centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1243

Procedimiento de Empleo Seguro
Splunk Cloud

Marzo 2026

Edita:

centro criptológico nacional

CCN
c=ES, l=MADRID, o=CCN, ou=SELLO ELECTRONICO, 2.5.4.97=VATES-S2800155J, serialNumber=S2800155J, cn=CCN
2026.04.06 09:13:53 +02'00'

Fecha de Edición: Marzo de 2026

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. Splunk Cloud es una solución de gestión de eventos e información de seguridad (SIEM) basada en la nube que proporciona visibilidad en tiempo real del comportamiento del sistema a través del análisis de datos generados por múltiples plataformas.
2. Splunk Cloud permite recopilar, indexar y analizar datos de eventos de diversas fuentes, permitiendo capacidades completas de búsqueda, monitorización, investigación y respuesta ante incidentes. Esta solución se apoya en una arquitectura basada en la nube (AWS) e incorpora servicios como Splunk Web, Admin Config Service (ACS) CLI y Splunkd.
3. El acceso administrativo se realiza mediante una interfaz web segura (HTTPS/TLS) y la CLI de ACS, un API nativo de la nube que permite la administración programática. No se permite el acceso directo por CLI estándar de Splunk Enterprise. Las tareas administrativas no cubiertas por ACS pueden gestionarse mediante el portal de soporte.
4. Algunas de sus características principales son:
    - Splunk Web: Interfaz gráfica basada en navegador compatible con los navegadores modernos. Actúa como punto de redirección para autenticación en el proveedor de identidad (IdP) con MFA. Las autorizaciones se gestionan internamente por Splunkd.
    - Splunkd: Componente principal que gestiona la autenticación, autorización y ejecución de búsquedas. Cada búsqueda inicia un proceso independiente que accede únicamente a los índices permitidos según los privilegios del usuario.
    - Admin Config Service (ACS): API de administración en la nube que permite tareas administrativas de forma automatizada o manual. No se permite la modificación directa de archivos .conf por ningún medio de acceso administrativo.
    - Recolección de datos: Utiliza forwarders (Universal o Heavy) para capturar datos desde sistemas remotos. Puede recolectar datos desde archivos, eventos de red, fuentes Windows (logs, registro, WMI, Active Directory), y fuentes adicionales como APIs, HTTP Event Collector, colas FIFO, y más.
    - Indexación: Los datos son almacenados en índices, que pueden ser redimensionados o trasladados a almacenamiento como Amazon S3. Permite definir políticas de retención y archivado de datos.
    - Autenticación y control de acceso: La autenticación se delega a un IdP externo que implementa MFA y asigna roles. Las autorizaciones se realizan en el producto en base al rol asignado. Splunk soporta roles predefinidos y personalizados para una gestión granular del acceso.

2 OBJETO Y ALCANCE

5. El objetivo del presente documento es servir como guía para realizar una instalación y configuración segura de la solución Splunk Cloud.
6. Esta solución no se sitúa dentro de la categoría “Sistemas de gestión de eventos de seguridad” del catálogo CPSTIC para categoría ALTA.

3 ORGANIZACIÓN DEL DOCUMENTO

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. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. Al tratarse de un servicio en la nube, se dará de alta los datos del cliente en la plataforma de **Splunk Cloud** [REF1] y se enviarán de forma segura los accesos pertinentes a la plataforma.
8. El envío de los datos se realizará mediante correo electrónico firmado digitalmente, a la cuenta que se ha proporcionado para el alta.
9. Una vez dado el alta en la plataforma se podrá activar las licencias por cada usuario dentro de la plataforma.
10. Para la recolección de eventos, se podrán utilizar Splunk Universal Forwarders o Heavy Forwarders, que deben ser instalados en los sistemas del cliente desde los que se desee enviar datos a Splunk Cloud. Estos componentes actúan como fuentes externas de datos confiables y forman parte integral del entorno operativo desde la fase inicial. Es responsabilidad del cliente desplegarlos correctamente como parte de la preparación del entorno antes de la ingestión de datos.
11. Ambos tipos de forwarders pueden descargarse desde el **Portal Oficial de Descargas de Splunk** [REF18]. Desde ese mismo portal es posible obtener el archivo con el hash SHA-512 para verificar la integridad del instalador, así como la firma digital X.509 para validar su autenticidad.
12. Para más información acerca de la instalación e implementación de los forwarders consultar la guía **Deploy heavy and light forwarders** [REF12].

