

veeam

Votre parcours vers la protection avec Veeam Data Cloud

Parcours d'intégration client





La prise en main de **Veeam Data Cloud** doit être claire, pas compliquée. Ce guide oriente les professionnels de l'IT, les architectes cloud et les ingénieurs cloud depuis la configuration jusqu'à la protection validée et la préparation opérationnelle. Il est conçu pour les équipes qui gèrent la configuration, la protection et la restauration, tout en offrant aux responsables informatiques une visibilité sur la progression et la réduction des risques.

À la fin de votre processus d'intégration, vous disposerez de la résilience des données qu'exige votre organisation pour assurer la continuité de votre activité, le tout étant réuni sous une plateforme SaaS intuitive et puissante.

PHASE 1 Foundation	PHASE 2 Être protégé	PHASE 3 Validation et passage à l'échelle
M1 : Obtenir l'accès	M4 : Réussir votre première sauvegarde	M8 : Valider votre protection
M2 : Établir la responsabilité	M5 : Vérifier les paramètres de sauvegarde et de rétention	M9 : Étendre votre couverture
M3 : Connecter votre premier workload	M6 : Développer des habitudes de supervision de base	M10 : Introduire progressivement des fonctionnalités avancées

Feuille de route en bref

Phase	Nom	Objectif
PHASE 1	Foundation	Obtenir l'accès, établir la responsabilité et connecter votre premier workload.
PHASE 2	Être protégé	Effectuer votre première sauvegarde, passez en revue les paramètres principaux et assurez-vous que votre protection fonctionne comme prévu dès la première fois.
PHASE 3	Validation et passage à l'échelle	Renforcer la confiance dans votre configuration, étendre l'adoption de Veeam Data Cloud de manière réfléchie et préparer l'exploitation en régime permanent.

À quoi ressemble la réussite après le processus d'intégration

Votre équipe doit être en mesure d'effectuer les actions suivantes :

- Accéder à votre environnement et le gérer en toute confiance.
- Veiller à ce que vos workloads prioritaires soient protégés.
- Exécuter et valider vos premières tâches de sauvegarde.
- Établir un workflow de restauration clair, compris par tous.
- Définir les rôles, la responsabilité et les routines de révision.
- Déterminer où vous souhaitez vous développer ensuite.
- Savoir où s'adresse pour obtenir de l'aide.



Comment utiliser ce guide

Chaque étape s'appuie sur la précédente ; il est donc recommandé de suivre les étapes dans l'ordre, à votre propre rythme.



Sommaire

PHASE 1 • Foundation	4
Étape 1 : Obtenir l'accès	4
Étape 2 : Établir la responsabilité	5
Étape 3 : Connecter votre premier workload	5
PHASE 2 • Être protégé	6
Étape 4 : Effectuer votre première sauvegarde réussie	6
Étape 5 : Vérification des paramètres de sauvegarde et de rétention	6
Étape 6 : Adopter des habitudes de supervision de base	7
Étape 7 : Comprendre pleinement vos options de restauration	7
PHASE 3 • Validation et passage à l'échelle	8
Étape 8 : Valider l'adéquation de votre protection à vos attentes	8
Étape 9 : Élargir votre couverture là où c'est logique	8
Étape 10 : Introduction progressive des fonctionnalités avancées	9
Liste de contrôle rapide	10
Annexe : Référence rapide	11



PHASE 1

Foundation

Objectif : obtenir l'accès, établir la responsabilité et connecter votre premier workload.

Votre premier mois avec Veeam Data Cloud est consacré à la mise en place de bases solides. Ne compliquez pas trop les choses: concentrez-vous sur l'accès, les rôles et la mise en place de votre premier chemin de protection.

Pour consulter le guide de l'utilisateur et la documentation de configuration, cliquez [ici](#).



Étape 1 : Obtenir l'accès

1. Vérifiez que vous avez accès à Veeam Data Cloud

Avant de démarrer, assurez-vous que les bonnes personnes peuvent accéder à Veeam Data Cloud et à la bonne organisation.

Commencez ici :

- Confirmez que votre abonnement **Veeam Data Cloud** est actif.
- Acceptez l'invitation à votre organisation.
- Connectez-vous à cloud.veeam.com
- Choisissez la bonne organisation si vous appartenez à plusieurs organisations.
- Consultez et acceptez les conditions générales.
- Assurez-vous que l'administrateur initial possède le niveau d'accès requis.

