

SQL Server 2022 / 2025 – Administration avancée et durcissement

2 jours (14 heures)

Expertise

Présentiel ou classe à distance

à partir de

1 470 € HT par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 01/10/2026.

Objectifs

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

- Identifier les principaux risques de sécurité liés à l'exploitation d'une instance SQL Server
- Appliquer une démarche de durcissement adaptée à SQL Server 2022 / 2025
- Renforcer l'authentification, les droits d'accès et la séparation des privilèges
- Sécuriser les communications, les données sensibles et les sauvegardes
- Mettre en place l'audit, la classification et la détection des vulnérabilités
- Intégrer SQL Server dans une démarche de supervision de sécurité avec Azure Arc et Microsoft Defender for Cloud.

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

À qui s'adresse cette formation ?

Administrateurs SQL Server, DBA, administrateurs systèmes, ingénieurs infrastructure et professionnels IT ayant déjà une expérience de l'administration SQL Server et souhaitant renforcer la sécurité, la gouvernance et l'exploitation avancée d'instances SQL Server 2022 / 2025.

Prérequis

Avoir une bonne connaissance de l'administration SQL Server. Avoir déjà manipulé les notions d'instances, de bases, de connexions, de rôles, de sauvegardes et de restauration. Avoir suivi la formation SQL22-ADM "SQL Server 2022/2025 – Conception administration et durcissement".

Programme

1 Pendant votre formation

SQL Server 2022 / 2025 – Administration avancée et durcissement

Jour 1 – Durcir l'instance SQL Server

- Revoir les risques liés à l'exploitation SQL Server
- Identifier les surfaces d'attaque d'une instance SQL Server
- Distinguer sécurité système, sécurité réseau, sécurité instance et sécurité base
- Comprendre les principes de défense en profondeur
- Identifier les risques liés aux comptes de service, comptes SQL, rôles élevés et accès d'administration

Réduire la surface d'exposition

- Revoir les fonctionnalités activées et les composants réellement nécessaires
- Sécuriser les accès réseau à l'instance SQL Server
- Contrôler les protocoles, ports et accès distants
- Limiter les usages à risque et les fonctionnalités non indispensables
- Intégrer le durcissement SQL Server dans une politique système et infrastructure

Renforcer l'authentification et les privilèges

- Choisir les modes d'authentification adaptés
- Privilégier Windows Authentication ou Microsoft Entra lorsque le contexte le permet
- Gérer les rôles serveur, rôles base et permissions avancées
- Appliquer le principe du moindre privilège
- Séparer les rôles DBA, exploitation, sécurité et administration système
- Sécuriser les comptes de service, notamment avec les comptes gMSA

Sécuriser les communications et les données sensibles

- Comprendre les enjeux de chiffrement des connexions SQL Server
- Mettre en perspective Force Encryption, Strict Encryption, certificats et chaînes de connexion
- Intégrer les apports de SQL Server 2022 et SQL Server 2025 sur le chiffrement des communications

- Identifier les impacts des pilotes récents, de TLS 1.3 et de TDS 8.0
- Identifier et classer les données sensibles
- Présenter les usages de Dynamic Data Masking, Always Encrypted et Row-Level Security
- Comprendre l'intérêt de TDE pour les fichiers, sauvegardes et tempdb
- Gérer le cycle de vie des certificats, clés de chiffrement et secrets associés
- Introduire Azure Key Vault dans les scénarios de protection des clés

Jour 2 – Gouverner, auditer et sécuriser les environnements avancés

Auditer et tracer les activités sensibles

- Mettre en place une stratégie d'audit SQL Server
- Identifier les événements sensibles à tracer
- Auditer les accès privilégiés, les changements de configuration et les opérations critiques
- Introduire les principes de réponse à incident et d'investigation SQL Server

Évaluer les vulnérabilités et la conformité

- Réaliser une revue de configuration de sécurité
- Identifier les écarts de configuration
- Exploiter les évaluations de vulnérabilité
- Prioriser les corrections selon le risque
- Documenter un plan de remédiation
- Utiliser Policy-Based Management pour contrôler les configurations sensibles
- Définir des standards de conformité SQL Server applicables à plusieurs instances

Sécuriser les sauvegardes et la reprise

- Revoir les risques liés aux sauvegardes non protégées
- Protéger les sauvegardes par chiffrement
- Tester les restaurations dans une logique de maîtrise du risque
- Prévoir la protection contre les suppressions ou altérations malveillantes
- Présenter les sauvegardes vers stockage immuable et les identités managées lorsque le contexte le permet

Introduction à SQL Server dans un contexte hybride

- Comprendre les apports de SQL Server activé par Azure Arc
- Positionner Microsoft Defender for Cloud pour SQL Server
- Identifier les prérequis et limites de l'intégration
- Exploiter les recommandations, alertes et évaluations de sécurité
- Relier les pratiques de durcissement local aux outils de sécurité cloud
- Inventorier et gouverner les instances SQL Server à l'échelle avec Azure Arc
- Exécuter des contrôles de conformité ou scripts ciblés sur des instances connectées

Intégrer les nouveautés SQL Server 2022 / 2025 utiles au durcissement

- Identifier les nouveautés SQL Server 2025 ayant un impact sécurité

- Comprendre PBKDF2 pour les hachages de mots de passe SQL
- Présenter TLS 1.3 avec TDS 8.0
- Présenter les identités managées avec Microsoft Entra et Azure Key Vault
- Mesurer les impacts d'exploitation liés aux pilotes, connexions, serveurs liés et réplication
- Distinguer les nouveautés utiles au durcissement de celles relevant du développement ou du tuning
- Prendre en compte les impacts de sécurité dans les architectures distribuées et haute disponibilité

Exemples de travaux pratiques (à titre indicatif)

- Réaliser une revue de configuration de sécurité d'une instance SQL Server
- Identifier les comptes, rôles et permissions à risque
- Configurer une stratégie d'audit ciblée
- Classifier des données sensibles et tester les protections disponibles
- Analyser des recommandations de sécurité issues d'un outil d'évaluation
- Construire une checklist de durcissement SQL Server 2022 / 2025
- Définir une politique de conformité simple avec Policy-Based Management
- Formaliser un mini-plan de réponse à incident SQL Server

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

Détails de la session

Du 1 octobre 2026 au 2 octobre 2026 (2 jours / 14 heures)

À distance

Du 1 octobre 2026 au 2 octobre 2026

À distance

- 1 octobre 2026 9h00 – 17h00
- 2 octobre 2026 9h00 – 17h00