

Splunk Enterprise Administration Fast Start

5 jours (35 heures)

Perfectionnement

Classe à distance

à partir de

4 000 € HT par personne (TVA en vigueur)

Contenu mis à jour le 25/09/2026. Document téléchargé le 02/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Décrire l'administration système
- Définir le déploiement Splunk
- Décrire la gestion des licences
- Identifier les applications Splunk
- Préparer les fichiers de configuration Splunk
- Déterminer les utilisateurs, rôles et mécanismes d'authentification
- Ingérer des données dans Splunk (Get Data In)
- Définir la recherche distribuée (Distributed Search)
- Décrire l'administration des données
- Expliquer les sourcetypes
- Mettre en oeuvre et déployer des forwarders
- Configurer les entrées de données (data inputs)
- Définir les file monitors
- Expliquer les entrées réseau (TCP/UDP), les entrées scriptées et les entrées HTTP (via le HTTP Event Collector)
- Personnaliser le processus de parsing lors de la phase d'ingestion
- Définir des transformations pour modifier les données avant indexation
- Décrire les configurations des knowledge objects au moment de la recherche.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Administrateurs systèmes et administrateurs en charge de la gestion d'un environnement Splunk Enterprise.

Prérequis

Avoir suivi la formation SPLUNK-POWERU "Splunk Power User Fast Start".

Programme

1 Pendant votre formation

Splunk Enterprise Administration Fast Start

Splunk Enterprise System Administration

Déploiement du serveur Splunk

- Présenter une vue d'ensemble de Splunk
- Identifier les composants de Splunk Enterprise
- Identifier les types de déploiement Splunk
- Lister les étapes d'installation de Splunk
- Utiliser les commandes CLI de Splunk

Splunk Server Monitoring

- Activer la Monitoring Console (MC)
- Identifier les types de licences Splunk
- Comprendre les violations de licence
- Ajouter et supprimer des licences
- Utiliser Splunk Diag

Applications Splunk

- Décrire les apps et add-ons Splunk
- Installer une application sur une instance Splunk
- Gérer l'accessibilité et les permissions des applications

Fichiers de configuration Splunk

- Décrire la structure des répertoires de configuration
- Comprendre le mécanisme de superposition des configurations (configuration layering)
- Utiliser btool pour analyser les paramètres de configuration

Splunk Indexes

- Comprendre le fonctionnement des index Splunk
- Identifier les types de index buckets
- Créer et manipuler des index
- Vue d'ensemble des metrics index

Gestion des index Splunk

- Revoir les fondamentaux de la gestion des index
- Identifier les bonnes pratiques de rétention des données
- Identifier les recommandations de sauvegarde
- Déplacer et supprimer des données d'index
- Comprendre l'utilisation du Fishbucket
- Restaurer un frozen bucket

Gestion des utilisateurs Splunk

- Ajouter des utilisateurs via l'authentification native
- Comprendre les rôles utilisateurs dans Splunk
- Créer un rôle personnalisé
- Gérer les utilisateurs

Configuration du forwarding de base

- Identifier les étapes de configuration des forwarders
- Configurer un Universal Forwarder
- Comprendre le Deployment Server

Recherche distribuée

- Comprendre le fonctionnement de la recherche distribuée
- Définir les rôles du search head et des search peers

Splunk Enterprise Data Administration

Introduction à l'administration des données

- Présenter une vue d'ensemble de Splunk
- Décrire les quatre phases du modèle distribué
- Décrire les types d'entrées de données et les paramètres de métadonnées
- Configurer des tests d'ingestion initiaux via Splunk Web
- Tester les index avec l'Input Staging

Ingestion des données – Staging

- Identifier les fichiers et répertoires de configuration Splunk
- Comprendre la priorité entre index-time et search-time
- Valider et mettre à jour les fichiers de configuration

Configuration des forwarders

- Identifier le rôle des indexers de production et des forwarders
- Comprendre et configurer les Universal Forwarders
- Comprendre et configurer les Heavy Forwarders
- Comprendre et configurer les forwarders intermédiaires
- Identifier les options supplémentaires des forwarders

Gestion des forwarders

- Comprendre le Splunk Deployment Server (DS)
- Gérer les forwarders via des deployment apps
- Configurer les clients de déploiement et les groupes de clients
- Superviser les activités de gestion des forwarders

Entrées de type Monitor

- Créer des entrées de surveillance de fichiers et répertoires
- Utiliser les paramètres optionnels des monitor inputs
- Déployer un monitor input distant

Entrées réseau et scriptées

- Créer des entrées réseau (TCP et UDP)
- Décrire les options avancées des entrées réseau

Entrées sans agent (Agentless)

- Créer une entrée scriptée simple

Optimisation des entrées

- Configurer le HTTP Event Collector (HEC) pour des entrées sans agent
- Présenter le Splunk App for Stream

Phase de parsing et données

- Identifier les entrées spécifiques Linux
- Identifier les entrées spécifiques Windows

Manipulation des données brutes

- Comprendre le traitement par défaut lors de la phase d'ingestion
- Configurer les options de parsing (sourcetype, encodage des caractères...)

Knowledge Objects associés

- Comprendre le traitement par défaut lors du parsing
- Optimiser et configurer le découpage des événements (line breaking)
- Comprendre l'extraction et l'affectation des timestamps et fuseaux horaires
- Utiliser Data Preview pour valider la création des événements

Création d'un Diag

- Comprendre la définition et l'utilisation des transformations de données
- Utiliser les transformations via props.conf et transforms.conf pour :
 - Masquer ou supprimer des données lors de l'indexation
 - Redéfinir le sourcetype ou le host selon le contenu des événements
 - Router les événements vers des index spécifiques
 - Empêcher l'indexation d'événements non souhaités
- Utiliser SEDCMD pour modifier les données brutes

Knowledge Objects associés

- Définir les extractions de champs par défaut et personnalisées (search time)
- Identifier les avantages et inconvénients des extractions au moment de l'indexation
- Configurer les extractions de champs indexés
- Comprendre les extractions par défaut au moment de la recherche
- Gérer les knowledge objects orphelins

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)

- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Accessibilité aux personnes en situation de handicap

Sessions

À distance

Du 5 octobre 2026 au 9 octobre 2026