centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC-1510

Procedimiento de empleo seguro
metaOLVIDO Dashboard

Enero 2024

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
2024.02.01 12:36:47 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-025-2.
Fecha de Edición: enero de 2024.

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. metaOLVIDO Dashboard en una aplicación web (Onpremise) que permite la gestión y aplicación centralizada de todas las políticas de metadatos de la organización, garantizando la máxima protección ante la fuga de información sensible. Entre sus principales funcionalidades se encuentran:

    - Gestión centralizada de plantillas de metadatos para establecer políticas homogéneas en la organización.
    - Gestión y distribución centralizada de actualizaciones de los distintos productos metaOLVIDO instalados en la Organización.
    - Visualización de toda la actividad realizada en los distintos nodos a través de diferentes gráficas e informes que muestran los metadatos procesados y organizados por grupos de metadatos.
    - Integración con LDAP para la asignación de plantillas de metadatos, así como para el control de acceso a la consola.

2 OBJETO Y ALCANCE

2. El presente documento tiene como objetivo detallar las configuraciones de seguridad del producto metaOLVIDO Dashboard, de forma que la protección y funcionamiento del producto se realice de acuerdo con unas garantías mínimas de seguridad.

3. Los componentes de metaOLVIDO Dashboard se distribuyen a través de un fichero comprimido ZIP el cual contiene todos los elementos necesarios para el despliegue de la aplicación (Base de datos + Aplicación).

4. metaOLVIDO Dashboard se ejecuta sobre Sistemas Operativos Linux (Ubuntu, Debian y SuSE). **Se recomienda instalar metaOLVIDO sobre una máquina virtual** con los siguientes recursos mínimos:

	Requisitos básicos		
	vCPU	**RAM**	**HD**
metaOLVIDO Dashboard	2	4	200 MB

5. El producto mencionado en esta guía ha sido cualificado e incluido en el **Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC)** en la familia de "***Gestión de metadatos***". Se recomienda consultar el Catálogo para conocer la versión cualificada en cada momento.

3 ORGANIZACIÓN DEL DOCUMENTO

6. El presente documento se estructura en las secciones indicadas a continuación:

   - 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. Referencias.
   - Apartado 7. Abreviaturas.

4 FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. El fichero de distribución de metaOLVIDO se pone a disposición del cliente a través de la solución LORETO del Centro Criptológico Nacional.
8. Una vez publicado, se comunica al cliente vía email la siguiente información relacionada con la descarga de la aplicación:
   - URL de acceso a la aplicación LORETO.
   - Contraseña de acceso.

   Desde la propia aplicación LORETO se mostrará el enlace para la descarga del fichero de distribución (ZIP) que contendrá los elementos necesarios para:
   - Creación e inicialización de la base de datos.
   - Despliegue de la aplicación.

   Además, se mostrará el Hash SHA256 del fichero ZIP publicado.
9. El manual de instalación y operación de metaOLVIDO Dashboard está disponible en la página web pública de la herramienta del Centro Criptológico Nacional.
10. Antes de realizar el despliegue la solución metaOLVIDO **se debe validar que el hash del paquete descargado es correcto**. En la citada página web de la solución, también se publican los valores *hash* de los paquetes de instalación.

4.2 REGISTRO Y LICENCIAS

11. Se puede verificar que el material entregado se corresponde con el material publicado mediante la comprobación del hash del fichero ZIP descargado, que queda registrado en la plataforma LORETO, para poder ser verificado en cualquier momento, quedando así registro de versión y paquetería.

4.3 CONSIDERACIONES PREVIAS

12. metaOLVIDO Dashboard se despliega sobre una infraestructura compuesta por los siguientes elementos: Apache + PHP + MariaDB.
13. Una vez la organización ha instalado estos componentes, deberá configurar el Servidor Web Apache y cargar los módulos PHP necesarios tal y como se especifica en el manual de instalación y operación de metaOLVIDO, sección “Configuración del entorno” páginas 4 a 6.

