

Mis à jour le 27/10/2026

S'inscrire

Formation Cohesity

2 jours (14 heures)

Présentation

Cohesity DataProtect est une solution de protection des données permettant de sauvegarder et de restaurer les environnements physiques, virtuels, applicatifs et NAS. Avec les Protection Groups, les politiques de rétention et les mécanismes de restauration, Cohesity permet de centraliser les opérations de sauvegarde et de renforcer la résilience des infrastructures.

Notre formation Cohesity vous permettra de maîtriser les opérations essentielles de sauvegarde et de restauration pour exploiter une infrastructure de protection des données au quotidien.

Vous apprendrez à comprendre l'architecture, à enregistrer les sources avec des agents ou des API et à configurer des politiques adaptées aux exigences métier. Vous organiserez la protection des serveurs, des machines virtuelles, des applications et des partages NAS.

À l'issue de la formation, vous serez en mesure de rechercher des points de restauration, de récupérer des fichiers et volumes et de réaliser une restauration instantanée sur les plateformes compatibles. Vous saurez également ajuster les groupes et piloter leurs exécutions.

Cette formation aborde également les tableaux de bord, les alertes, les rapports et les journaux pour diagnostiquer les incidents. Les fonctionnalités DataLock et de rétention étendue complètent les ateliers pour renforcer la sécurité et fiabiliser vos pratiques d'exploitation.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Décrire l'architecture et les composants de Cohesity DataProtect pour les environnements physiques, virtuels, applicatifs et NAS

- Enregistrer et configurer les sources de protection avec des agents et des API selon les plateformes
- Créer et optimiser les Protection Groups et les Protection Policies selon les exigences de sauvegarde, de rétention et de conformité
- Exécuter les sauvegardes et les restaurations de fichiers, de volumes et de machines virtuelles sur les plateformes compatibles
- Superviser les opérations, diagnostiquer les échecs et piloter les exécutions de protection et de restauration
- Configurer les mécanismes DataLock et de rétention étendue selon les exigences de sécurité

Public visé

- Administrateur sauvegarde
- Administrateur système
- Administrateur virtualisation
- Ingénieur infrastructure
- Technicien d'exploitation informatique

Pré-requis

- Expérience de l'administration de Windows Server et de Linux
- Connaissance d'un environnement de virtualisation tel que VMware vSphere ou Microsoft Hyper-V
- Maîtrise des principes de sauvegarde, de rétention et des objectifs de perte de données et de délai de reprise
- Connaissances des réseaux, des droits d'accès et des partages SMB et NFS

Pré-requis techniques

- Poste de travail avec processeur quatre cœurs et 8 Go de mémoire vive minimum pour accéder au laboratoire distant
- Navigateur Google Chrome ou Mozilla Firefox dans une version maintenue compatible avec la console du laboratoire
- Connexion Internet stable autorisant l'accès sécurisé à la console et aux outils du laboratoire distant
- Compte nominatif avec les droits nécessaires aux exercices sur un environnement Cohesity DataProtect isolé de la production
- Laboratoire distant préparé avec des serveurs Windows Server et Linux, des hyperviseurs compatibles, une application et des partages NAS de test

Programme de notre formation Cohesity

[Jour 1 - Matin]

Architecture et préparation des sources

- Architecture de Cohesity DataProtect : cluster, nœuds, stockage distribué, console d'administration et composants de protection
- Couverture des environnements physiques, virtuels, applicatifs et NAS : flux de données et responsabilités des composants
- Préparation des sources : compatibilité, connectivité réseau, résolution de noms, comptes de service et droits minimaux
- Installation et configuration du Cohesity Agent pour les serveurs physiques Windows et Linux et les applications concernées
- Enregistrement des hyperviseurs VMware, Hyper-V, Nutanix AHV et RHV par leurs interfaces de gestion, distinction des accès NAS génériques et des intégrations par API
- Atelier pratique : explorer le cluster, enregistrer un serveur physique avec agent, une source virtuelle par son interface de gestion et un partage NAS, puis vérifier la découverte des objets.

[Jour 1 - Après-midi]

Politiques et exécution des sauvegardes

- Création et modification des Protection Groups : sélection des objets, règles d'inclusion et d'exclusion, organisation par criticité
- Configuration des Protection Policies : planification, rétention, objectifs de perte de données, fenêtres de sauvegarde et maîtrise de la capacité
- Mise en œuvre de DataLock et de la rétention étendue : durée de verrouillage, droits dédiés, exigences de conformité et conséquences des modifications
- Exécution des sauvegardes des serveurs Windows et Linux, des machines VMware, Hyper-V, Nutanix AHV et RHV, des applications et des sources NAS, selon leurs spécificités de cohérence et de compatibilité
- Pilotage des exécutions avec Run Now : choix des objets, pause des prochaines exécutions, reprise, annulation et nouvelle tentative selon les actions disponibles
- Atelier pratique : créer des groupes et une politique, configurer une rétention étendue et DataLock sur des données de test, puis lancer et contrôler des sauvegardes à la demande.

[Jour 2 - Matin]

Recherche et restauration des données

- Utilisation de la recherche et des filtres pour retrouver les objets protégés, les exécutions et les points de restauration
- Choix du point de restauration, de la destination et des options de récupération : droits, écrasement et contrôle des dépendances
- Restauration de fichiers et de volumes pour les serveurs physiques Windows et Linux selon les fonctionnalités prises en charge
- Restauration des machines VMware, Hyper-V, Nutanix AHV et RHV, avec restauration instantanée lorsque la plateforme et la version le permettent
- Récupération des applications et des données NAS : cohérence, permissions et validation fonctionnelle après restauration
- Atelier pratique : rechercher un point de restauration, récupérer un fichier et un volume compatibles, démarrer une machine virtuelle par restauration instantanée et vérifier les données applicatives ou NAS restaurées.

[Jour 2 - Après-midi]

Supervision et exploitation quotidienne

- Lecture des tableaux de bord : couverture de protection, états des tâches, capacité, durées et respect des objectifs de sauvegarde
- Exploitation des alertes, des rapports et des journaux pour identifier les incidents et documenter leur résolution
- Diagnostic des échecs : agents, authentification, connectivité, instantanés, accès NAS et ressources des destinations de restauration
- Gestion du cycle des tâches : distinction entre pause et reprise de la protection, annulation d'une exécution et nouvelle tentative selon les possibilités du type de tâche, puis utilisation de Resubmit pour resoumettre une restauration échouée
- Bonnes pratiques opérateur : contrôle quotidien des échecs, ajustement des groupes et politiques, suivi des rétentions verrouillées et validation régulière des restaurations
- Atelier pratique : diagnostiquer un échec simulé avec les alertes et journaux, corriger sa cause, relancer une sauvegarde, resoumettre une restauration et produire une synthèse d'exploitation.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.