Le premier utilisateur d'une nouvelle organisation Veeam Data Cloud se voit automatiquement attribuer le **rôle d'administrateur** de l'organisation, qui lui permet de gérer les utilisateurs et d'effectuer des actions de configuration.

Selon le workload que vous intégrez, des étapes de configuration supplémentaires peuvent être nécessaires.

Dans le cas de **Veeam Data Cloud pour Salesforce**, vous devrez également télécharger deux plug-ins :

[Téléchargez l'application client externe](#) pour que Veeam Data Cloud puisse se connecter à Salesforce. Il s'agit d'une fonctionnalité de sécurité supplémentaire destinée à protéger votre environnement. Pour permettre aux utilisateurs finaux de Salesforce de désarchiver leurs propres données, téléchargez notre extension Salesforce.

Pour **Veeam Intelligence**, vous devrez [accepter le message d'adhésion qui s'affiche](#).



Étape 2 : Établir la responsabilité

Définir la responsabilité dès le départ

Une expérience d'intégration plus fluide commence par des responsabilités claires. Assurez-vous donc que vous et votre équipe soyez alignés sur les points suivants :

- Qui est responsable de l'administration de la plateforme.
- Qui gère les tâches de sauvegarde et restauration.
- Qui a besoin d'avoir une visibilité sur l'état de la protection.
- Qui valide les politiques et décisions de rétention.

Il n'est pas nécessaire de faire un grand exercice de gouvernance ici ; assurez-vous simplement d'établir suffisamment de clarté pour avoir une base de référence et continuer à avancer.

Attribuer les rôles appropriés

Le contrôle d'accès en fonction du rôle (RBAC) vous permet d'agir plus rapidement sans perdre le contrôle. Pour cette étape, concentrez-vous sur :

- Limiter les autorisations élevées au groupe le plus restreint possible.
- Donner aux opérateurs l'accès dont ils ont besoin pour faire leur travail, mais rien de plus afin de rester aussi sécurisé que possible.
- Séparer la responsabilité administrative d'une visibilité plus globale lorsque cela est approprié.

Étape 3 : Connecter votre premier workload






La façon la plus rapide d'obtenir de la valeur est de protéger quelque chose de réel. Vos priorités à cette étape incluent :

- Choisir le premier workload que vous souhaitez protéger.
- Valider les prérequis.
- Connecter votre environnement.
- Confirmer que votre service peut détecter les données que vous souhaitez sauvegarder.

Point de contrôle

Pour de nombreux clients, c'est à ce moment que le projet d'intégration commence à passer de la phase de configuration à celle de l'avancement.

À la **fin de la phase 1**, vous devriez avoir :

-  Accès confirmé.
-  Responsabilité administrative initiale établie.
-  Rôles principaux attribués.
-  Votre premier workload connecté.
-  Documentation du produit et ressources de configuration mises en favoris pour l'équipe.

PHASE 2

Être protégé

Objectif : compléter votre première sauvegarde, revoir les paramètres essentiels et vérifier que votre protection fonctionne comme attendu dès la première utilisation.

Maintenant que votre environnement est connecté, passons de la mise en place à la démonstration de la restauration et de la résilience. C'est là que vous et votre équipe commencerez à voir la véritable valeur de Veeam Data Cloud.

Étape 4 : Effectuer votre première sauvegarde réussie

Sauvegardes dans Veeam Data Cloud

Votre première sauvegarde réussie constitue véritablement une étape importante ! Cela montre que votre environnement est configuré, connecté et protège activement les données de votre organisation.

À ce stade, concentrez-vous sur :

- Commencez la protection du workload sélectionné.
- Confirmez que vos sauvegardes ont été effectuées avec succès.
- Passez en revue les avertissements ou les éléments en échec au fur et à mesure qu'ils apparaissent.
- Assurez-vous que vos objets protégés correspondent à vos attentes.

À ce stade, maintenez des objectifs réalistes. À ce stade, vous validez la pertinence d'un mode, sans chercher à résoudre tous les problèmes d'un coup.

Étape 5 : Vérification des paramètres de sauvegarde et de rétention

Une fois la protection en place, assurez-vous que votre configuration est alignée sur le mode de fonctionnement quotidien de votre équipe.