4.4 INSTALACIÓN

14. La instalación de la aplicación está formada por 2 fases: La primera se refiere a todas las tareas relacionadas con la base de datos y la segunda con el propio despliegue de la aplicación.

15. La organización se encargará de la instalación de estos componentes siguiendo las instrucciones especificadas en el manual de instalación y operación de metaOLVIDO, sección “Creación de la base de datos y despliegue de la aplicación” páginas 6 a 8.
16. Se establecerán los parámetros específicos de la aplicación en el fichero: `/var/www/html/api/config.json` tal y como se indica en el manual de instalación y operación de metaOLVIDO, sección “Fichero de configuración metaOLVIDO Dashboard” páginas 8 y 9.
17. El parámetro: “apiKey” identifica de forma única la instalación del producto en la organización, y permite validar la legitimidad de los diferentes clientes metaOLVIDO (endPoint y Server) con los que interactúa.
18. El parámetro: “authorizedLDAPUsers” se utiliza para indicar los uid de los usuarios del LDAP habilitados para el acceso a la consola metaOLVIDO Dashboard. Para utilizar esta funcionalidad es necesario configurar el cliente de LDAP tal y como se especifica en el manual de instalación y operación de metaOLVIDO, sección “Fichero de configuración del LDAP” página 9.

5 FASE DE CONFIGURACIÓN

5.1 AUTENTICACIÓN

19. El acceso a la interfaz gráfica de metaOLVIDO Dashboard se realiza desde un navegador utilizando HTTPS sobre TLSv1.2 y está controlado mediante el uso de una pareja de valores usuario y contraseña.
20. Para el acceso a la interfaz gráfica se distinguen 2 tipos de usuarios:
    - Usuario de base de datos: Se podrán crear tantos usuarios como se requieran, las contraseñas se almacenan en la base de datos local cifradas mediante un algoritmo hash. Este algoritmo no es configurable por parte del usuario.
    - Usuario de LDAP: Por defecto todos los usuarios del LDAP tendrán acceso a la aplicación, **se recomienda configurar el parámetro "authorizedLDAPUsers"** para identificar al usuario o grupo de usuarios que tendrán acceso a la interfaz gráfica de metaOLVIDO Dashboard.
21. El inicio de sesión en metaOLVIDO requiere introducir el nombre de usuario y su contraseña de acceso con el fin de validar la identidad de la persona que desea autenticarse en el sistema.
22. Si estos datos son incorrectos, metaOLVIDO notificará el motivo del rechazo e invitará al usuario a introducir los datos nuevamente; si, por el contrario, son correctos, se autorizará el acceso.
23. En caso de producirse 3 errores consecutivos en el inicio de sesión, el usuario quedará bloqueado y podrá iniciar el proceso de regeneración de contraseña desde la ventana inicio de sesión, tal y como se detalla en el manual de instalación y operación de metaOLVIDO, sección "Regeneración de contraseña de usuario Base de Datos", página 11.

5.2 ADMINISTRACIÓN DEL PRODUCTO

5.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

24. Se utilizará la interfaz web para la operación del producto y para algunas labores de configuración, como la gestión de usuarios de base de datos y la integración con el LDAP corporativo para la autenticación en la interfaz gráfica de metaOLVIDO. La conexión a esta interfaz se realiza mediante HTTPS sobre TLSv1.2 por defecto.
25. Las restricciones de acceso remoto HTTPS quedan delegadas en la seguridad de redes de la organización.
26. Tan solo se puede acceder al producto remotamente mediante HTTPS. No existe otro tipo de acceso no seguro como HTTP, Telnet, etc.

