**AWS Backup sur plusieurs Comptes AWS**

Vous pouvez utiliser la fonctionnalité de gestion multicomptes dans AWS Backup pour gérer et surveiller vos tâches de sauvegarde, de restauration et de copie sur l'ensemble des tâches Comptes AWS que vous configurez AWS Organizations. [AWS Organizations](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html) est un service qui propose une gestion basée sur des règles pour plusieurs utilisateurs Comptes AWS à partir d'un seul compte de gestion. Elle vous permet de standardiser la façon dont vous mettez en œuvre les stratégies de sauvegarde, en réduisant simultanément les erreurs et les efforts liés aux procédures manuelles. À partir d'une vue centralisée, vous pouvez facilement identifier les ressources de tous les comptes qui répondent aux critères qui vous intéressent.

Si vous configurez AWS Organizations, vous pouvez configurer AWS Backup pour surveiller les activités de tous vos comptes en un seul endroit. Vous pouvez également créer une stratégie de sauvegarde et l'appliquer à certains comptes spécifiques qui font partie de votre organisation et afficher les activités de sauvegarde agrégées directement à partir de la console AWS Backup. Cette fonctionnalité permet aux administrateurs de sauvegarde de surveiller efficacement l'état des tâches de sauvegarde sur des centaines de comptes dans l'ensemble de leur entreprise à partir d'un seul compte de gestion.

**ANNEXE Procédure de sauvegarde inter-compte**

|  |  |
| --- | --- |
|  | Créez un compte de gestion dans AWS Organizations et ajoutez des comptes sous le compte de gestion. |
|  | Activez la fonctionnalité de gestion inter-comptes dans AWS Backup |
|  | Administrateur délégué |
|  | 1. Créez une politique de sauvegarde à appliquer à toutes les entités Comptes AWS de votre compte de gestion. |
|  | 1. Gérez les tâches de sauvegarde, de restauration et de copie dans toutes vos tâches Comptes AWS. |
|  | 1. Avantage du services centralisé AWS Backup |

1. **Créez un compte de gestion dans AWS Organizations et ajoutez des comptes sous le compte de gestion**.
2. **Activez la fonctionnalité de gestion inter-comptes dans AWS Backup**

Avant de pouvoir utiliser la gestion inter-comptes dans AWS Backup, vous devez activer la fonctionnalité (c'est-à-dire, vous y inscrire). Une fois la fonctionnalité activée, vous pouvez créer des stratégies de sauvegarde qui vous permettent d'automatiser la gestion simultanée de plusieurs comptes.

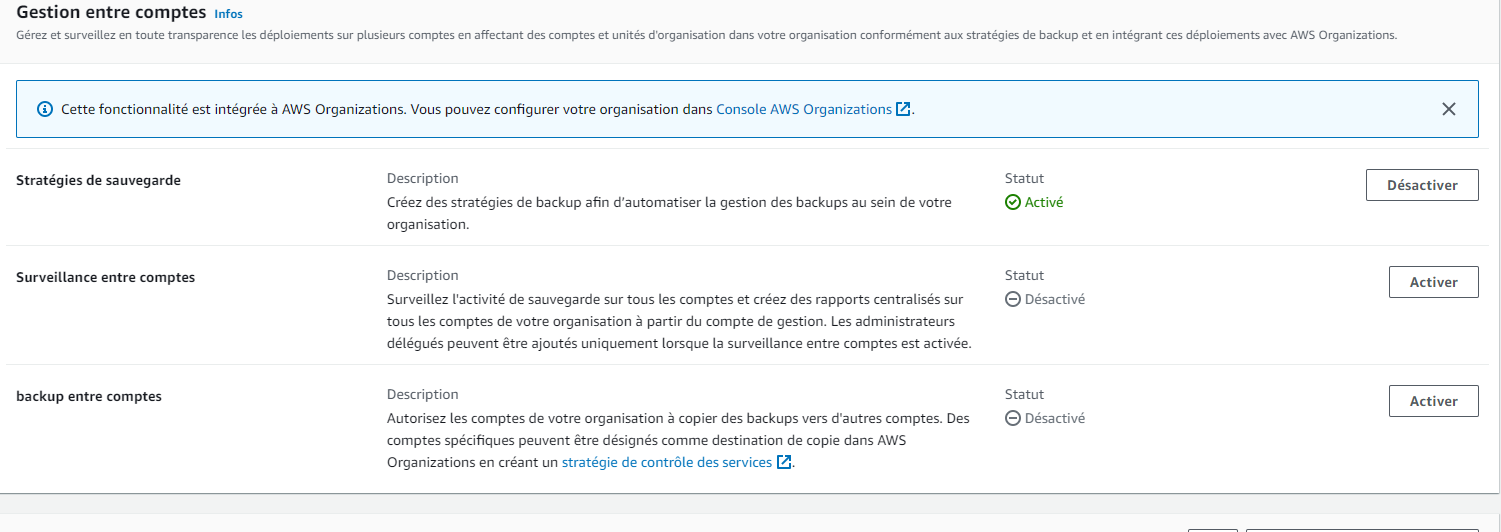
###### Pour activer la gestion inter-comptes

