centro criptológico nacional

Guía de seguridad TIC
CCN-STIC 887B

Guía rápida de Prowler

Marzo 2023

MINISTERIO DE DEFENSA

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

cpage.mpr.gob.es

Edita:

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
2023.04.13 18:38:44 +02'00'

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2023

NIPO: 083-23-109-4
Fecha de Edición: marzo de 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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

Prowler: Guía de inicio rápido

Prowler es una herramienta de software libre que permite analizar el estado de la seguridad de múltiples servicios y recursos desplegados en la nube de forma manual o automática.

En el momento de escribir esta guía, Prowler soporta 250 controles o chequeos para AWS, 20 para Azure y 43 para Google Cloud, sin embargo, la aplicación del nuevo ENS está soportado para AWS y es lo que se contempla en esta guía.

La instalación y uso de la herramienta para análisis del estado de seguridad basado en el ENS se describe en esta guía. La documentación oficial de la herramienta para su instalación y uso se encuentra en la siguiente dirección web: https://docs.prowler.cloud. El código fuente de la herramienta se encuentra en la siguiente dirección web: https://github.com/prowler-cloud/prowler.

A continuación, se muestran algunos ejemplos de las posibles visualizaciones de una auditoría del ENS automatizada con Prowler:

Estado de Cumplimiento de ENS RD2022 - AWS:

46.55% (1060) NO CUMPLE	53.45% (1217) CUMPLE

Resultados de ENS RD2022 - AWS:

Proveedor	Marco/Categoria	Estado	Alto	Medio	Bajo	Opcional
aws	operacional/explotación	NO CUMPLE	819	0	17	0
aws	medidas de protección/protección de los servicios	NO CUMPLE	1	0	0	0
aws	operacional/control de acceso	NO CUMPLE	620	0	0	0
aws	operacional/monitorización del sistema	NO CUMPLE	172	0	0	0
aws	medidas de protección/protección de los soportes de información	NO CUMPLE	238	0	0	0
aws	medidas de protección/protección de las comunicaciones	NO CUMPLE	413	0	0	0

* Solo aparece el Marco/Categoria que contiene resultados.

Resultados detallados de ENS en:
- CSV: /Users/toni/output/prowler-output-741399645537-20230316134413_ens_rd2022_aws.csv

