Rôles d'accès à la NetApp Console

NetApp Console setup and administration

NetApp
February 11, 2026

Sommaire

Rôles d’accès à la NetApp Console

En savoir plus sur les rôles d’accès à la NetApp Console

La gestion des identités et des accès (IAM) dans la NetApp Console fournit des rôles prédéfinis que vous pouvez attribuer aux membres de votre organisation à différents niveaux de votre hiérarchie de ressources. Avant d’attribuer ces rôles, vous devez comprendre les autorisations incluses dans chaque rôle. Les rôles se répartissent dans les catégories suivantes : plateforme, application et service de données.

Rôles de la plateforme

Les rôles de plate-forme accordent des autorisations d’administration à la NetApp Console , y compris l’attribution de rôles et la gestion des utilisateurs. La console a plusieurs rôles de plate-forme.

Rôle de la plateforme	Responsabilités
"Administrateur de l’organisation"	Permet à un utilisateur d’accéder sans restriction à tous les projets et dossiers au sein d’une organisation, d’ajouter des membres à n’importe quel projet ou dossier, ainsi que d’effectuer n’importe quelle tâche et d’utiliser n’importe quel service de données qui n’a pas de rôle explicite associé. Les utilisateurs dotés de ce rôle gèrent votre organisation en créant des dossiers et des projets, en attribuant des rôles, en ajoutant des utilisateurs et en gérant des systèmes s’ils disposent des informations d’identification appropriées. Il s’agit du seul rôle d’accès qui peut créer des agents de console.
"Administrateur de dossier ou de projet"	Permet à un utilisateur un accès illimité aux projets et dossiers attribués. Ils peuvent ajouter des membres aux dossiers ou aux projets qu’ils gèrent, ainsi qu’effectuer n’importe quelle tâche et utiliser n’importe quel service de données ou application sur les ressources du dossier ou du projet qui leur est attribué. Les administrateurs de dossier ou de projet ne peuvent pas créer d’agents de console.
"Administrateur de la fédération"	Permet à un utilisateur de créer et de gérer des fédérations avec la console, ce qui permet l’authentification unique (SSO).
"Téléspectateur de la Fédération"	Permet à un utilisateur de visualiser les fédérations existantes avec la console. Impossible de créer ou de gérer des fédérations.
"Administrateur de partenariat"	Permet à un utilisateur de créer et de gérer des partenariats.
"Visionneuse de partenariat"	Permet à un utilisateur de visualiser les partenariats existants. Impossible de créer ou de gérer des partenariats.
"Super administrateur"	Donne à l’utilisateur un sous-ensemble de rôles d’administrateur. Ce rôle est conçu pour les petites organisations qui n’ont peut-être pas besoin de répartir les responsabilités de la console entre plusieurs utilisateurs.
"Super spectateur"	Donne à l’utilisateur un sous-ensemble de rôles de spectateur. Ce rôle est conçu pour les petites organisations qui n’ont peut-être pas besoin de répartir les responsabilités de la console entre plusieurs utilisateurs.

Rôles d'application

Voici une liste des rôles dans la catégorie d'application. Chaque rôle accorde des autorisations spécifiques dans le cadre de son périmètre désigné. Les utilisateurs sans le rôle d'application ou de plateforme requis ne peuvent pas accéder à l'application correspondante.

Rôle de l'application	Responsabilités
"Administrateur Google Cloud NetApp Volumes"	Les utilisateurs disposant du rôle Google Cloud NetApp Volumes peuvent découvrir et gérer Google Cloud NetApp Volumes.
"Visionneuse de Google Cloud NetApp Volumes"	Les utilisateurs disposant du rôle utilisateur Google Cloud NetApp Volumes peuvent consulter Google Cloud NetApp Volumes.
"Administrateur Keystone"	Les utilisateurs disposant du rôle d'administrateur Keystone peuvent créer des demandes de service. Permet aux utilisateurs de surveiller et d'afficher l'utilisation, les ressources et les détails d'administration au sein du locataire Keystone auquel ils accèdent.
"Visionneuse Keystone"	Les utilisateurs disposant du rôle de visualiseur Keystone NE PEUVENT PAS créer de demandes de service. Permet aux utilisateurs de surveiller et d'afficher la consommation, les actifs et les informations administratives au sein du locataire Keystone auquel ils accèdent.
Rôle de configuration du médiateur ONTAP	Les comptes de service dotés du rôle de configuration de médiateur ONTAP peuvent créer des demandes de service. Ce rôle est requis dans un compte de service pour configurer une instance du"Médiateur cloud ONTAP" .
"Analyste de soutien aux opérations"	Fournit un accès aux alertes et aux outils de surveillance et la possibilité de saisir et de gérer les cas d'assistance.
"Administrateur de stockage"	Administrez les fonctions de santé et de gouvernance du stockage, découvrez les ressources de stockage, ainsi que modifiez et supprimez les systèmes existants.
"Visionneuse de stockage"	Affichez l'état du stockage et les fonctions de gouvernance, ainsi que les ressources de stockage précédemment découvertes. Impossible de découvrir, de modifier ou de supprimer les systèmes de stockage existants.
"Spécialiste de la santé du système"	Administrer les fonctions de stockage, de santé et de gouvernance, toutes les autorisations de l'administrateur de stockage, sauf l'impossibilité de modifier ou de supprimer les systèmes existants.