5.2.2 CONFIGURACIÓN DE ADMINISTRADORES

27. Los usuarios de la aplicación web metaOLVIDO Dashboard no disponen de diferentes perfiles o roles, todos los usuarios tendrán los mismos privilegios y capacidades.
28. El script de inicialización de la base de datos crea un usuario por defecto (metaclean) a partir del cual iniciaremos sesión en la interfaz web y se podrán crear los usuarios de base de datos que se requieran, así como configurar la integración con el LDAP corporativo en su caso.
29. Se debe modificar tanto la contraseña como el email asociado al usuario *metaclean*, siguiendo la política de contraseñas establecida en el apartado 5.2.3 POLÍTICA DE CONTRASEÑAS Y PARÁMETROS DE SESIÓN. Para ello, acceder al menú: Administración → Gestión de usuarios tal y como se especifica en el manual de instalación y operación de metaOLVIDO, sección “Gestión de usuarios”, página 18.

5.2.3 POLÍTICA DE CONTRASEÑAS Y PARÁMETROS DE SESIÓN

30. El producto permite definir el tiempo de inactividad de las sesiones, tras el cual será necesario reautenticarse. Por defecto está establecido en 10 minutos. La configuración del tiempo de inactividad se realiza en el fichero de configuración `/var/www/html/api/config.json` a través del parámetro “timeout_minutes”.
31. Para la creación de usuarios, el prodcuto obliga a completar los siguientes parámetros: Login, Password, Nombre e Email. Las restricciones de cada uno de estos parámetros son las siguientes:
    - Login: No permite caracteres en blanco y permite hasta un máximo de 50 caracteres.
    - Password: Longitud entre 12 y 50 caracteres, al menos una mayúscula, un número y un carácter especial.
    - Nombre: Longitud entre 1 y 50 caracteres.
    - Email: Formato de correo válido entre 12 y 50 caracteres.

5.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

32. Los únicos puertos (y servicios) abiertos son HTTPS y SSH.

5.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

33. El acceso a la GUI mediante HTTPS se debe configurar mediante un certificado firmado por un CA válida y reconocida por el organismo, para ello se deberá proceder como se indica en el apartado 5.5 GESTIÓN DE CERTIFICADOS.
34. El producto utiliza por defecto el protocolo TLS versión 1.2 o superior. La configuración de dicho protocolo corresponde a la organización.

5.5 GESTIÓN DE CERTIFICADOS

35. El configurador del sistema de la organización realizará los siguientes pasos para la configuración de los certificados requeridos para el protocolo HTTPS:

    - Copiar el fichero de certificado a utilizar en metaOLVIDO (fichero denominado de ahora en adelante metaOLVIDO.crt) a la ruta `/etc/ssl/certs/metaOLVIDO.crt` a través de SSH/SCP. El fichero de certificado no debe tener clave de apertura.
    - Copiar el fichero de clave privada del certificado a utilizar en metaOLVIDO (fichero denominado de ahora en adelante metaOLVIDO.key) a la ruta `/etc/ssl/private/metaOLVIDO.key` a través de SSH/SCP.
    - Copiar el fichero de claves públicas de la entidad certificadora y sus entidades de certificación intermedias, que firman el certificado anterior a utilizar en metaOLVIDO (fichero denominado de ahora en adelante ca.crt) a la ruta `/etc/ssl/certs/ca.crt` a través de SSH/SCP. El fichero de certificado no debe tener clave de apertura.
    - Editar el archivo `/etc/apache2/sites-available/default-ssl.conf` mediante vi:
        - Modificar la línea que comienza por SSLCertificateFile de forma que quede así:

          `SSLCertificateFile /etc/ssl/certs/metaOLVIDO.crt`
        - Modificar la línea que comienza por SSLCertificateKeyFile de forma que quede así:

          `SSLCertificateFile /etc/ssl/private/metaOLVIDO.key`
        - Agregar tras la línea anterior la línea indicada a continuación:

          `SSLCertificateFile /etc/ssl/certs/ca.crt`

36. El configurador del sistema de la organización realizará los siguientes pasos para la configuración del certificado requerido para la integración con el servicio LDAPS:

    - Crear el directorio: `/etc/ldap/cacerts` y copiar el certificado CA del servidor LDAP en el directorio: `/etc/ldap/cacerts` (fichero denominado de ahora en adelante ca.cert.ldap.pem)
    - Editar el fichero: `/etc/ldap/ldap.conf` y añadir la siguiente configuración:

      ```
      TLS_CACERTDIR /etc/ldap/cacerts
      TLS_CACERT /etc/ldap/cacerts/ca.cert.ldap.pem
      TLS_REQCERT hard
      ```

5.6 SINCRONIZACIÓN HORARIA

37. Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados para permitir una alta fiabilidad en los sistemas de auditoría y logging.