4.2 ENTORNO DE INSTALACIÓN SEGURO

13. Al tratarse de un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el producto.
14. El acceso se realiza mediante el uso de HTTPS con TLS1.2 para las comunicaciones seguras.
15. Sólo los usuarios autorizados y con la licencia activa podrán acceder al producto.
16. Ambos forwarders deben ser instalados por el cliente en entornos seguros y configurados con TLS1.2 siguiendo la documentación **Securing the Splunk platform with TLS** [REF15].

4.3 REGISTRO Y LICENCIAS

17. Para realizar la solicitud del servicio, se necesita una cuenta en el **Portal de Splunk** [REF17]. Desde ahí, se debe solicitar una instancia Cloud y se asigna una URL tipo: *"https://<instancia>.splunkcloud.com"*. No es necesario realizar una instalación, ya que el entorno ya estaría desplegado.
18. Una vez activada para el usuario, la licencia se basa en un modelo de uso. Existen diferentes modalidades, pudiendo medirse ese uso según diferentes parámetros listados en **Splunk Princing Options** [REF19].

4.4 CONSIDERACIONES PREVIAS

19. Al ser un servicio alojado en la nube, la consideración principal es, tener conexión a Internet y darse de alta en la plataforma para hacer uso del producto.

20. Los prerrequisitos para poder usar el producto son los siguientes:

    - Se necesita tener una suscripción a Splunk Cloud.
    - Tener configurados mecanismos de ingesta de datos. Esto puede incluir:
        - Splunk Universal Forwarder
        - Splunk Heavy Forwarder
        - AWS

21. Para más información sobre los forwarders compatibles con Splunk Cloud y cómo integrarlos correctamente, consultar la guía oficial **Enable forwarding on a Splunk Enterprise instance** [REF16].

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

22. El producto consta de los siguientes componentes principales:

    - Estación de trabajo de gestión: utilizada para fines de gestión.
    - Forwarders del producto: utilizados para recopilar eventos como fuentes de datos externas confiables.
    - Parte cloud del producto: VPC utilizada con la versión configurada.
    - Parte cloud fuera del producto: Componentes de AWS que son parte del entorno.
    - IdP con MFA: Para la autenticación de los usuarios.

23. Cada cliente de Splunk Cloud Platform en AWS tiene su propio entorno dentro de su propia Amazon Virtual Private Cloud (AWS VPC), donde se pueden aplicar controles de cifrado para los datos en tránsito y en reposo. AWS ofrece directrices de seguridad que las utilidades pueden usar al configurar su AWS VPC.

24. Los siguientes servicios de AWS serán considerados como parte del entorno de operación:

    - AWS Cloudwatch: servicio que monitorea aplicaciones, responde a cambios de rendimiento, optimiza el uso de recursos y proporciona información sobre la salud operativa.
    - AWS Cloudtrail: servicio de AWS que ayuda a habilitar la gobernanza, el cumplimiento y las auditorías de operaciones y riesgos. Las acciones realizadas por un usuario, rol o servicio de AWS se registran como eventos en CloudTrail.
    - AWS KMS: se utiliza para proteger toda la información en tránsito, almacenada, credenciales y certificados mediante mecanismos de cifrado.
    - AWS IAM: IAM se utiliza para gestionar los usuarios del servicio que usan el servicio AWS VPC para la asignación de la nube privada virtual de cada cliente.
    - AWS S3: se utiliza para la prevención de pérdida de datos, manteniendo el acceso a datos antiguos que se necesitan con fines de cumplimiento.
    - AWS ELB: se utiliza para distribuir el tráfico entrante entre múltiples instancias.
    - AWS EBS: se utiliza para almacenar los datos del servicio EC2 en la nube. Ofrece alta disponibilidad y mejor rendimiento que S3.
    - AWS WAF: redirige la conexión al AWS ELB donde se alojan las instancias de AWS EBS que contienen el producto.

