Splunk Core Certified Power User

Descrición

Este curso está deseñado para usuarios que son novos en Splunk e queren converterse en expertos nos seguintes temas de Splunk:

Usuarios avanzados que queren dominar o uso do tempo nas buscas. Os temas centraranse na busca e formato de tempo, así como no uso de comandos de tempo e no traballo con fusos horarios.

Procesamento estatístico: para identificar e usar comandos de transformación e funcións eval para calcular estatísticas sobre datos. Os temas abarcarán os tipos de series de datos, os principais comandos de transformación, as funcións de avaliación matemáticas e estatísticas, o uso de eval como función e os comandos de renomeamento e ordenamento.

Comparación de valores: aprenderás a comparar valores de campo usando funcións e expresións eval. Os temas centraranse no uso das funcións de comparación e condicionais do comando eval, así como no uso de expresións eval cos comandos de formato de campo e where.

Modificación de resultados: os comandos usaranse para manipular a saída e normalizar os datos. Os temas centraranse en comandos específicos para manipular campos e os seus valores, modificar conxuntos de resultados e xestionar datos que faltan. Ademais, abordarán o uso de funcións específicas do comando `eval` para normalizar campos e os seus valores en múltiples fontes de datos.

Análise de correlación: aprende a calcular a co-ocurrencia entre campos e analizar datos de múltiples conxuntos de datos. Os temas centraranse nos comandos `transaction`, `append`, `appendcols`, `union` e `join`.

Creación de obxectos de coñecemento: crea obxectos de coñecemento para o teu entorno de busca usando a interface web de Splunk. Os temas abordarán os tipos de obxectos de coñecemento, a secuencia de operacións en tempo de busca e os procesos para crear tipos de eventos, accións de fluxo de traballo, etiquetas, alias, macros de busca e campos calculados.

Creación de extractos de campo: aprende sobre a extracción de campos e a utilidade Field Extractor (FX). Os temas abordarán cando se extraen certos campos e como usar FX para crear extractos de campo usando expresións regulares e delimitadas.

Modelos de datos: aprende a crear e optimizar modelos de datos. Os temas abordarán conxuntos de datos, deseño de modelos de datos, uso do editor de táboas dinámicas e optimización de modelos de datos.

Obxectivos

Ao finalizar este curso, o alumnado poderá:

- Dominar SPL a nivel de usuario avanzado
- Crear buscas máis complexas e eficientes
- Usar comandos como stats, eval, case, timechart, chart, eventstats, lookup, etc.
- Manipular e enriquecer datos
- Crear e modificar campos
- Normalizar e transformar información
- Enriquecer eventos mediante buscas e táboas externas
- Realizar análises de datos avanzadas
- Obter métricas, tendencias e correlacións
- Traballar con datos e comparacións baseadas no tempo
- Resolver casos de uso reais de negocios, TI ou seguridade
- Crear informes e paneis eficaces
- Deseñar visualizacións claras e útiles
- Crear paneis interactivos
- Compartir resultados con outros usuarios de Splunk
- Optimizar buscas
- Mellorar o rendemento das consultas
- Aplicar as mellores prácticas de SPL
- Reducir o consumo de recursos innecesarios
- Prepararse para a certificación e completar con éxito o contido clave do exame.

Dirixido a

Usuarios iniciais de Splunk e analistas de datos, analistas de seguridade ou operacións (SOC, operacións de TI)

BENEFICIOS

Opción gratuita dun exame de certificación oficial

Diploma de asistencia

Perfil do docente

Docente coas seguintes competencias:

- Coñecementos avanzados de Splunk Enterprise
- Uso experto de SPL (Linguaxe de procesamento de buscas)
- Creación de buscas, informes e paneis complexos
- Dominio de comandos avanzados (stats, eval, lookup, eventstats, timechart, etc.)
- Coñecemento do ecosistema Splunk