Rôles des services de données

Voici une liste des rôles dans la catégorie de service de données. Chaque rôle accorde des autorisations spécifiques dans le cadre de son périmètre désigné. Les utilisateurs qui ne disposent pas du rôle de service de données requis ou d'un rôle de plateforme ne pourront pas accéder au service de données.

Rôle du service de données	Responsabilités
"Super administrateur de sauvegarde et de récupération"	Effectuez toutes les actions dans NetApp Backup and Recovery.
"Administrateur de sauvegarde et de récupération"	Effectuez des sauvegardes sur des snapshots locaux, répliquez-les sur un stockage secondaire et sauvegardez-les sur un stockage d'objets.

Rôle du service de données	Responsabilités
"Administrateur de restauration de sauvegarde et de récupération"	Restaurer les charges de travail dans la sauvegarde et la récupération.
"Administrateur de clone de sauvegarde et de récupération"	Cloner des applications et des données dans la sauvegarde et la récupération.
"Visionneuse de sauvegarde et de récupération"	Afficher les informations de sauvegarde et de récupération.
"Administrateur de reprise après sinistre"	Effectuez toutes les actions dans le service NetApp Disaster Recovery .
"Administrateur de basculement de reprise après sinistre"	Effectuer des basculements et des migrations.
"Administrateur d'application de reprise après sinistre"	Créez des plans de réplication, modifiez les plans de réplication et démarrez les basculements de test.
"Visionneuse de reprise après sinistre"	Afficher uniquement les informations.
Visionneuse de classification	Permet aux utilisateurs d'afficher les résultats de l'analyse de NetApp Data Classification . Les utilisateurs disposant de ce rôle peuvent afficher les informations de conformité et générer des rapports pour les ressources auxquelles ils sont autorisés à accéder. Ces utilisateurs ne peuvent pas activer ou désactiver l'analyse des volumes, des buckets ou des schémas de base de données. La classification ne comporte pas de rôle d'administrateur.
"Administrateur de la résilience aux ransomwares"	Gérez les actions sur les onglets Protéger, Alertes, Récupérer, Paramètres et Rapports de NetApp Ransomware Resilience.
"Visionneuse de résilience aux ransomwares"	Affichez les données de charge de travail, affichez les données d'alerte, téléchargez les données de récupération et téléchargez les rapports dans Ransomware Resilience.
"Comportement utilisateur de Ransomware Resilience administrateur"	Configurez, gérez et affichez la détection, les alertes et la surveillance des comportements suspects des utilisateurs dans Ransomware Resilience.
"Visualiseur de comportement utilisateur de Ransomware Resilience"	Affichez les alertes et les informations sur les comportements suspects des utilisateurs dans Ransomware Resilience.
Administrateur SnapCenter	Offre la possibilité de sauvegarder des instantanés à partir de clusters ONTAP sur site à l'aide de NetApp Backup and Recovery pour les applications. Un membre disposant de ce rôle peut effectuer les actions suivantes : * Effectuer n'importe quelle action à partir de Sauvegarde et récupération > Applications * Gérer tous les systèmes dans les projets et dossiers pour lesquels il dispose d'autorisations * Utiliser tous les services de la NetApp Console SnapCenter n'a pas de rôle de visualiseur.

