Nouveau rôle sur Scalingo : collaborez sans exposer vos données

28 août 2025 - 5 min de lecture

Pour collaborer efficacement, sans compromettre la stabilité ou la sécurité de vos applications et de leurs données, nous introduisons aujourd'hui un nouveau rôle pensé pour donner davantage d'autonomie à vos équipes techniques, tout en protégeant vos paramètres sensibles et les données de vos clients.

Mieux outiller la collaboration

Chez Scalingo, la simplicité a toujours été une valeur centrale, y compris dans la manière de collaborer autour du développement de vos applications. Lorsqu'une équipe grandit ou qu'un projet manipule des données de santé (HDS), il est primordial que ses collaborateurs disposent de droits adaptés à leurs missions.

Jusqu'alors, un collaborateur invité sur une application disposait quasiment des mêmes permissions que son propriétaire : déploiement, configuration, logs, gestion des autres utilisateurs, des secrets et des données.

Ce fonctionnement convient à de nombreuses équipes pour lesquelles l'association des mécanismes de cloisonnement et de sécurité du dépôt de code et de la plateforme de déploiement offre un niveau de contrôle adapté. Le rôle Collaborateur permet ainsi d'onboarder rapidement des profils de confiance avec un accès complet à l'environnement applicatif et à ses données.

Dans des organisations plus structurées, vous avez été nombreux à nous remonter que ce niveau d'accès pouvait s'avérer inadapté ou trop large pour certains profils.

Un rôle pensé pour les contributeurs

Le nouveau rôle **Collaborateur Limité** s'adresse principalement aux développeurs, contributeurs ou prestataires qui doivent intervenir sur vos applications sans pour autant pouvoir en modifier la configuration, déployer du code non validé ou accéder aux bases de données.

Il est particulièrement adapté si :

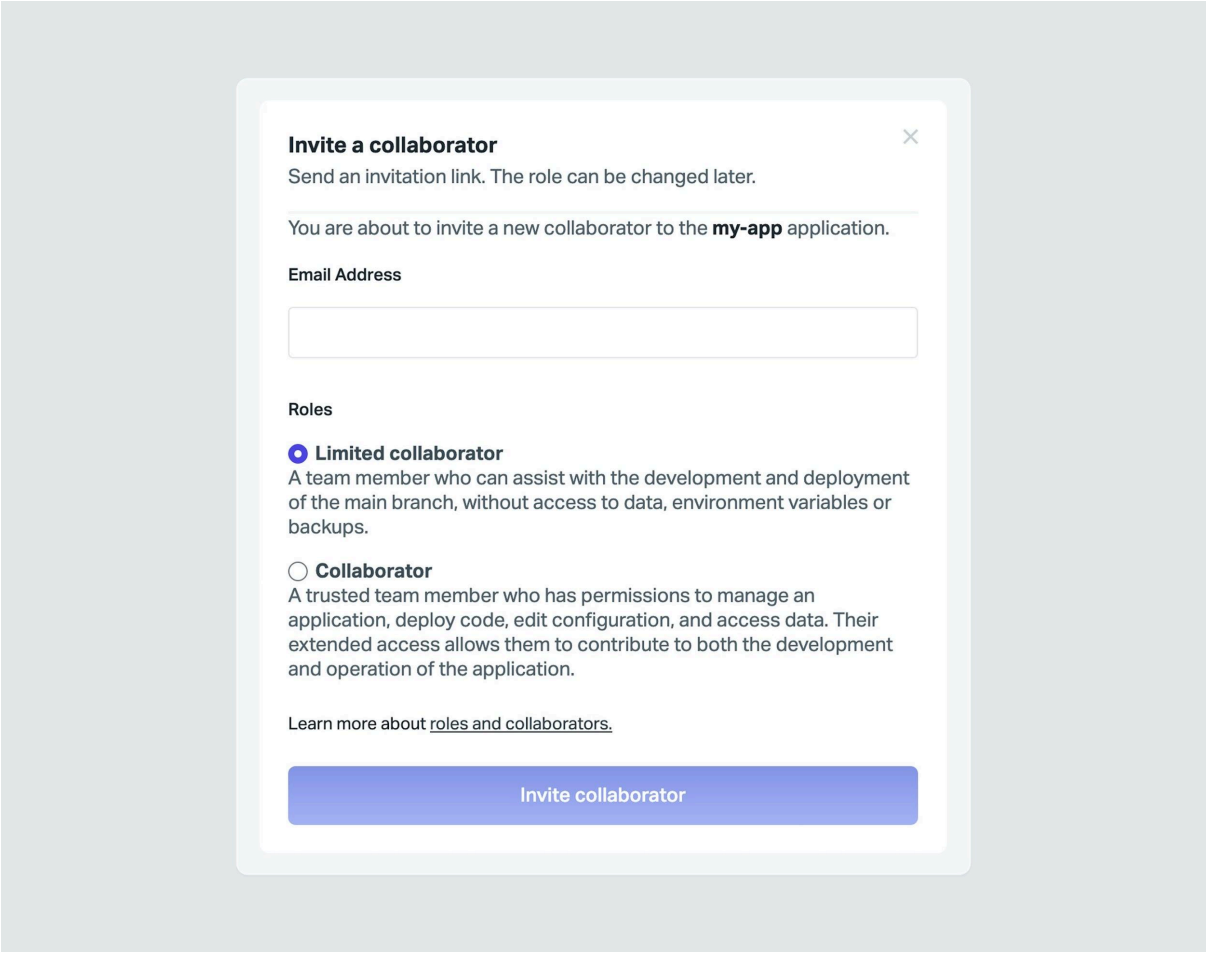
- Vous travaillez avec des développeurs externes ou freelances
- Vous souhaitez restreindre l'accès aux données à un noyau réduit
- Vous encadrez des profils juniors ou du personnel de support
- Vous préparez votre projet à des exigences de sécurité ou de conformité

Un collaborateur limité peut intervenir sur une application en accédant à sa configuration en lecture seule, en suivant les déploiements, en redéployant la branche par défaut ou en consultant les logs et les métriques récentes. En revanche, il n'a pas accès aux variables d'environnement, ne peut pas modifier sa configuration, interagir avec les bases de données ou encore gérer les collaborateurs.

