HCI. Dentro del directorio */var/log* se encuentran las carpetas correspondientes a cada uno de los componentes del sistema (*nova, cinder*, etc.).

    b) Comprobar la integridad de los paquetes instalados con *rpm -qaV*.

    c) Comprobar la versión y *hash* de la instalación desde el *dashboard* accediendo a la opción *KatuaSDI->About.*

    d) Actualizar la BIOS del sistema a la última versión disponible en la web de soporte del producto.

    e) Actualizar los paquetes del sistema a la última versión disponible en la web de soporte del producto.

    f) Revisar la caducidad de certificados de la PKI integrada. En caso necesario, regenerar e instalar los certificados.

67. En la sección 2 del *Manual de Usuario del dashboard* [1] se describen los procedimientos de actualización y regeneración de certificados.

7. *CHECKLIST*

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Autenticación segura	☐	☐	
Configuración de administradores	☐	☐	
Configuración de interfaces de red	☐	☐	
CONFIGURACIÓN DE PROTOCOLOS SEGUROS			
Gestión de certificados	☐	☐	
OPERACÍON			
AUDITORIA			
Activación auditoría	☐	☐	
Registro de mensajes del sistema	☐	☐	
Logs de componentes de la plataforma HCI	☐	☐	
Verificación de paquetes	☐	☐	
Comprobación de versión y *hash* de producto	☐	☐	

8. REFERENCIAS

[1] «Manual de usuario del dashboard de Katua SDI Platform,» [En línea].

[2] «Manual de usuario de línea de comando de Katua SDI Platform,» [En línea].

[3] CCN-STIC-104 Catálogo de productos con clasificación ZONING.

[4] Guía CCN-STIC-807 - Criptografía de empleo en el Esquema Nacional de Seguridad.

9. ABREVIATURAS

CLI *Command Line Interface*

CCN Centro Criptológico Nacional

CPD Centro de Procesamiento de Datos

DoS *Denial of Service*

DDoS *Distributed Denial of Service*

ENS Esquema Nacional de Seguridad

HCI *Hyper-Converged Infrastructre*

HTML *HyperText Markup Language*

HTTPS *Hypertext Transfer Protocol Secure*

PKI *Public Key Infrastruture*

POST Power-*on self-test*

SCP *Secure Copy*

SSH *Secure Shell*

STIC Seguridad de las Tecnologías de la información y comunicación

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