5 FASE DE INSTALACIÓN

5.1 ADQUISICIÓN DE LA LICENCIA

25. La adquisición de una licencia para Splunk Cloud Platform se realiza a través de los siguientes modelos:
    - Workload pricing: Basado en la capacidad de cómputo medida en unidades de Splunk Virtual Compute (SVC).
    - Ingest Pricing: Basado en el volumen de datos ingeridos medido en GB/día.
26. Para obtener más información sobre los modelos de precios y adquirir una licencia, visitar la sección **Platform Pricing** [REF2].

5.2 CONFIGURACIÓN INICIAL DEL ENTORNO

27. Una vez adquirida la licencia, configurar el entorno de Splunk Cloud Platform:
    - Acceso al entorno: Iniciar sesión en el portal de Splunk Cloud utilizando las credenciales proporcionadas.
    - Configuración de políticas de acceso: Establecer políticas de acceso para garantizar que solo los usuarios autorizados puedan interactuar con el entorno.
    - Integración con AWS: Si el entorno está basado en AWS, configura la conectividad privada y las políticas de acceso necesarias para integrar Splunk Cloud Platform con los servicios de AWS.
28. Para una guía detallada sobre la configuración inicial, consultar el manual de administración de Splunk Cloud **Admin Manual** [REF3].

5.3 INGESTA DE DATOS

29. Para comenzar a trabajar con los datos en Splunk Cloud Platform, es necesario ingerir datos desde diversas fuentes:
    - Fuentes de datos externas: Utilizar Splunk Universal Forwarders o Heavy Forwarders para recopilar eventos de dispositivos y aplicaciones.
    - Configuración de entradas de datos: Configurar entradas de datos para recibir información desde archivos, directorios, eventos de red, datos de Windows, entre otros.
    - Monitoreo de datos de AWS: Si se estas utilizando AWS, configurar la ingesta de datos desde servicios como CloudWatch, CloudTrail y VPC Flow Logs.
30. Para obtener instrucciones detalladas sobre cómo ingerir datos en Splunk Cloud Platform a través de AWS, consultar la documentación **Get AWS data into Splunk Cloud Platform** [REF4].
31. Para obtener instrucciones detalladas sobre cómo ingerir datos en Splunk Cloud Platform a través de forwarders, consultar la documentación **Use forwarders to get data into Splunk Cloud Platform** [REF11].

5.4 ADMINISTRCIÓN Y MONITOREO

32. Una vez que los datos están siendo ingeridos, administrar y monitorear el entorno:

- Monitoreo de la salud del sistema: Utilizar la Consola de Monitoreo en la Nube para supervisar el rendimiento del sistema, el uso de recursos y la utilización de licencias.
- Administración de configuraciones: Emplear el Servicio de Configuración Administrativa (ACS) para realizar tareas de configuración y gestión de manera autónoma.
- Auditoría y registros: Configurar y revisar los registros de auditoría para rastrear acciones y eventos dentro del entorno.

33. Para más información sobre la administración y monitoreo en Splunk Cloud Platform, consultar el recurso **Splunk Cloud Platform deployment** [REF5].

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

34. Al tratarse de un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el producto. Para más información sobre el producto se debe consultar la documentación completa **Splunk Cloud Documentation** [REF6]**.**
35. El acceso se realiza mediante el uso de HTTPS con TLS1.2 o superior para las comunicaciones seguras y sólo los usuarios autorizados podrán acceder al producto. Todos los usuarios deben ser autenticados por el IdP antes de cual interacción con el producto.
36. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por el IdP. Sólo los usuarios con el rol de administrador pueden realizar las tareas de seguridad y modificar la configuración del producto.