1. Connectez-vous à AWS Management Console et ouvrez AWS Backup console à l'adresse [**https://console.aws.amazon.com/backup**](https://console.aws.amazon.com/backup)**.**

Vous pouvez effectuer cette étape uniquement depuis le compte de gestion.

1. Dans le volet de navigation de gauche, choisissez **Paramètres** pour ouvrir la page de gestion inter-comptes.
2. Dans la section **Stratégies de sauvegarde** choisissez **Activer**.

Ceci vous donne accès à tous les comptes et vous permet de créer des stratégies qui automatisent la gestion de plusieurs comptes dans votre organisation simultanément.



1. Dans la section **Surveillance inter-comptes** choisissez **Activer**.

Cela vous permet de surveiller les activités de sauvegarde, de copie et de restauration de tous les comptes de votre organisation à partir de votre compte de gestion.

1. **Administrateur délégué**

L'administration déléguée constitue un moyen pratique pour les utilisateurs assignés à un compte de membre enregistré d'effectuer la plupart des tâches AWS Backup administratives. Vous pouvez choisir de déléguer l'administration de AWS Backup à un compte membre dans AWS Organizations, étendant ainsi la possibilité AWS Backup de gérer depuis l'extérieur du compte de gestion et à l'ensemble de l'organisation.

### Prérequis

Avant de pouvoir déléguer l'administration des sauvegardes, vous devez d'abord enregistrer au moins un compte membre dans votre AWS organisation en tant qu'**administrateur délégué**. Avant de pouvoir enregistrer un compte en tant qu'administrateur délégué, vous devez d'abord configurer les éléments suivants :