Fig 1. Tabla resumen de resultados basado en los requisitos del ENS

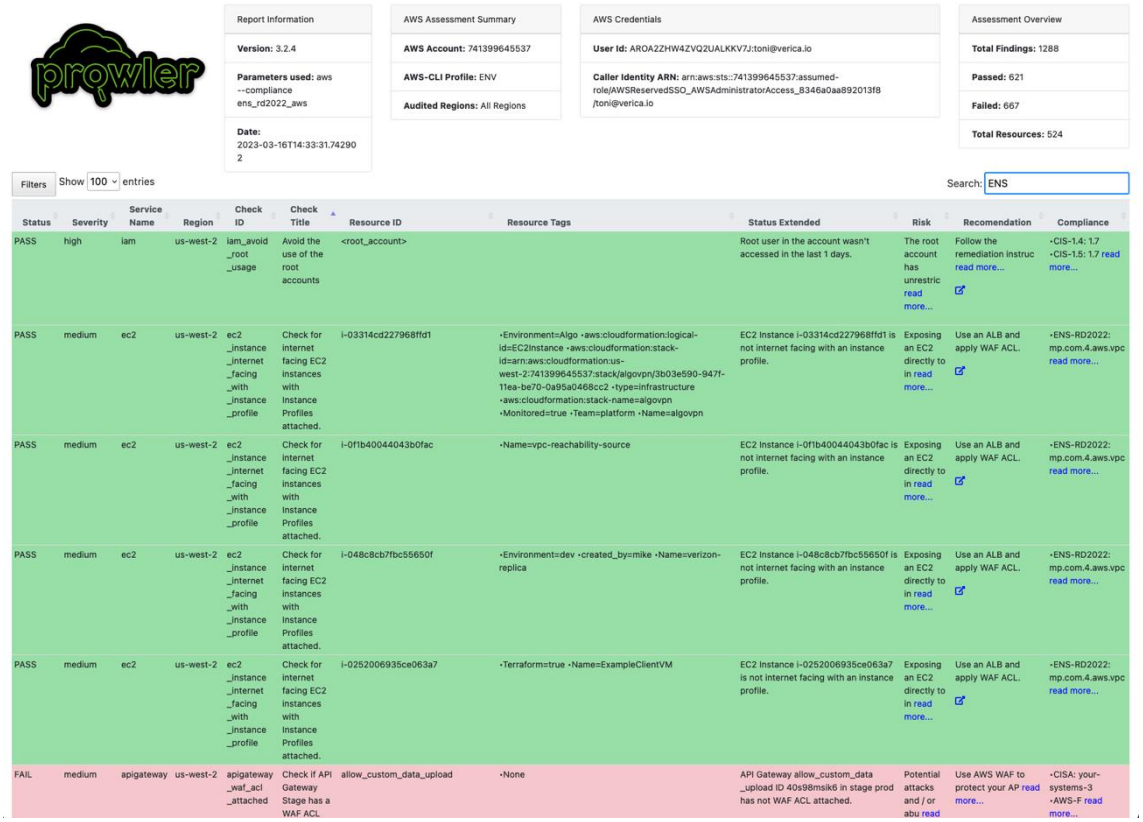

Fig 2. Ejemplo de reporte generado automáticamente en formato HTML.

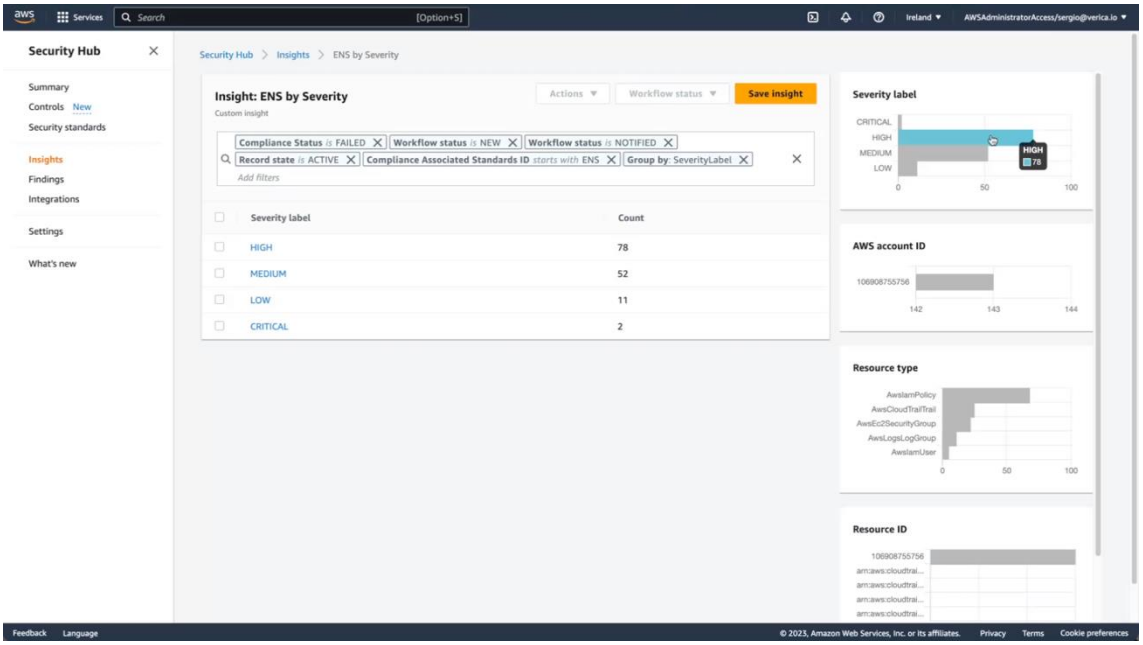

Fig 3. Ejemplo de reporte generado en AWS Security Hub.

A lo largo de la guía se hace referencia a controles de seguridad basados en las recomendaciones del ENS, dichos controles tienen unos identificadores únicos del tipo “op.exp.4.aws.sys.1“. Cada uno de esos identificadores se corresponde con un control o chequeo de Prowler. En esta guía de inicio rápido se muestra cómo generar informes con Prowler que permitan ver el resultado de todos esos controles en múltiples formatos y analizar el estado de la seguridad de la

infraestructura en AWS y así tomar decisiones que permitan mejorar la postura de seguridad en la nube.