6.2 AUTENTICACIÓN

37. El producto delega la autenticación y autorización en el IdP, para que los usuarios se autentiquen antes de cualquier interacción con el producto cuando el acceso se realiza a través de la interfaz web. Sin embargo, existe un único usuario administrador capaz de iniciar sesión directamente por la autenticación de Splunk, este usuario pertenece al equipo de soporte de Splunk y no existe posibilidad de crear otro usuario para la organización con los mismos privilegios.
38. La autenticación nativa de Splunk para el usuario administrador está protegida mediante una política de contraseñas que impone los siguientes requisitos de seguridad:
    - La contraseña debe tener una longitud mínima de 12 caracteres.
    - Debe incluir al menos una letra mayúscula y una letra minúscula.
    - Es obligatorio el uso de números y caracteres especiales (por ejemplo: !@#$%^&*()).
    - No se permite reutilizar ninguna de las últimas 10 contraseñas empleadas previamente.
    - Las contraseñas deben ser cambiadas obligatoriamente cada 90 días.
39. La contraseña inicial del usuario administrador se envía de forma segura a la cuenta de correo asociada al registro del tenant. Esta contraseña cumple con la política de contraseñas predeterminada definida por Splunk Cloud Platform.
40. Para más información acerca del procedimiento de cambio de contraseña, acceder a la documentación **Change a user password** [REF13].
41. Para más información acerca de la expiración de sesiones en splunk web consultar la documentación **Configure user session timeouts** [REF14]**.**
42. Los permisos se basan en el modelo de permisos de control de acceso basado en roles (RBAC). Un rol concede los permisos para realizar un conjunto de tareas y un grupo de roles es un conjunto de roles que permite a los usuarios realizar las tareas en el producto. Un usuario puede ser miembro de un rol. El producto puede usar varios roles.

43. El producto usa el Multi-Factor Authentication (MFA) propio del IdP configurado, protege el acceso a los datos y aplicaciones, y al mismo tiempo mantiene la simplicidad para los usuarios. Proporciona más seguridad, ya que requiere una segunda forma de autenticación y ofrece autenticación segura a través de una variedad de métodos de autenticación.

44. Más información en la guía **Integrate an Identity Provider** [REF7].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

45. Al ser un producto en la nube que forma parte de la infraestructura de AWS, la administración se realiza de forma remota utilizando el protocolo seguro HTTPS con TLS 1.2 o superior para el establecimiento de las comunicaciones seguras.

46. Los certificados usados por el servidor usan RSA con una longitud de clave de 2048 bits.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

47. Al tratarse de un servicio en la nube siendo parte de la infraestructura de AWS, la administración del producto se realiza de forma remota.

48. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en RBAC. Sólo los usuarios con el rol de administrador pueden realizar las tareas de seguridad y modificar la configuración del producto.

49. El producto utiliza RBAC (Control de Acceso Basado en Roles) para acceder a los recursos. A continuación, se enumeran cuatro roles fundamentales integrados. Los primeros tres se aplican a todos los tipos de recursos:

    - Admin: dispone de todos los permisos.
    - Power: permite editar todos los objetos compartidos y alertas.
    - User: permite crear, editar y ejecutar búsquedas.
    - SC_admin: se emplea para crear otros usuarios y roles, solo disponible para el equipo de soporte de Splunk, un único admin por organización.

50. En Splunk Cloud Platform, los roles se gestionan a través de la interfaz de usuario de Splunk Web o mediante la Admin Config Service (ACS) API.

51. La asignación de roles a usuarios se realiza durante el proceso de creación del usuario. Es posible asignar múltiples roles a un solo usuario, lo que le otorga un conjunto combinado de capacidades. La asignación de roles puede hacerse manualmente o mediante la integración con un proveedor de identidad (IdP) que soporte SAML 2.0, como Azure AD

52. Las capacidades en Splunk Cloud Platform determinan las acciones que un usuario puede realizar. Estas capacidades se asignan a los roles y, por ende, a los usuarios. Algunas capacidades comunes incluyen:

    - search: Permite realizar búsquedas.
    - admin_all_objects: Permite administrar todos los objetos.
    - edit_user: Permite editar usuarios.
    - edit_roles: Permite editar roles.