Pour cette étape, concentrez-vous sur :

- Paramétrez votre politique de sauvegarde.
- Définissez les paramètres de rétention.
- Établissez une couverture pour les utilisateurs, les sites ou les services clés.
- Les fonctionnalités disponibles selon votre formule d'abonnement.

C'est à ce stade que votre première tâche de sauvegarde devient le fondement de la protection opérationnelle.



Étape 6 : Adoptez des habitudes de supervision de base

Vous n'avez pas encore besoin d'établir un processus lourd. Au contraire, cette étape vise à instaurer une meilleure visibilité sur votre environnement.

Vous pouvez commencer à instaurer un rythme pour cela avec les actions suivantes :

- Vérifier régulièrement l'état de vos sauvegardes.
- Vérifier les tableaux de bord et les vues d'activité.
- S'assurer que les bonnes personnes savent où chercher les problèmes.
- Établir une cadence légère pour les vérifications d'intégrité.

La confiance vient du fait de savoir ce qui se passe dans l'ensemble de votre environnement, sans se contenter de supposer que les choses se passent bien.

Étape 7 : Comprendre pleinement vos options de restauration

Au cours de cette phase, assurez-vous que votre équipe peut :

- Identifier les options de restauration disponibles.
- Comprendre qui peut effectuer des restaurations.
- Réaliser un scénario de restauration de base.
- Documenter le premier workflow de restauration. Vous ne devez pas encore réaliser un exercice de restauration à grande échelle, mais vous devez savoir comment fonctionne la restauration avant d'en avoir besoin.

Point de contrôle

À la fin de la **phase 2**, vous devriez avoir :

- ✔ Toutes vos sauvegardes sont correctement configurées et effectuées avec succès. La stratégie de base et les paramètres de rétention sont également examinés.
- ✔ Des routines de supervision de base sont en place.
- ✔ Un processus de restauration simple est établi et compris par l'équipe.
- ✔ Vous avez rapidement établi une confiance dans le bon fonctionnement de la protection Veeam Data Cloud.

PHASE 3

Validation et passage à l'échelle

Objectif : compléter votre première sauvegarde, revoir les paramètres essentiels et vérifier que votre protection fonctionne comme attendu dès la première utilisation.

À ce stade, les éléments de base sont en principe opérationnels. Le moment est donc venu de valider, peaufiner et déterminer les prochaines étapes pour votre organisation.

Étape 8 : Valider l'adéquation de votre protection à vos attentes

C'est le bon moment pour faire une pause et vous poser quelques questions directes :

- Tous les workloads sont-ils protégés ?
- Les sauvegardes se terminent-elles de manière régulière ?
- Les rôles et l'appropriation sont-ils encore clairs, surtout après les tests ?
- Existe-t-il des lacunes en termes de visibilité, de rétention ou de préparation à la restauration ?

Ce contrôle est important. C'est ainsi que les équipes passent de la simple configuration de leur environnement de protection des données à une confiance totale en celui-ci.

Étape 9 : Élargir votre couverture là où c'est logique

Une fois que votre premier workload est stable, identifiez votre prochaine priorité logique. Cela peut consister à ajouter des utilisateurs supplémentaires, à étendre la couverture des workload, à assurer une application plus complète des politiques, ou à renforcer la coordination entre les équipes qui partagent la responsabilité de la protection et de la restauration.

L'extension doit suivre la preuve de concept. Démarrez par ce qui est prioritaire, puis étendez votre couverture en toute confiance.





□+ Étape 10 : Introduction progressive des fonctionnalités avancées

C'est le moment de vous assurer que vous et votre équipe comprenez ce qu'il est possible de faire après avoir configuré et mis en place votre environnement Veeam Data Cloud.

En fonction de votre service et de votre plan Veeam Data Cloud, l'étape suivante peut comprendre :

- Extension de la protection des workloads.
- Fonctionnalités supplémentaires d'IA.
- Des stratégies de résilience plus solides, mieux adaptées aux exigences de votre entreprise.

L'objectif ici est simple : savoir ce qui est disponible pour vous et décider de ce qui mérite votre attention ensuite.

Point de contrôle

Une bonne intégration doit vous permettre de disposer d'un système que votre équipe pourra exploiter en toute confiance à l'avenir.

À la fin de la phase 3, vous devriez avoir :

- ✓ Confiance dans votre configuration initiale.
- ✓ Protection vérifiée pour toutes les workloads.
- ✓ Une appropriation opérationnelle claire.
- ✓ Une routine de révision répétable.