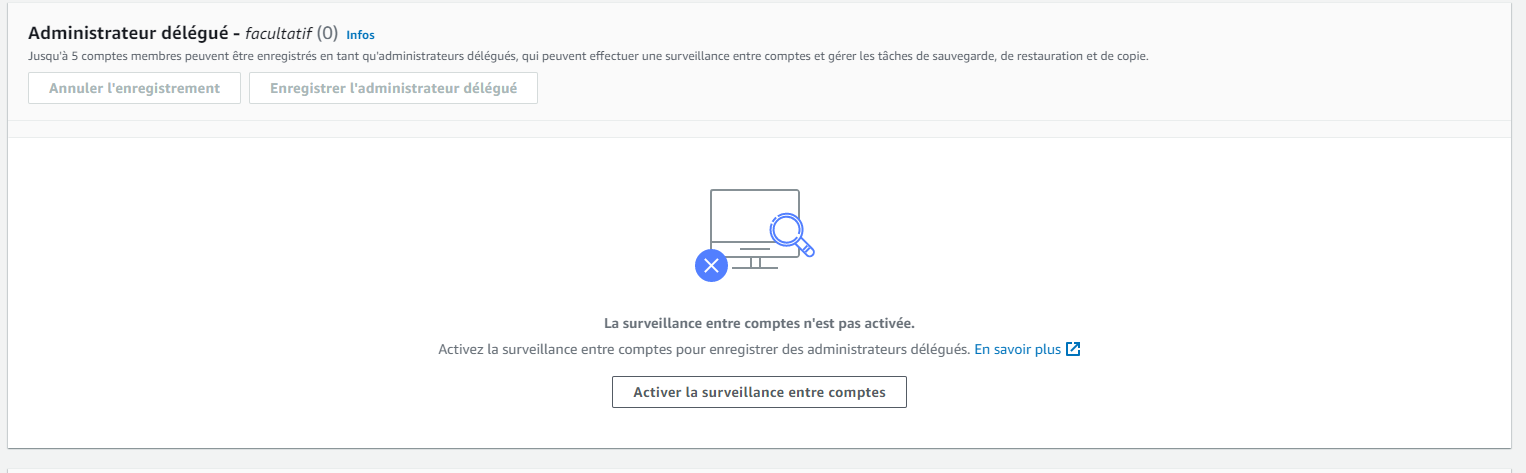
* [AWS Organizations doit être activé et configuré](https://docs.aws.amazon.com/https:/docs.aws.amazon.com/organizations/latest/userguide/orgs_tutorials_basic.html) avec au moins un compte membre en plus de votre compte de gestion par défaut.
* Dans la AWS Backup console, assurez-vous que **les politiques de sauvegarde, la surveillance entre comptes** et **les fonctionnalités de sauvegarde entre comptes** sont activées. Ils se trouvent sous le volet **Administrateurs délégués** de la AWS Backup console.

**Enregistrer un compte membre en tant que compte administrateur délégué**

Voici la première section : Utilisation de AWS Backup console pour enregistrer un compte administrateur délégué afin de surveiller les tâches multicomptes. Pour déléguer des AWS Backup politiques, vous utiliserez la console Organizations de la section suivante.

**Pour enregistrer un compte de membre à l'aide de la AWS Backup console :**

1. [Connectez-vous à AWS Backup console à l'](https://console.aws.amazon.com/https:/console.aws.amazon.com/)aide des informations d'identification de votre compte de gestion AWS Organizations.
2. Dans **Mon compte**, dans la barre de navigation de gauche de la console, choisissez **Paramètres**.
3. Dans le volet **Administrateur délégué**, cliquez sur **Enregistrer l'administrateur délégué** ou sur **Ajouter un administrateur délégué**.
4. Sur la page **Enregistrer l'administrateur délégué**, sélectionnez le compte que vous souhaitez enregistrer, puis choisissez **Enregistrer le compte**.