1. Despliegue automático:

Para obtener reportes de Prowler para una cuenta de AWS se puede usar una plantilla existente de CloudFormation que automatizará y generará los reportes en el momento de desplegarla y también de forma periódica si así se especifica. Los reportes se almacenarán en un bucket de Amazon S3 que se crea automáticamente. Adicionalmente, siguiendo los siguientes pasos, Prowler enviará las recomendaciones a AWS Security Hub.

Requisitos y pasos:

1. Hay que activar AWS Security Hub en la región de AWS donde se esté trabajando, en este ejemplo usaremos Irlanda (eu-west-1):

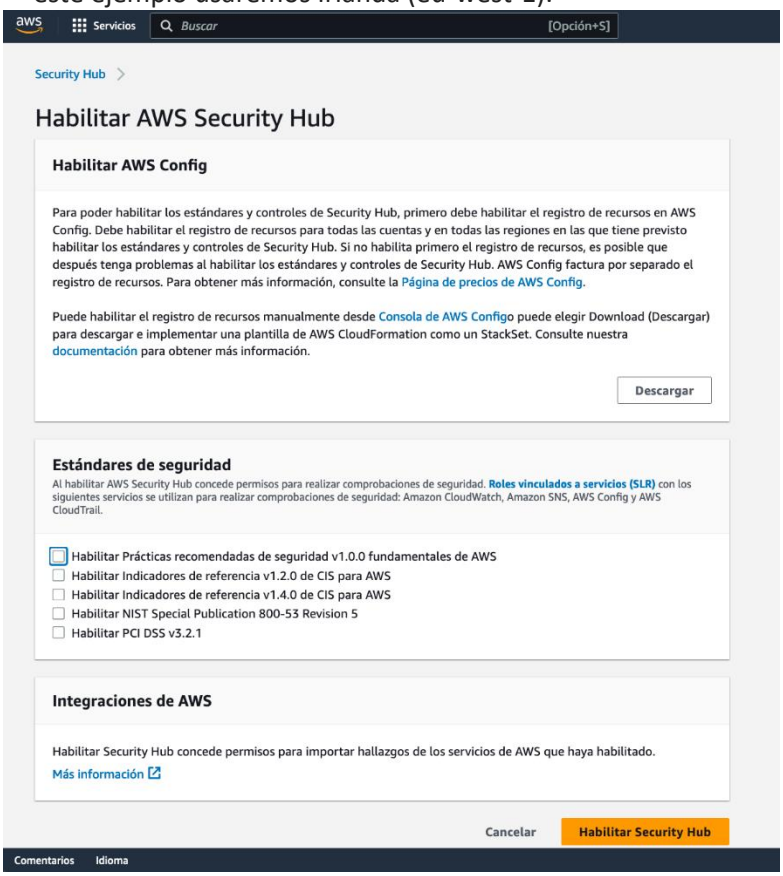

Fig 4. Activación de AWS Security Hub

NOTA: Aunque Prowler por defecto puede escanear en todas las regiones disponibles de AWS, el servicio AWS Security Hub funciona basado en región, así que deberíamos activarlo en todas las regiones que queramos usarlo y enviar resultados de Prowler. En esta guía se usa una sola región.