Liste de contrôle rapide

Mesures immédiates :

- Confirmez que votre abonnement **Veeam Data Cloud** est actif.
- Acceptez l'invitation à votre organisation.
- Connectez-vous à cloud.veeam.com.
- Confirmez la responsabilité administrative initiale.
- Identifiez qui gèrera la sauvegarde et la restauration.
- Connectez votre première charge de travail (workload).

D'ici la Phase 1 :

- Attribuez les rôles utilisateur.
- Effectuez la configuration initiale.
- Validez la préparation à la première sauvegarde.
- Partagez les principales ressources de configuration avec l'équipe.

D'ici la Phase 2 :

- Toutes vos données devraient être sauvegardées avec succès.
- Passez en revue la politique et les paramètres de rétention.
- Établissez des habitudes de supervision de base.
- Comprenez les options de restauration et responsabilités et assurez-vous qu'elles sont en adéquation avec vos exigences de conformité.

D'ici la phase 3 :

- Assurez-vous que votre protection est conforme aux exigences.
- Étendez la couverture là où c'est nécessaire.
- Établissez des révisions opérationnelles régulières.
- Identifiez les prochaines fonctionnalités que vous pourriez envisager d'adopter.



Remarque à l'intention des décideurs IT

Au cours des trois premières phases, votre chemin vers le succès ne s'arrête pas à la mise en service de votre plateforme.

La réussite signifie que toutes vos données sont protégées, que l'Intégrité de la sauvegarde soit visible, que les processus et politiques de restauration soient compris, et que les responsabilités soient clairement définies. Il en résulte moins d'incertitude, moins de frictions opérationnelles et une plus grande confiance dans la capacité de votre équipe à protéger ce qui compte le plus et à restaurer les données en cas de besoin.

Une fois les bases établies, vous pouvez véritablement exploiter tout le potentiel de Veeam Data Cloud et constater comment nous pouvons être votre partenaire en matière de protection des données.

Annexe :

Référence rapide

Au fur et à mesure que votre environnement évolue, ces ressources accompagnent votre équipe lors de la configuration, de la validation et des opérations continues.

Gestion des accès et des comptes :

- [Créez un compte Veeam](#) : Configurez l'accès pour démarrer.
- [Mon compte](#) : Gérez les utilisateurs, les accès, les abonnements, etc.
- [État du système Veeam Data Cloud](#) : Disponibilité et temps de fonctionnement des services.

Guide produit et configuration :

- [Centre d'assistance Veeam](#) : Guides de l'utilisateur et documentation de configuration.

Formation et déploiement :

- [Veeam University](#) : Intégration à votre rythme et formation professionnelle.
- [Webinaires d'intégration](#) : Sessions d'intégration en direct, animées par des experts.

Dépannage et support :

- [Base de connaissances](#) : Dépannage et meilleures pratiques.
- [Community Hub](#) et [R&D Forums](#) : Entraide et discussions.
- [Créer un ticket de support](#) : Soumettez et gérez vos demandes d'assistance.

Restez informé :

- [Journal des modifications de Veeam Data Cloud](#) : Mises à jour de produit et modifications du produit.
- [Bibliothèque de ressources](#) : Ressources axées sur les solutions et rapports sectoriels.
- Si votre équipe intègre plusieurs services, il est judicieux de documenter dès le début votre modèle de responsabilités internes, afin que chaque groupe sache ce dont il est responsable et comment le succès sera mesuré.

➔ [Connectez-vous à Veeam Data Cloud](#)
et commencez à protéger votre premier workload.



À propos de Veeam Software

Veeam, acteur de référence de la confiance des données et de l'IA, est une société spécialisée dans l'aide aux organisations pour garantir que leurs données et leur IA sont pleinement comprises, sécurisées et résilientes, afin de pouvoir accélérer leur innovation en matière d'IA sécurisée à grande échelle. En tant que leader du marché en matière de résilience des données et de gestion de la posture de sécurité des données, Veeam est conçu pour la convergence de l'identité, des données, de la sécurité et des risques liés à l'IA.

Basé à Seattle et possédant des bureaux dans plus de 30 pays, Veeam protège plus de 550 000 clients dans le monde, dont 82 % des entreprises du Fortune 500,

Pour en savoir plus, rendez-vous sur www.veeam.com ou suivez Veeam sur LinkedIn [@veeam-software](#) et X [@veeam](#).