Liens connexes

- "En savoir plus sur la gestion des identités et des accès de la NetApp Console"

- "Démarrer avec NetApp Console IAM"
- "Gérer les membres de la NetApp Console et leurs autorisations"
- "En savoir plus sur l'API pour NetApp Console IAM"

Rôles d'accès à la plateforme NetApp Console

Attribuez des rôles de plateforme aux utilisateurs pour accorder des autorisations de gestion de la NetApp Console, attribuer des rôles, ajouter des utilisateurs, créer des agents de console et gérer les fédérations.

Exemple de rôles organisationnels pour une grande organisation multinationale

XYZ Corporation organise l'accès au stockage des données par région (Amérique du Nord, Europe et Asie-Pacifique), offrant un contrôle régional avec une surveillance centralisée.

L'**administrateur de l'organisation** dans la console de la société XYZ crée une organisation initiale et des dossiers distincts pour chaque région. L'**administrateur de dossier ou de projet** de chaque région organise les projets (avec les ressources associées) dans le dossier de la région.

Les administrateurs régionaux dotés du rôle **Administrateur de dossier ou de projet** gèrent activement leurs dossiers en ajoutant des ressources et des utilisateurs. Ces administrateurs régionaux peuvent également ajouter, supprimer ou renommer les dossiers et les projets qu'ils gèrent. L'**administrateur de l'organisation** hérite des autorisations pour toutes les nouvelles ressources, maintenant ainsi la visibilité de l'utilisation du stockage dans l'ensemble de l'organisation.

Au sein de la même organisation, un utilisateur se voit attribuer le rôle **Administrateur de la fédération** pour gérer la fédération de l'organisation avec son IdP d'entreprise. Cet utilisateur peut ajouter ou supprimer des organisations fédérées, mais ne peut pas gérer les utilisateurs ou les ressources au sein de l'organisation. L'**administrateur de l'organisation** attribue à un utilisateur le rôle de **spectateur de fédération** pour vérifier l'état de la fédération et afficher les organisations fédérées.

Les tableaux suivants indiquent les actions que chaque rôle de plate-forme de console peut effectuer.

Rôles d'administration de l'organisation

Tâche	Administrateur de l'organisation	Administrateur de dossier ou de projet
Créer des agents	Oui	Non
Créer, modifier ou supprimer des systèmes depuis la console (ajouter ou découvrir des systèmes)	Oui	Oui
Créer des dossiers et des projets, y compris la suppression	Oui	Non
Renommer les dossiers et projets existants	Oui	Oui
Attribuer des rôles et ajouter des utilisateurs	Oui	Oui
Associer des ressources à des dossiers et des projets	Oui	Oui
Associer des agents à des dossiers et des projets	Oui	Non
Supprimer les agents des dossiers et des projets	Oui	Non

Tâche	Administrateur de l'organisation	Administrateur de dossier ou de projet
Gérer les agents (modifier les certificats, les paramètres, etc.)	Oui	Non
Gérer les informations d'identification depuis Administration > Informations d'identification	Oui	Oui
Créer, gérer et afficher les fédérations	Oui	Non
Inscrivez-vous au support et soumettez des cas via la console	Oui	Oui
Utiliser des services de données qui ne sont pas associés à un rôle d'accès explicite	Oui	Oui
Afficher la page d'audit et les notifications	Oui	Oui

Rôles de la Fédération

Tâche	Administrateur de la fédération	Téléspectateur de la Fédération
Créer une fédération	Oui	Non
Vérifier un domaine	Oui	Non
Ajouter un domaine à une fédération	Oui	Non
Désactiver et supprimer les fédérations	Oui	Non
Fédérations de tests	Oui	Non
Voir les fédérations et leurs coordonnées	Oui	Oui

Rôles de partenariat

Tâche	Administrateur de partenariat	Visionneuse de partenariat
Peut créer un partenariat	Oui	Non
Attribuer des rôles aux membres partenaires	Oui	Non
Peut ajouter des membres à un partenariat	Oui	Non
Peut afficher les détails du partenariat de l'organisation	Oui	Oui

Rôles de super administrateur et de spectateur

Le rôle **Super administrateur** offre un accès complet pour gérer les fonctionnalités de la console, le stockage et les services de données. Ce rôle convient à ceux qui supervisent l'administration et la gouvernance. En revanche, le rôle **Super spectateur** offre un accès en lecture seule, idéal pour les auditeurs ou les parties prenantes qui ont besoin de visibilité sans apporter de modifications.