53. En el contexto de una configuración cualificada de Splunk Cloud Platform, la creación y autenticación de usuarios debe realizarse exclusivamente a través de un IdP compatible con SAML 2.0. En este modelo, Splunk delega completamente la autenticación de usuarios al IdP, y no se permite la creación de usuarios con credenciales internas (nombre de usuario y contraseña) dentro del propio entorno de Splunk. Esta configuración garantiza un control centralizado de identidades, el cumplimiento de políticas corporativas de seguridad y el uso obligatorio de mecanismos de autenticación robustos como MFA.
54. Para obtener más información sobre la gestión de usuarios y roles en Splunk Cloud Platform, consultar la documentación **Define roles on the Splunk platform with capabilities** [REF8].

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

55. Todo acceso al producto se realiza mediante el uso de HTTPS con TLS1.2 o superior.

6.5 GESTIÓN DE CERTIFICADOS

56. Al tratarse de un servicio en la nube siendo parte de la infraestructura de AWS los certificados usan RSA con longitud de clave de 2048 bits. Este cifrado es suficientemente robusto y, aunque se considera seguro para las comunicaciones en el momento de creación de este documento, se recomienda la utilización de RSA con longitud de clave de 3072 bits.
57. Para la gestión y configuración de la longitud de clave ver la subsección “Creación de claves” de la sección “3.1.2.2 Protección de claves criptográficas” de la **Guía de seguridad de las TIC CCN-STIC 887G** [REF9]**.**

6.6 SERVIDORES DE AUTENTICACIÓN

58. El producto usa un IdP previamente configurado para que los usuarios se autentiquen antes de cualquier interacción con el producto cuando el acceso se realiza a través de la interfaz web.
59. En el caso del usuario sc_admin, se autentica directamente contra el servidor de Splunk.

6.7 SINCRONIZACIÓN

60. Al tratarse de un servicio en la nube, los servidores donde está alojado el servicio se sincronizan mediante el uso de NTP con el proveedor de servicios en la nube.

6.8 ACTUALIZACIONES

61. Las actualizaciones se realizan automáticamente cuando están disponibles. Este proceso está completamente controlado por el CSP (Proveedor de Servicios en la Nube) porque el producto es parte de la infraestructura de AWS.
62. Todas las actualizaciones están firmadas digitalmente y aplicadas automáticamente por el CSP.

6.9 AUTO-CHEQUEOS

63. Al tratarse de un servicio en la nube, el proveedor de servicios en la nube realiza los auto-chequeos (self-test) de integridad del software y de la operación de los algoritmos y funciones criptográficas del producto de manera automatizada.

6.10 ALTA DISPONIBILIDAD

64. Al tratarse de un servicio en la nube, el proveedor de servicios en la nube brinda el servicio de alta disponibilidad sobre los servidores donde se aloja el servicio y las conexiones para el acceso al mismo.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

65. Splunk Cloud Platform registra automáticamente todos los eventos de seguridad relevantes mediante su sistema de auditoría integrado. Este registro de actividades permite a los administradores realizar un seguimiento preciso de las acciones realizadas en la plataforma, facilitando la trazabilidad y el cumplimiento de políticas de seguridad.

66. Cada evento de auditoría contiene la siguiente información:

    - Marca de tiempo: indica la fecha y hora exacta en la que ocurrió el evento.
    - Información de usuario: identifica al usuario que generó el evento. En caso de no estar disponible, el sistema asocia el evento al usuario autenticado en ese momento.
    - Información adicional: incluye detalles específicos del evento, como el tipo de acción realizada, si tuvo éxito o fue denegada, y otros metadatos técnicos.

67. Los eventos de auditoría se almacenan en el índice interno _audit, que está accesible mediante búsquedas desde la interfaz web de Splunk Cloud. Los usuarios con permisos adecuados pueden consultar esta información aplicando filtros como tipo de evento, identidad del usuario, fecha, estado del evento (éxito o error), entre otros.

68. Para la comunicación entre el forwarder y Splunk Cloud, se utilizan canales cifrados mediante TLS 1.2 o superior, garantizando la integridad y confidencialidad de los datos durante la transmisión.