2. Una vez activado, hay que permitir aceptar resultados de Prowler desde la sección "Integraciones":

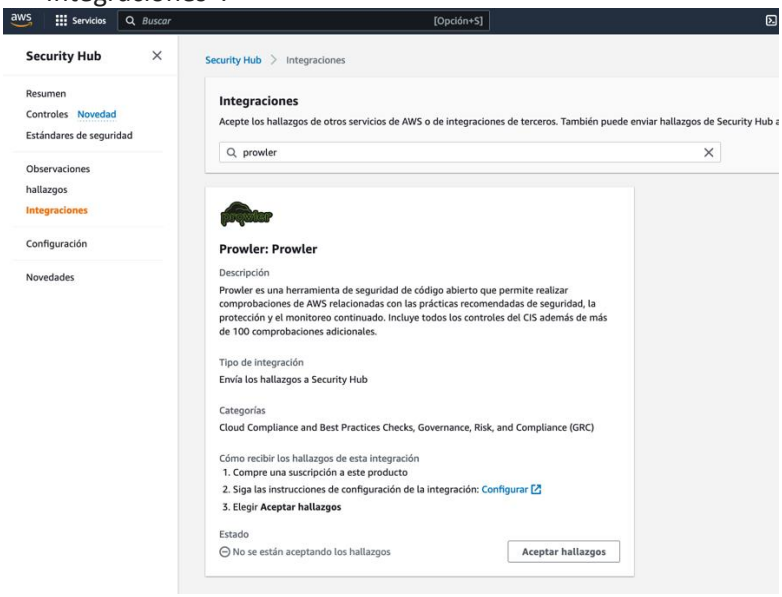

Fig 5. Habilitar Prowler recibir recomendaciones y resultados cada vez que se ejecute.

3. Para desplegar la plantilla de AWS Cloudformation de Prowler debemos descargarla desde el repositorio oficial de Prowler en GitHub (https://github.com/prowler-cloud/prowler), concretamente el fichero [codebuild-prowlerv3-audit-account-cfn.yaml] que se encuentra en [contrib/codebuild/codebuild-prowlerv3-audit-account-cfn.yaml]
4. Desde la consola de AWS CloudFormation, en la misma región donde hemos activado AWS Security Hub, clic en "Crear pila" y después "Con recursos nuevos (estándar)":

Fig 6. Seleccionar plantilla de CloudFormation.

5. Y se selecciona la plantilla yaml que hemos descargado:

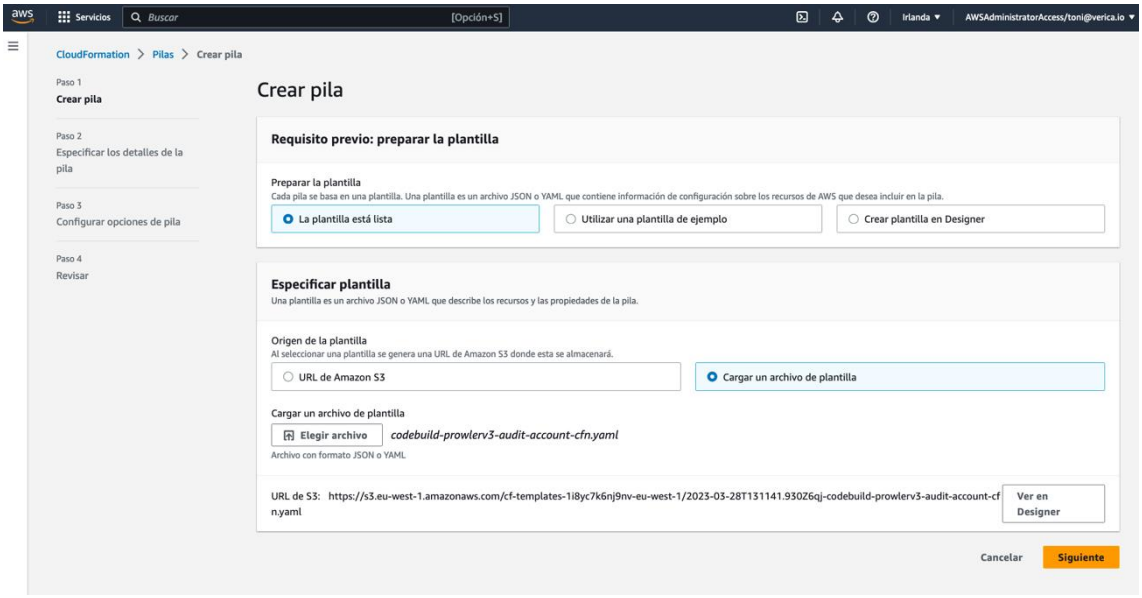

Fig 7. Subir plantilla a la pila de CloudFormation.