Les organisations doivent utiliser l'accès **Super administrateur** avec parcimonie afin de minimiser les risques de sécurité et de se conformer au principe du moindre privilège. La plupart des organisations devraient

attribuer des rôles précis avec uniquement les autorisations nécessaires pour réduire les risques et améliorer l'auditabilité.

Exemple de super rôles

ABC Corporation dispose d'une petite équipe de cinq personnes qui utilisent la NetApp Console pour les services de données et la gestion du stockage. Au lieu de distribuer plusieurs rôles, ils attribuent le rôle de **Super administrateur** à deux membres seniors de l'équipe qui gèrent toutes les tâches administratives, y compris la gestion des utilisateurs et la configuration des ressources. Les trois membres restants de l'équipe se voient attribuer le rôle de **Super visualiseur**, leur permettant de surveiller l'état du stockage et l'état du service de données sans pouvoir modifier les paramètres.

Rôle	Rôles hérités
Super administrateur	• Administrateur de l'organisation • Administrateur de dossier ou de projet • Administrateur de la fédération • Administrateur de partenariat • Administrateur de la résilience aux ransomwares • Administrateur de reprise après sinistre • Super administrateur de sauvegarde • Administrateur de stockage • Administrateur Keystone • Administrateur Google Cloud NetApp Volumes
Super spectateur	• Visionneuse d'organisation • Téléspectateur de la Fédération • Visionneuse de partenariat • Visionneuse de résilience aux ransomwares • Visionneuse de reprise après sinistre • Visionneuse de sauvegarde • Visionneuse de stockage • Visionneuse Keystone • Visionneuse de Google Cloud NetApp Volumes

Rôles d’application

Rôles Google Cloud NetApp Volumes dans la NetApp Console

Vous pouvez attribuer le rôle suivant aux utilisateurs pour leur donner accès aux Google Cloud NetApp Volumes dans la NetApp Console.

Google Cloud NetApp Volumes utilise le rôle suivant :

- * Administrateur Google Cloud NetApp Volumes * : découvrez et gérez les Google Cloud NetApp Volumes dans la console.
- * Visionneuse de Google Cloud NetApp Volumes * : Affichez les Google Cloud NetApp Volumes dans la console.

Rôles d’accès Keystone dans la NetApp Console

Les rôles Keystone donnent accès aux tableaux de bord Keystone et permettent aux utilisateurs de visualiser et de gérer leur abonnement Keystone . Il existe deux rôles Keystone : administrateur Keystone et visualiseur Keystone . La principale différence entre les deux rôles réside dans les actions qu’ils peuvent entreprendre dans Keystone. Le rôle d’administrateur Keystone est le seul rôle autorisé à créer des demandes de service ou à modifier des abonnements.

Exemple de rôles Keystone dans la NetApp Console

La société XYZ dispose de quatre ingénieurs de stockage de différents départements qui consultent les informations d’abonnement Keystone . Bien que tous ces utilisateurs doivent surveiller l’abonnement Keystone , seul le chef d’équipe est autorisé à faire des demandes de service. Trois membres de l’équipe se voient attribuer le rôle de * visualiseur Keystone **, tandis que le chef d’équipe se voit attribuer le rôle d'** administrateur Keystone * afin qu’il existe un point de contrôle sur les demandes de service pour l’entreprise.

Le tableau suivant indique les actions que chaque rôle Keystone peut effectuer.

Fonctionnalité et action	Administrateur Keystone	Visionneuse Keystone
Afficher les onglets suivants : Abonnement, Ressources, Surveillance et Administration	Oui	Oui
* Page d’abonnement Keystone * :		
Voir les abonnements	Oui	Oui
Modifier ou renouveler les abonnements	Oui	Non
* Page des ressources Keystone * :		
Afficher les actifs	Oui	Oui
Gérer les actifs	Oui	Non
* Page d’alertes Keystone * :		

Fonctionnalité et action	Administrateur Keystone	Visionneuse Keystone
Afficher les alertes	Oui	Oui
Gérer les alertes	Oui	Non
Créer des alertes pour soi-même	Oui	Oui
* Licenses and subscriptions*:		
Peut afficher les licences et les abonnements	Oui	Oui
* Page des rapports Keystone * :		
Télécharger les rapports	Oui	Oui
Gérer les rapports	Oui	Oui
Créer des rapports pour soi-même	Oui	Oui
Demandes de service:		
Créer des demandes de service	Oui	Non
Afficher les demandes de service créées par n'importe quel utilisateur au sein de l'organisation	Oui	Oui

Rôle d'accès d'analyste de support opérationnel pour la NetApp Console

Vous pouvez attribuer le rôle d'analyste de support opérationnel aux utilisateurs afin de leur donner accès aux alertes et à la surveillance. Les utilisateurs disposant de ce rôle peuvent également ouvrir des cas d'assistance.