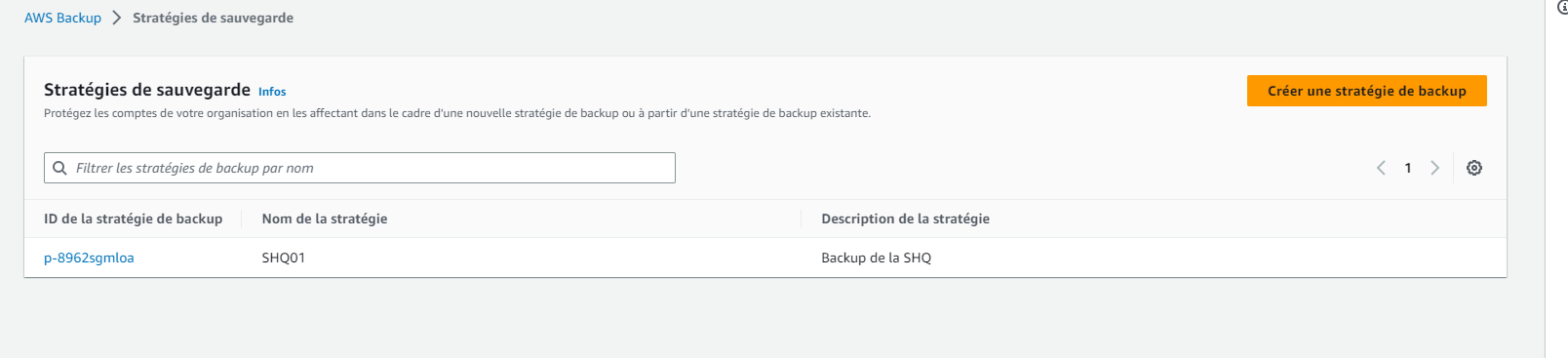


1. **Création d’une politique de sauvegarde**

Après avoir activé la gestion entre comptes, créez une politique de sauvegarde entre comptes à partir de votre compte de gestion.

###### Pour créer une politique de sauvegarde

1. Dans le volet de navigation de gauche, choisissez **Stratégies de sauvegarde**. Sur la page **Stratégies de sauvegarde**, choisissez **Créer des stratégies de sauvegarde**.



1. Dans la section **Détails**, entrez un nom de stratégie de sauvegarde et fournissez une description.
2. Dans la section **Détails des plans de sauvegarde**, cliquez sur l’onglet Éditeur et procédez comme suit :
   1. Pour **Nom du plan de sauvegarde**, entrez un nom.
   2. Pour **Régions**, choisissez une région dans la liste.
3. Dans la section **Configuration de règle de sauvegarde**, choisissez **Ajouter une règle de sauvegarde**.
   1. Dans **Nom de la règle**, entrez le nom de la règle. Le nom de la règle est sensible à la casse et ne peut contenir que des caractères alphanumériques ou des traits d'union.
   2. Pour **Planification**, choisissez une fréquence de sauvegarde dans la liste **Fréquence**, puis choisissez l'une des options dans **Fenêtre de sauvegarde**. Nous vous recommandons de choisir **Utiliser les paramètres par défaut de la fenêtre de sauvegarde, c'est recommandé**.
4. Pour **Cycle de vie**, choisissez les paramètres de cycle de vie de votre choix.
5. Pour **Nom du coffre de sauvegarde**, entrez un nom. Il s'agit du coffre-fort de sauvegarde où les points de récupération créés par vos sauvegardes seront stockés.

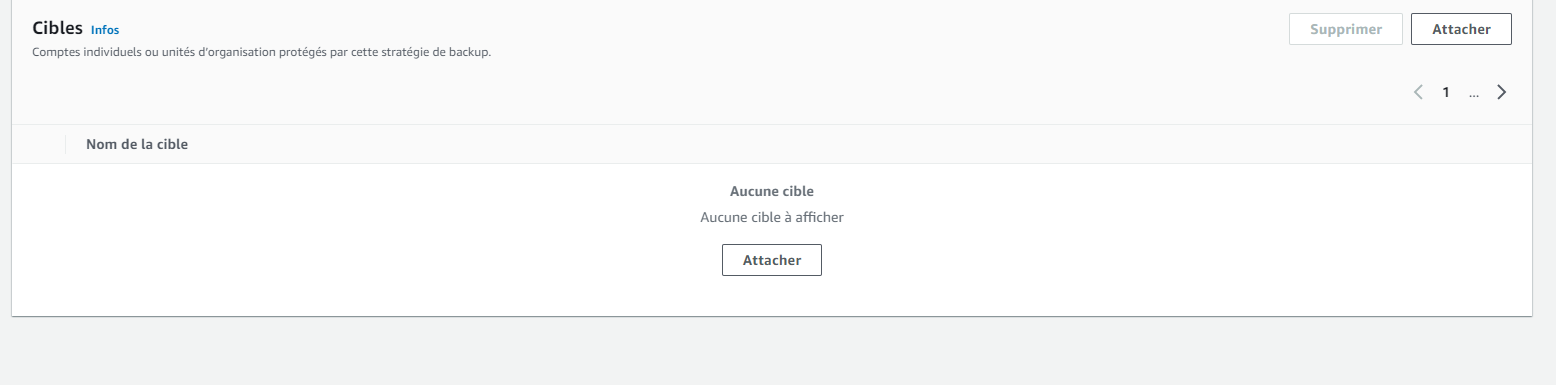
Assurez-vous que le coffre-fort de sauvegarde existe dans tous vos comptes. AWS Backup ne vérifie pas cela.