- Aplicacións comúns (ITSI, ES a nivel de usuario, aplicacións de provedores)
- Mellores prácticas para a análise e optimización de buscas
- Casos de uso do mundo real (Operacións de TI, Seguridade, Analítica empresarial)
- Experiencia probada con proxectos de produción de Splunk
- Coñecemento de casos de uso empresariais
- Capacidade para explicar como aplicar Splunk en entornos do mundo real, non só teoría

PROGRAMA	Programación 2026/27
TIPO	CURSO
MATRÍCULA	Gratuíta
PERIODO INSCRICIÓN	15/06/2026 - 31/08/2026
PROBA DE SELECCIÓN	03/09/2026 (17:30)
CRITERIOS DE SELECCIÓN	Proba técnica presencial no CNTG en Santiago de Compostela
Nº PRAZAS	12 (Mínimo 10)
METODOLOXÍA	Virtual + teleformación
TIPO DE EDICIÓN	Edición única tarde (desempregados/as e ocupados/as)
DURACIÓN	32 horas (25h virtuais, 7h teleformación)
DATA INICIO	12/10/2026
DATA FIN	23/10/2026
HORARIO	Virtual: 19 a 23 de outubro de 16:00 a 21:00 horas.
LUGAR DE DOCENCIA	Edificio localizado na r/Airas Nunes s/n, barrio de Conxo, en
CERTIFICACIÓN OFICIAL	Sí

EXAME CERTIFICACIÓN Splunk Core Certified Power User

MÓDULOS TRANSVERSAIS Igualdade de 5 horas

TECNOLOXÍA Splunk

Ciberseguridade/Ciberseguridad

PERIODO DOCENCIA 12/10/2026 - 23/10/2026

Temario

TEMARIO CURSO VIRTUAL (25 HORAS)

Traballando co tempo:
Módulo 1 - Busca con tempo
Módulo 2 - Formato de tempo
Módulo 3 - Uso de comandos de tempo
Módulo 4 - Traballando con fusos horarios

Procesamento estatístico:
Módulo 1 - Que é unha serie de datos?
Módulo 2 - Transformación de datos
Módulo 3 - Manipulación de datos co comando eval
Módulo 4 - Formato de datos

Comparación de valores:
Módulo 1 - Uso de eval para a comparación
Módulo 2 - Filtrado con WHERE

Modificación do resultado:
Módulo 1 - Manipulación da saída
Módulo 2 - Modificación de conxuntos de resultados
Módulo 3 - Xestión de datos faltantes
Módulo 4 - Modificación de valores de campo
Módulo 5 - Normalización con eval

Análise de correlación:
Módulo 1 - Cálculo da co-ocurrencia entre campos
Módulo 2 - Análise de varias fontes de datos

Creación de obxectos de coñecemento:
Tema 1 - Obxectos de coñecemento e operacións en tempo de busca
Tema 2 - Creación de tipos de eventos
Tema 3 - Creación de accións de fluxo de traballo
Tema 4 - Creación de etiquetas e alias
Tema 5 - Creación de macros de busca
Tema 6 - Creación de campos calculados

Creación de extractos de campo:
Módulo 1 - Usando o extractor de campos
Módulo 2 - Creando extractos de campos usando expresións regulares 3 - Creando extractos de campos delimitados

Modelos de datos
Módulo 1 - Introdución aos conxuntos de datos de modelos de datos
Módulo 2 - Deseño de modelos de datos
Módulo 3 - Creando unha táboa dinámica
Módulo 4 - Acelerando modelos de datos

TEMARIO TELEFORMACIÓN (7 HORAS)

- WHAT IS SPLUNK (SSC)
- INTRO TO SPLUNK (SSC)
- USING FIELDS (SSC)
- VISUALIZATIONS (SSC)
- INTRO TO KNOWLEDGE OBJECTS (SSC)
- SEARCH UNDER THE HOOD (SSC)