Consultez la documentation pour découvrir le détail des permissions associées avec chaque rôle.

Quand l'utiliser ?

Ce rôle a vocation à devenir le choix par défaut lors de l'invitation d'un nouveau collaborateur sur vos applications.



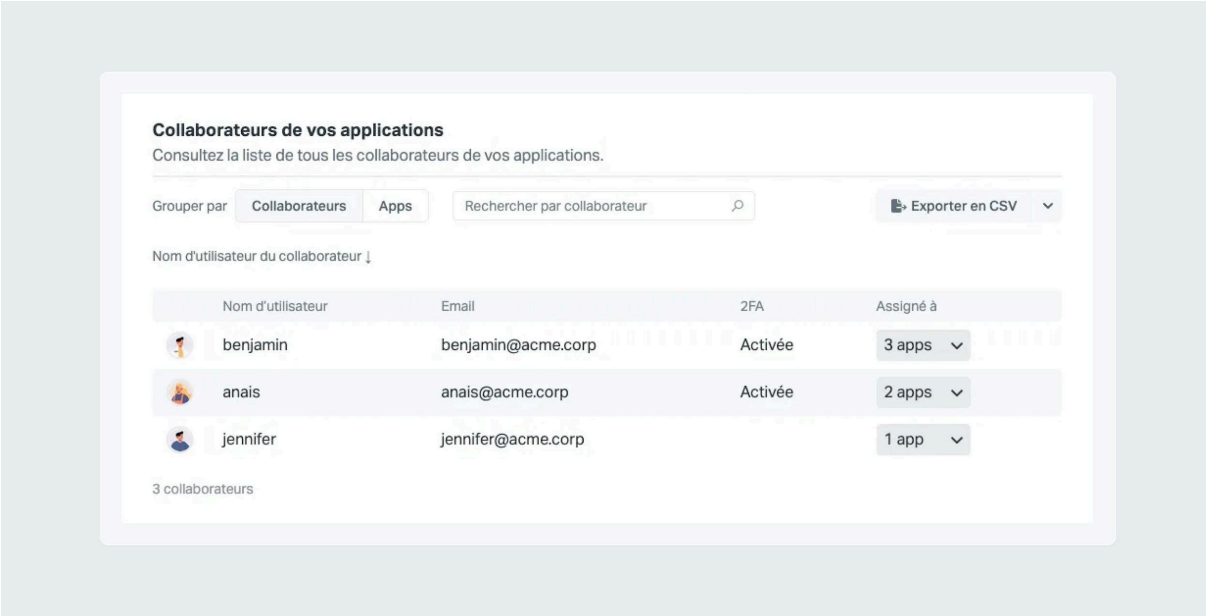
Ce rôle garantit un niveau d'accès initial minimal qui peut à tout moment, lors de l'invitation ou a posteriori, être réévalué en fonction des missions et des habilitations de l'utilisateur concerné.

Certains privilèges nécessitent une attention particulière et ne doivent être attribués qu'à des personnes de confiance, qualifiées et légitimes.

La revue des droits d'accès, un réflexe à adopter

L'ajout de ce nouveau rôle est aussi l'occasion idéale d'effectuer une revue des droits d'accès et de l'adéquation des rôles de vos collaborateurs avec leurs responsabilités actuelles. En effet, dans ses Recommandations relatives à l'administration sécurisée des SI, l'ANSSI préconise une revue régulière des droits d'accès.

Certains accès pourront être réduits, si les droits sont trop larges, et vous pourrez également identifier des comptes ou accès obsolètes qu'il conviendra de supprimer.



Pour aller plus loin, vous pouvez également vous appuyer sur l'API Scalingo pour intégrer ce type de vérification dans vos outils internes.

Nos recommandations pour sécuriser l'accès à vos applications

Nous avons également publié un guide de gestion des accès par type d'équipe qui rassemble nos recommandations pour tirer le meilleur parti des fonctionnalités existantes en matière de gestion des accès et de sécurité chez Scalingo. Ce guide vous aidera à configurer vos applications et choisir les bons rôles en fonction de la structure de votre équipe ou de votre organisations.

Startup, équipe produit ou agence multi-projets, chaque typologie d'organisation peut tirer partie de ces bonnes pratiques afin de trouver le juste équilibre entre collaboration et sécurité.

Une nouvelle étape vers une gestion des accès plus fine

Cette évolution est le fruit d'un travail de recherche qui répond à un besoin fort que vous nous avez exprimé : pouvoir déléguer pour fluidifier les processus de travail, mais pouvoir déléguer sans exposer inutilement vos données.

Ce nouveau rôle a été pensé pour s'intégrer naturellement à vos pratiques et vos flux de travail actuels. Nous espérons qu'il facilitera le développement collaboratif de vos applications tout en renforçant la sécurité de l'accès à vos données.

Ce n’est qu’une première étape d’un chantier plus vaste visant à vous offrir un contrôle à la fois précis et flexible de la gestion des accès. Elle pose les fondations de l’avenir de l’IAM sur Scalingo que nous construisons activement grâce à vos retours.

Pour aller plus loin

- Lire la documentation sur la collaboration avec Scalingo
- Consulter la matrice de permissions détaillée
- Gérer vos collaborateurs dans le dashboard