69. Además, es posible que el Fowarder envíe los eventos a Splunk Cloud y a una ubicación externa a la vez, configurando los mecanismos de forwarding de Splunk. Aunque Splunk Cloud solo dé soporte para el canal entre Forwarder y Splunk Cloud, se recomienda configurar el reenvío de registros de auditoría a un servidor externo para asegurar la conservación de los datos en caso de incidencias operativas.

6.12 BACKUP

70. Al tratarse de un servicio en la nube, las copias de seguridad son realizadas por el proveedor en su plataforma.

7 FASE DE OPERACIÓN

71. El correcto funcionamiento de Splunk Cloud Platform requiere que se cumplan una serie de condiciones en el entorno operacional:

    - Splunk Cloud Platform es una solución gestionada por Splunk, lo que garantiza que el producto reciba de forma automática las últimas actualizaciones de seguridad para protegerlo frente a amenazas y vulnerabilidades conocidas.
    - Los registros de auditoría se almacenan en el índice interno _audit. Estos registros son inmutables dentro del entorno gestionado de Splunk Cloud y solo son accesibles para usuarios autorizados mediante búsquedas controladas. Se recomienda configurar el reenvío de registros a una ubicación externa para reforzar la protección frente a modificaciones o eliminaciones no autorizadas.
    - La gestión de certificados en Splunk Cloud se realiza a través del soporte de Splunk o mediante la interfaz Admin Config Service (ACS) para ciertas operaciones. Es responsabilidad del cliente supervisar las fechas de expiración de certificados personalizados y solicitar su renovación a través del portal de soporte cuando sea necesario.
    - Splunk Cloud cuenta con mecanismos integrados de resiliencia y replicación de datos. No obstante, se recomienda configurar exportaciones periódicas o reenvío de datos clave a almacenamiento externo, como Amazon S3, si se requiere una política de retención adicional controlada por el cliente.

72. Splunk Cloud proporciona varias herramientas para supervisar el estado y rendimiento de la plataforma durante su operación:

    - Cloud Monitoring Console (CMC): Es la herramienta principal para la supervisión en Splunk Cloud. Ofrece una interfaz basada en paneles con visualizaciones preconfiguradas sobre el uso de recursos, rendimiento de búsquedas, estado de ingesta de datos, uso de licencias y otros indicadores clave. Está diseñada para brindar visibilidad operativa tanto a implementaciones simples como a despliegues complejos en la nube. Mas información en la guía **Cloud Monitoring Console** [REF10].
    - Supervisión de estado del sistema (Health Report): Aunque en Splunk Cloud no se accede directamente al endpoint /server/health/splunkd, se dispone de reportes de estado de servicios clave a través de la consola de monitorización o mediante solicitudes al soporte técnico. Las revisiones de estado permiten detectar anomalías en la ingesta de datos, disponibilidad del servicio o latencia en las búsquedas. Splunk también puede habilitar alertas sobre eventos críticos del sistema en el entorno gestionado.

8 REFERENCIAS

[REF1] Splunk Cloud Platform
https://www.splunk.com/en_us/products/splunk-cloud-platform.html

[REF2] Platform Pricing
https://www.splunk.com/en_us/products/pricing/platform-pricing.html

[REF3] Admin manual
https://help.splunk.com/en/splunk-cloud-platform/administer/admin-manual/9.3.2411/get-started-managing-splunk-cloud-platform/welcome-to-the-splunk-cloud-platform-admin-manual

[REF4] Get AWS data into Splunk Cloud Platform
https://help.splunk.com/en/splunk-cloud-platform/administer/admin-manual/9.3.2411/get-data-into-splunk-cloud-platform/get-amazon-web-services-aws-data-into-splunk-cloud-platform

[REF5] Splunk Cloud Platform deployment
https://lantern.splunk.com/Splunk_Platform/Getting_Started/Managing_your_Splunk_Cloud_Platform_deployment