5.7 ACTUALIZACIONES

38. Las diferentes actualizaciones serán comunicadas al cliente vía email. El acceso al paquete de actualización estará disponible a través de la herramienta LORETO, de la misma forma a como se indica en el apartado 4.1 ENTREGA SEGURA DEL PRODUCTO.
39. El paquete de actualización contendrá, además de los diferentes ficheros de la aplicación, un fichero con las instrucciones necesarias para la correcta actualización del producto.
40. Antes de realizar la actualización, la organización debe verificar que el hash SHA-256 del paquete ZIP descargado es correcto, confirmando de este modo que no se ha realizado ninguna modificación del paquete.
41. Para comprobar la versión del producto accederemos a la página de login de la interfaz web de metaOLVIDO donde podremos ver la nueva versión.

5.8 SNMP

42. No se habilita el servicio SNMP en los componentes de metaOLVIDO.

5.9 ALTA DISPONIBILIDAD

43. Se delega en el motor de virtualización del cliente la capacidad de alta disponibilidad ante errores de apagado o sufrimiento de alguna otra avería.

5.10 AUDITORÍA

5.10.1 REGISTRO DE EVENTOS

44. El registro de eventos se encuentra detallado en el manual de instalación y operación de metaOLVIDO, sección “Fichero de Log -Registro de Actividad-” página 9.
45. En el directorio: /var/www/html/api/log se creará un fichero con el formato: MetaClean_MMM-AAAA.log donde se registrarán todas las acciones realizadas desde la interfaz metaOLVIDO Dashboard. Cada registro de auditoría almacenará la fecha y hora del evento, el usuario que genera el registro de autoría y la acción realizada. Si el resultado del evento es algún fallo se añadirá el siguiente texto al final de la cadena: "`:::: Result :::: Fail`".

    El formato de los registros de logs es el siguiente:

    ```
    [Mon 2024-01-08 04:33:37 PM] [usuario:metaclean] Edita plantilla: MetaClean_Web_Service
    ```

    Salida de log ante un intento de inicio de sesión fallido:

    ```
    [Mon 2024-01-08 04:34:13 PM] [usuario:] Error de inicio de sesión del usuario: metaclean :::: Result :::: Fail
    ```

5.10.2 ALMACENAMIENTO LOCAL

46. Todos los registros de logs se almacenan en el directorio: /var/www/html/api/log Estos logs rotan mensualmente.
47. Por defecto, la política de retención de los ficheros de logs es de un año. Esta configuración solo puede ser modificada por un usuario Administrador de la máquina.

5.10.3 ALMACENAMIENTO REMOTO

48. No se habilita el almacenamiento remoto de registros de auditoría.

5.11 BACKUP

49. No existe un método de backup de la máquina. Al tratarse de máquinas virtuales, se recomienda realizar una copia del estado de las diferentes máquinas virtuales de forma periódica y almacenarlo en una ubicación segura.

6 REFERENCIAS

REF1 Manual de instalación y operación de metaOLVIDO.
https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/503-metaolvido-dashboard/file

7 ABREVIATURAS

CCN	Centro Criptológico Nacional.
CPD	Centro de Procesamiento de Datos.
GUI	Interfaz Gráfica de Usuario.
HTTPS	Hypertext Transfer Protocol Secure.
SSH	Secure Shell.
TLS	Transport Layer Security.
URL	Uniform Resource Locator.

PUBLICACIONES DE DEFENSA

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