1. (facultatif) Choisissez une région de destination dans la liste si vous souhaitez que vos sauvegardes soient copiées dans une autre Région AWS, puis ajoutez des balises. Vous pouvez choisir des balises pour les points de récupération créés, quels que soient les paramètres de copie entre régions. Vous pouvez également ajouter d'autres règles.
2. Dans la section **Attribution de ressources**, indiquez le nom du rôle AWS Identity and Access Management (IAM). Pour utiliser le rôle AWS Backup lié à un service, fournissezservice-role/AWSBackupDefaultServiceRole.

AWS Backup assume ce rôle dans chaque compte afin d'obtenir les autorisations nécessaires pour effectuer des tâches de sauvegarde et de copie, y compris les autorisations relatives aux clés de chiffrement, le cas échéant. AWS Backup utilise également ce rôle pour effectuer des suppressions au cours du cycle de vie.

Ajoutez des balises au plan de sauvegarde, si vous le souhaitez. Le nombre maximum de tags autorisés est de 20.

1. Dans la section **Paramètres avancés**, choisissez **Windows VSS** si la ressource que vous sauvegardez exécute Microsoft Windows sur une instance Amazon EC2. Cela vous permet d'effectuer des sauvegardes Windows VSS cohérentes avec les applications.
2. Choisissez **Ajouter un plan de sauvegarde** pour l'ajouter à la stratégie, puis choisissez **Créer une stratégie de sauvegarde**.
3. Dans la section **Cibles**, choisissez l'unité d’organisation ou le compte auquel vous souhaitez attacher la stratégie, puis choisissez **Attacher**. La stratégie peut également être ajoutée à des unités d’organisation ou comptes spécifiques.



1. **Surveillance des activités dans plusieurs comptes AWS**

Pour surveiller les tâches de sauvegarde, de copie et de restauration entre les comptes, vous devez activer la surveillance inter-comptes. Cela vous permet de surveiller les activités de sauvegarde sur tous les comptes à partir du compte de gestion de votre organisation. Après votre inscription, toutes les tâches de votre organisation qui ont été créées après l'inscription sont visibles. Lorsque vous vous désinscrivez, AWS Backup conserve les tâches dans la vue agrégée pendant 30 jours (à partir de l'état Terminus). Les tâches créées après la désinscription ne sont pas visibles et n'affichent pas les tâches de sauvegarde nouvellement créées.