[REF6] Splunk Cloud Documentation
https://help.splunk.com/en/splunk-cloud-platform/release-notes/9.3.2411/splunk-cloud-platform-release-notes/welcome-to-splunk-cloud-platform

[REF7] Integrate an Identity Provider
https://docs.splunk.com/Documentation/SCS/latest/Admin/IntegrateIdP

[REF8] Define roles on the Splunk platform with capabilities
https://help.splunk.com/en/splunk-cloud-platform/administer/manage-users-and-security/9.3.2408/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities

[REF9] Guía de seguridad de las TIC CCN-STIC 887G
https://www.ccn-cert.cni.es/es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/6882-ccn-stic-887g-guia-de-configuracion-segura-para-monitorizacion-y-gestion-aws/file?format=html

[REF10] Cloud Monitoring Console
https://help.splunk.com/en/splunk-cloud-platform/release-notes/9.3.2411/splunk-cloud-platform-release-notes/cloud-monitoring-console

[REF11] Use forwarders to get data into Splunk Cloud Platform
https://docs.splunk.com/Documentation/SplunkCloud/latest/Data/UsingforwardingagentsCloud?

[REF12] Deploy heavy and light forwarders
https://help.splunk.com/en/splunk-cloud-platform/forward-and-process-data/forwarding-and-receiving-data/9.3.2411/deploy-heavy-and-light-forwarders/enable-forwarding-on-a-splunk-enterprise-instance

[REF13] Change a user password
https://help.splunk.com/en/splunk-cloud-platform/administer/manage-users-and-security/9.3.2408/manage-credentials-and-keys/change-a-user-password

[REF14] Configure user session timeouts
https://docs.splunk.com/Documentation/Splunk/9.4.2/Admin/Configureusertimeouts

[REF15] Securing the Splunk platform with TLS
https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Securing_the_Splunk_platform_with_TLS

[REF16] Enable forwarding on a Splunk Enterprise instance
https://help.splunk.com/en/splunk-cloud-platform/forward-and-process-data/forwarding-and-receiving-data/9.3.2411/deploy-heavy-and-light-forwarders/enable-forwarding-on-a-splunk-enterprise-instance

[REF17] Splunk Cloud Account
https://login.splunk.com/

[REF18] Splunk Cloud Universal Forwarder
https://www.splunk.com/en_us/download/universal-forwarder.html

[REF19] Splunk Pricing Options
https://www.splunk.com/en_us/resources/splunk-pricing-options.html

9 ABREVIATURAS

ACS	Admin Config Service
AD	Active Directory
API	Application Programming Interface
AWS	Amazon Web Services
CLI	Command Line Interface
CloudTrail	Amazon CloudTrail
CloudWatch	Amazon CloudWatch
CMC	Cloud Monitoring Console
CPSTIC	Catálogo de Productos y Servicios TIC
CPU	Central Processing Unit
CRL	Certificate Revocation List
CSP	Cloud Service Provider
EBS	Elastic Block Store
EC2	Elastic Compute Cloud
ECDSA	Elliptic Curve Digital Signature Algorithm
ELB	Elastic Load Balancing
ENS	Esquema Nacional de Seguridad.
FIFO	First In, First Out
FTP	File Transfer Protoco
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
IdP	Identity provider
IKE	Internet Key Exchange
IoMT	Internet of Medical Things
IoT	Internet of Things
IT	Information Technology
KMS	Key Management Service
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Factor Authentication
NTP	Network Time Protocol
OT	Operational Technology
PAM	Privileged Access Manager
RBAC	Role-Based Access Control

RSS	Really Simple Syndication
S3	Simple Storage Service
SAML	Security Assertions Markup Language
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SPL	Search Processing Language
SSH	Secure Shell
SSO	Single Sign On
STIC	Servicio de Tecnologías de la Información y Telecomunicaciones
SVC	Splunk Virtual Compute
TLS	Transport Layer Security
URL	Uniform Resource Locator
VPC	Virtual Private Cloud
WAF	Web Application Firewall
WMI	Windows Management Instrumentation
XSRF	Cross-Site Request Forgery
XSS	Cross-Site Scripting