DAWAN

Plan de la formation

www.dawan.fr

Formation Veeam Backup & Replication 13

Durée :	3 jours (21 heures)
Tarif inter-entreprises :	2 275,00 € HT (Présentiel) 1 820,00 € HT (Distanciel)
Public :	Administrateurs systèmes et réseaux, administrateurs VMware vSphere ou Hyper-V, ingénieurs infrastructures et responsables de sauvegarde.
Pré-requis :	Connaissances de l'administration de Windows Server ou Linux - Connaissances de VMware vSphere et/ou Hyper-V - Notions de réseau et de stockage.
Objectifs :	Déployer Veeam Backup & Replication 13 et utiliser ses interfaces d'administration - Configurer les sauvegardes, les copies et les dépôts immuables - Restaurer les données et préparer la reprise d'activité - Renforcer la sécurité et superviser l'environnement.
Méthode pédagogique :	Alternance d'apports théoriques, de démonstrations et d'ateliers pratiques sur un environnement de formation - Mises en situation de sauvegarde et de restauration - Vérification des acquis au fil des exercices.
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.

Modalité d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	RéS103186-F
Note de satisfaction des participants :	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Définir une stratégie de cyberrésilience avec Veeam 13

Identifier les composants de Veeam Backup & Replication 13 et leurs rôles
Définir les objectifs RPO et RTO, les priorités métier et les scénarios d’incident
Appliquer la règle 3-2-1-1-0 et organiser les copies isolées ou immuables
Comparer les modes de déploiement, les éditions et les contraintes de licence
Repérer les évolutions de la branche 13.x utiles à son infrastructure

Atelier pratique : concevoir une architecture de protection et un scénario de reprise

Déployer le serveur et les interfaces d’administration

Vérifier les prérequis système, les flux réseau et les compatibilités
Comparer le déploiement Windows et Veeam Software Appliance sous Linux
Installer le serveur de sauvegarde selon le scénario retenu
Prendre en main la console et l’interface Web, leurs fonctions et leurs limites
Configurer les accès, les notifications et la sauvegarde de configuration

Préparer une évolution de version et vérifier les conditions de migration de plateforme

Atelier pratique : déployer Veeam 13 et réaliser les premiers contrôles depuis les interfaces d'administration

Configurer une infrastructure de sauvegarde hybride

Ajouter les serveurs de virtualisation et organiser les composants de traitement
Configurer les proxies et choisir les modes de transport
Déployer les dépôts de sauvegarde et découvrir Veeam Infrastructure Appliance
Configurer un dépôt Linux renforcé et les règles d'immutabilité
Intégrer un stockage objet local ou cloud et organiser un Scale-Out Backup Repository
Dimensionner les dépôts, les flux réseau et les tâches concurrentes

Atelier pratique : connecter l'infrastructure virtuelle et configurer les cibles de sauvegarde

Protéger les machines et les données

Créer et planifier des tâches de sauvegarde de machines virtuelles
Définir les méthodes de sauvegarde, le traitement applicatif et les règles de rétention
Configurer les copies de sauvegarde et le chiffrement
Organiser la protection des serveurs Windows et Linux avec les agents
Identifier les possibilités de protection des partages NAS et du stockage objet
Situer la prise en charge des autres hyperviseurs et des charges cloud selon la version et les composants déployés

Atelier pratique : mettre en œuvre une politique de sauvegarde et contrôler les copies et points de restauration

Restaurer et vérifier les données protégées

Restaurer une machine complète, des disques et des fichiers
Utiliser Instant Recovery et les restaurations granulaires applicatives
Choisir un point de restauration et contrôler son état de sécurité
Tester les sauvegardes dans un environnement isolé avec SureBackup
Identifier les possibilités de restauration vers le cloud et leurs prérequis
Vérifier les données restaurées et documenter les résultats

Atelier pratique : restaurer une machine et des données puis tester la reprise d'un service

Mettre en œuvre la réplication et la reprise d’activité

Configurer une tâche de réplication et les correspondances réseau
Préparer une bascule et un retour en production
Distinguer réplication, CDP VMware et Universal CDP selon la version 13.x et les plateformes prises en charge
Organiser l’ordre de reprise des services et leurs dépendances
Mesurer les RPO et RTO obtenus pendant un test

Atelier pratique : exécuter un scénario de bascule et de retour en production

Renforcer la sécurité de l’infrastructure

Organiser la séparation des rôles et le contrôle d’accès RBAC
Configurer l’authentification multifacteur et identifier les possibilités de SSO
Protéger les identifiants, les certificats et les clés de chiffrement
Contrôler la configuration avec Security & Compliance Analyzer
Exploiter les fonctions de détection de logiciels malveillants et de restauration sécurisée disponibles
Définir une procédure de traitement des alertes et de récupération après incident

Atelier pratique : vérifier les droits, analyser les paramètres de sécurité et préparer une restauration contrôlée

Superviser, maintenir et dépanner Veeam 13

Analyser les tableaux de bord, les résultats des tâches et les journaux
Surveiller la capacité et identifier les limites de performance
Organiser les mises à jour du logiciel et des appliances
Sauvegarder et restaurer la configuration du serveur
Présenter les possibilités d’Enterprise Manager, de Veeam ONE et d’automatisation
Formaliser les contrôles d’exploitation et les tests périodiques

Atelier pratique : diagnostiquer un incident et construire une procédure d’exploitation de l’environnement