**Pour surveiller plusieurs comptes**

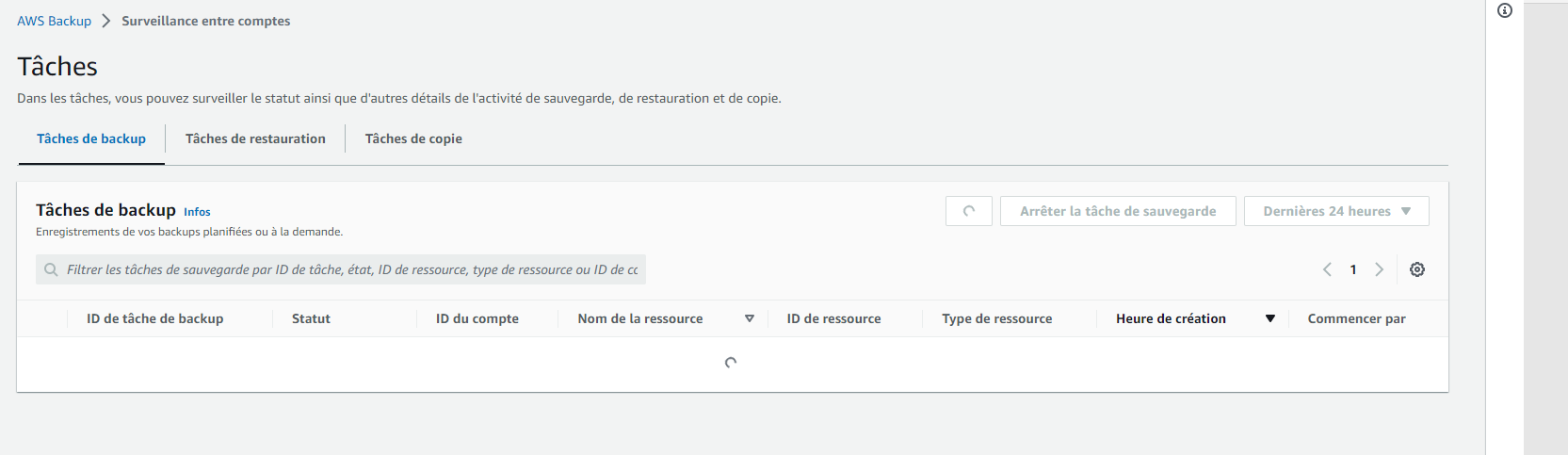
1. Connectez-vous à AWS Management Console et ouvrez AWS Backup console à l'adresse <https://console.aws.amazon.com/backup>.

Vous ne pouvez le faire qu'à partir du compte de gestion.

1. Dans le volet de navigation de gauche, choisissez **Paramètres** pour ouvrir la page de gestion inter-comptes.
2. Dans la section **Surveillance inter-comptes** choisissez **Activer**.

Cela vous permet de surveiller les activités de sauvegarde et de restauration de tous les comptes de votre organisation à partir de votre compte de gestion.

1. Dans le volet de navigation de gauche, choisissez **Surveillance inter-comptes**.
2. Sur la page **Surveillance inter-comptes**, cliquez sur l'onglet **Tâches de sauvegarde**, **Tâches de restauration** ou **Tâches de copie** pour afficher toutes les tâches créées dans l’ensemble de vos comptes. Vous pouvez voir chacun de ces jobs par Compte AWS identifiant, et vous pouvez voir tous les jobs d'un compte spécifique.



1. Dans la zone de recherche, vous pouvez filtrer les tâches par **ID de compte**, **Statut** ou **ID de tâche**.

Par exemple, vous pouvez cliquer sur l'onglet **Tâches de sauvegarde** et afficher toutes les tâches de sauvegarde créées dans l’ensemble de vos comptes. Vous pouvez filtrer la liste par **ID de compte** et afficher toutes les tâches de sauvegarde créées dans ce compte.

1. **Avantage du services centralisé AWS Backup**

L'un des avantages de l'utilisation d'un service centralisé AWS Backup par rapport à la création de plusieurs AWS Backup pour chaque compte est la réduction des coûts liés à la gestion des sauvegardes et à la gestion des politiques de rétention des données.

En effet, en utilisant un service centralisé, vous pouvez économiser sur les coûts de stockage, car vous n'aurez pas besoin de dupliquer les données de sauvegarde sur chaque compte. De plus, en utilisant un seul service AWS Backup, vous pouvez mieux gérer les politiques de rétention des données, ce qui peut également réduire les coûts liés au stockage de données inutiles ou obsolètes.

De plus, en centralisant le service AWS Backup, vous pouvez bénéficier d'une vue d'ensemble de l'état de la sauvegarde de toutes vos instances, bases de données et applications, ce qui peut faciliter la gestion des sauvegardes et des restaurations en cas de besoin.

En fin de compte, la décision d'utiliser un service centralisé AWS Backup ou plusieurs AWS Backup dépendra de vos besoins et de vos contraintes spécifiques en matière de coûts, de gestion et de sécurité. Il est important de considérer tous les aspects avant de prendre une décision pour votre organisation.