6. Clic en “Siguiente” y rellenar los siguientes datos:
   a. “**Nombre de la pila**” que se llamará “**Verificacion-ENS-con-Prowler**”.
   b. “**LogsRetentionInDays**” es para indicar los días que se deseen mantener los logs del entorno, no está relacionado con los informes, es útil para debug. “**3**” es por defecto.
   c. “**ProwlerOptions**” permite personalizar cómo se ejecutará Prowler y es el parámetro más importante, si queremos ejecutar los controles relacionados con el ENS y a la vez generar reportes en todos los formatos disponibles además de enviar las recomendaciones a AWS Security Hub debemos especificar las opciones siguientes sin comillas “**--compliance ens_rd2022_aws --filter-region eu-west-1 --security-hub**”:
      i. **--compliance ens_rd2022_aws** porque vamos a analizar concretamente el nuevo ENS.
      ii. **--filter-region eu-west-1** ya que en este caso "eu-west-1” es la región de Irlanda donde hemos activado AWS Security Hub, se pueden añadir tantas regiones como sea necesario separadas por espacio. Deben tener Security Hub con Prowler activado.
      iii. **--security-hub** ya que vamos a enviar los resultados a AWS Security Hub.
   d. “**ProwlerScheduler**”: Prowler se ejecutará justo al desplegar la plantilla y posteriormente se ejecutará cada vez que se indique con este parámetro. Por defecto cada día a las 22h.
   e. “**ServiceName**”: añade un identificador único al despliegue, “**prowler**”.
7. Clic en “Siguiente” y se dejan los valores por defecto en esa pantalla.

8. Clic en “Siguiente” y en la última pantalla de selecciona la opción “Capacidades” y después “Enviar”:

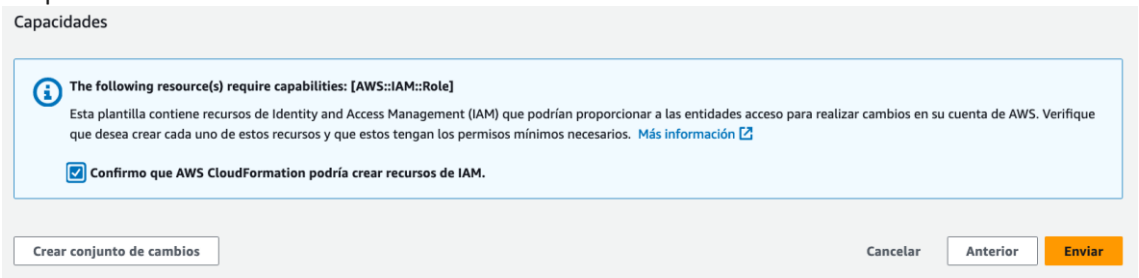

Fig 8. Enviar la configuración para crear el despliegue de Prowler.

9. Después de unos 3 minutos aproximadamente estará disponible el entorno, se verá “CREATE_COMPLETE” junto al nombre de la pila:

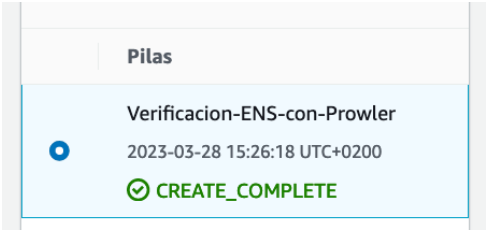

Fig 9. Despliegue de plica completado.

10. En este momento Prowler estará ejecutándose y tardará unos minutos más en producir resultados, depende del número de recursos que haya en la cuenta de AWS y en dicha región. En la sección “Outputs” aparecerá el nombre del bucket donde se almacenarán los informes en html,csv,json y json con formato ASFF.

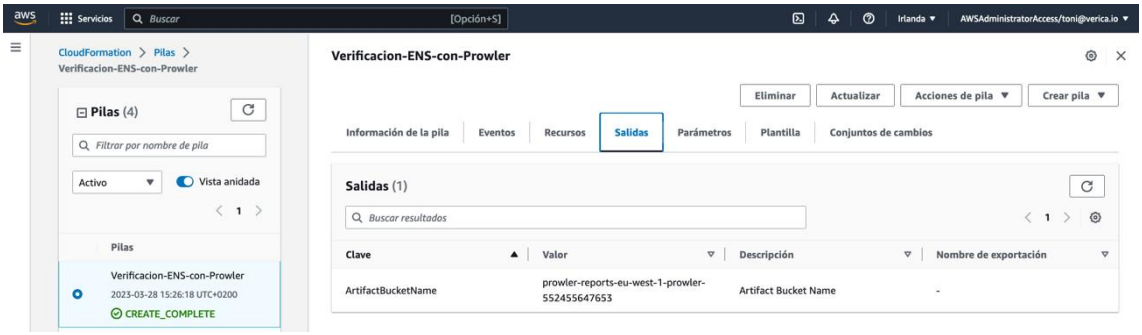

Fig 10. Sección “Salidas” de la pila desplegada donde podemos ver el nombre del bucket de S3.

Adicionalmente veremos los hallazgos en AWS Security Hub:

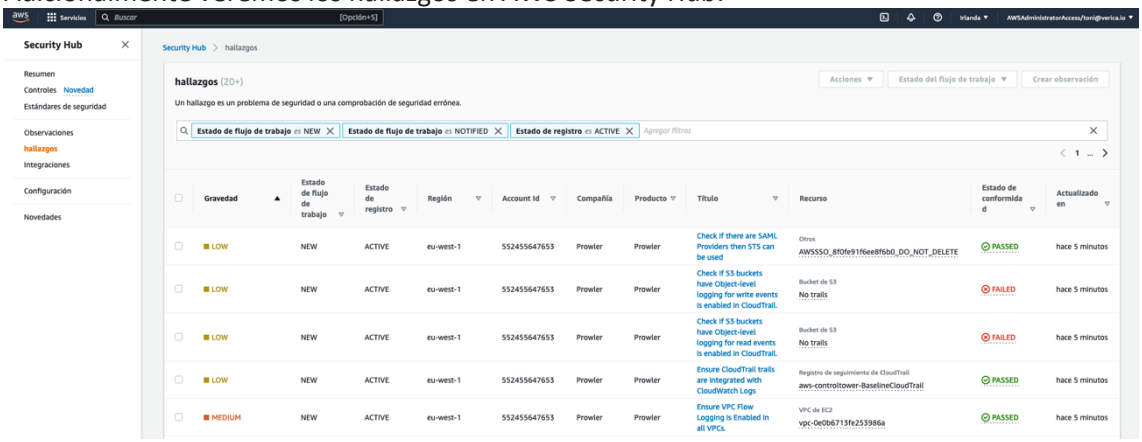

Fig 11. Hallazgos de Prowler AWS Security Hub.

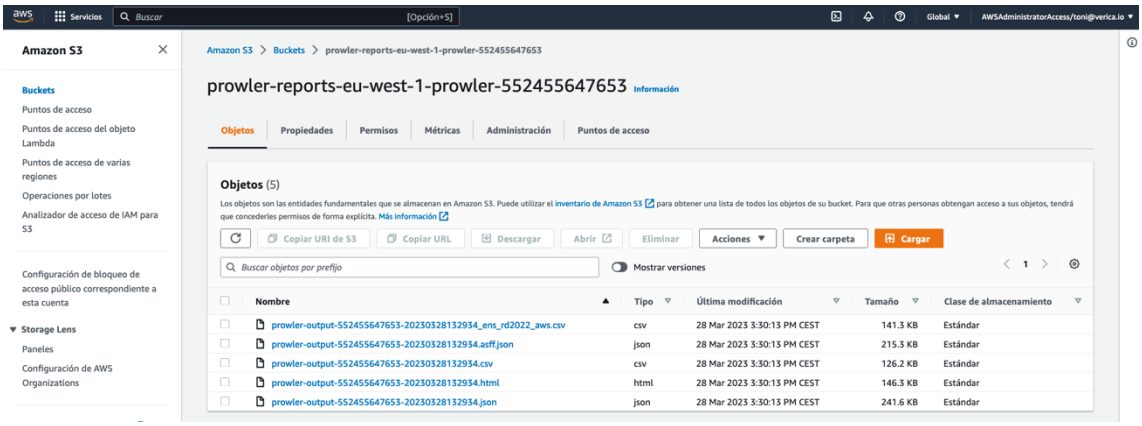

Fig 12. Reportes creados en el bucket S3.

11. Los reportes generados corresponden a:
    a. prowler-output-*_ens_rd2022_aws.csv: CSV específico del nuevo ENS con especificaciones concretas del ENS.
    b. prowler-output-*.asff.json: JSON específico enviado a AWS Security Hub.
    c. prowler-output-*.csv: CSV con todos los metadatos que ofrece Prowler.
    d. prowler-output-*.html: HTML resumido con los metadatos mas relevantes para auditorías.
    e. prowler-output-*.json: JSON con todos los metadatos que ofrece Prowler.
12. Para más información sobre despliegue de infraestructura como código con AWS CloudFormation visite el siguiente enlace: https://docs.aws.amazon.com/es_es/AWSCloudFormation/latest/UserGuide/Welcome.html

2. Despliegue manual:

Si se requiere usar Prowler desde la línea de comandos ya sea en una estación de trabajo o en una instancia de EC2 y hacer comprobaciones puntuales o específicas, se puede hacer desde Linux, MacOS o Windows. Para ello es necesario tener Python 3.9 o superior junto con el gestor de paquetes PIP.

Ejecutando el siguiente comando con PIP se instalará Prowler y todas sus dependencias:

```
pip install prowler
```

Prowler necesitará permisos para poder realizar la tarea de análisis en la cuenta de AWS que se pretende escanear, para ello debe ejecutarse con un perfil que tenga al menos los siguientes permisos: SecurityAudit y ViewOnlyAccess como politicas IAM y también estos permisos adicionales listados aquí https://github.com/prowler-cloud/prowler/blob/master/permissions/prowler-additions-policy.json y para poder enviar recomendaciones as AWS Security Hub estos permisos https://github.com/prowler-cloud/prowler/blob/master/permissions/prowler-security-hub.json.

Todas las opciones de instalación y requisitos están contempladas en la siguiente dirección https://docs.prowler.cloud/en/latest/#quick-start

Y ahora se ejecuta Prowler para analizar los controles del ENS en todas las regiones de AWS y ver los resultados por pantalla:

```
prowler --compliance ens_rd2022_aws
```

Al igual que en el despliegue automático, este comando generará todos los reportes en un directorio llamado “output” desde donde se ejecute el comando.

Estado de Cumplimiento de ENS RD2022 - AWS:

46.55% (1060) NO CUMPLE	53.45% (1217) CUMPLE

Resultados de ENS RD2022 - AWS:

Proveedor	Marco/Categoria	Estado	Alto	Medio	Bajo	Opcional
aws	operacional/explotación	NO CUMPLE	819	0	17	0
aws	medidas de protección/protección de los servicios	NO CUMPLE	1	0	0	0
aws	operacional/control de acceso	NO CUMPLE	620	0	0	0
aws	operacional/monitorización del sistema	NO CUMPLE	172	0	0	0
aws	medidas de protección/protección de los soportes de información	NO CUMPLE	238	0	0	0
aws	medidas de protección/protección de las comunicaciones	NO CUMPLE	413	0	0	0

* Solo aparece el Marco/Categoria que contiene resultados.

Resultados detallados de ENS en:
- CSV: /Users/toni/output/prowler-output-741399645537-20230316134413_ens_rd2022_aws.csv

Fig 13. Tabla resumen de resultados basado en los requisitos del ENS

Si se necesita enviar recomendaciones a AWS Security Hub en una región en particular (donde esté activado AWS Security Hub, en este ejemplo Irlanda que es eu-west-1) se ejecutará Prowler de la siguiente forma:

```
prowler --compliance ens_rd2022_aws \
        --filter-region eu-west-1 \
        --security-hub
```

3. Más información sobre Prowler:

- Para desplegar en múltiples cuentas a la vez se puede usar CloudFormation StackSets o siguiendo las instrucciones siguientes: https://github.com/prowler-cloud/prowler/tree/master/contrib/org-multi-account
- Si se ejecuta Prowler sin opciones analizará la cuenta en todas sus regiones disponibles.

- Al usar "--security-hub" se envían todos los resultados a Security Hub, incluyendo FAILED y PASSED, para enviar solo FAILED usar adicionalmente la opción "-q".
- Para obviar resultados fallados por estar aceptados se pueden hacer listas de permitidos, más información aquí: https://docs.prowler.cloud/en/latest/tutorials/allowlist/

Para profundizar más en el uso e integración de Prowler en otras aplicaciones así como usar otros controles de seguridad que pueden ser útiles ejecutar para incrementar el alcance de análisis de cuentas de AWS, visite la web de la herramienta: https://github.com/prowler-cloud/prowler. Para usar Prowler como un servicio online puede visitar https://prowler.pro

PUBLICACIONES DE DEFENSA

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