Analyste de soutien opérationnel

Tâche	Peut effectuer
Gérez vos propres informations d'identification utilisateur depuis Paramètres > Informations d'identification	Oui
Voir les ressources découvertes	Oui
Inscrivez-vous au support et soumettez des cas via la console	Oui
Afficher la page d'audit et les notifications	Oui
Afficher, télécharger et configurer les alertes	Oui

Rôles d’accès au stockage pour la NetApp Console

Vous pouvez attribuer les rôles suivants aux utilisateurs pour leur donner accès aux fonctionnalités de gestion du stockage dans la NetApp Console. Vous pouvez attribuer aux utilisateurs un rôle administratif pour gérer le stockage ou un rôle de spectateur pour la surveillance.

Ces rôles ne sont pas disponibles à partir de l’API de partenariat de la NetApp Console .

Les administrateurs peuvent attribuer des rôles de stockage aux utilisateurs pour les ressources et fonctionnalités de stockage suivantes :

Ressources de stockage :

- Clusters ONTAP sur site
- StorageGRID
- E-Series

Services et fonctionnalités de la console :

- Conseiller numérique
- Mises à jour logicielles
- Planification du cycle de vie
- Durabilité

Exemple de rôles de stockage dans la NetApp Console

XYZ Corporation, une société multinationale, dispose d’une grande équipe d’ingénieurs et d’administrateurs de stockage. Ils permettent à cette équipe de gérer les actifs de stockage pour leurs régions tout en limitant l’accès aux tâches principales de la console telles que la gestion des utilisateurs, la création d’agents et la gestion des licences.

Au sein d’une équipe de 12 personnes, deux utilisateurs se voient attribuer le rôle **Storage viewer** qui leur permet de surveiller les ressources de stockage associées aux projets de console auxquels ils sont affectés. Les neuf autres se voient attribuer le rôle **Administrateur de stockage** qui inclut la possibilité de gérer les mises à jour logicielles, d’accéder à ONTAP System Manager via la console, ainsi que de découvrir les ressources de stockage (ajouter des systèmes). Une personne de l’équipe se voit attribuer le rôle de **Spécialiste de l’état du système** afin qu’elle puisse gérer l’état des ressources de stockage dans sa région, mais pas modifier ni supprimer de systèmes. Cette personne peut également effectuer des mises à jour logicielles sur les ressources de stockage pour les projets qui lui sont attribués.

L’organisation dispose de deux utilisateurs supplémentaires avec le rôle **Administrateur de l’organisation** qui peuvent gérer tous les aspects de la console, y compris la gestion des utilisateurs, la création d’agents et la gestion des licences, ainsi que de plusieurs utilisateurs avec le rôle **Administrateur de dossier ou de projet** qui peuvent effectuer des tâches d’administration de la console pour les dossiers et les projets auxquels ils sont affectés.

Le tableau suivant présente les actions effectuées par chaque rôle de stockage.

Fonctionnalité et action	Administrateur de stockage	Spécialiste de la santé du système	Visionneuse de stockage
Gestion du stockage:			
Découvrir de nouvelles ressources (créer des systèmes)	Oui	Oui	Non
Afficher les systèmes découverts	Oui	Oui	Non
Supprimer les systèmes de la console	Oui	Non	Non
Modifier les systèmes	Oui	Non	Non
Créer des agents	Non	Non	Non
Conseiller numérique			
Afficher toutes les pages et fonctions	Oui	Oui	Oui
* Licenses and subscriptions*			
Afficher toutes les pages et fonctions	Non	Non	Non
Mises à jour logicielles			
Afficher la page de destination et les recommandations	Oui	Oui	Oui
Examiner les recommandations de versions potentielles et les principaux avantages	Oui	Oui	Oui
Afficher les détails de mise à jour d'un cluster	Oui	Oui	Oui
Exécutez les vérifications préalables à la mise à jour et téléchargez le plan de mise à niveau	Oui	Oui	Oui
Installer les mises à jour logicielles	Oui	Oui	Non
Planification du cycle de vie			
Examiner l'état de la planification des capacités	Oui	Oui	Oui
Choisissez l'action suivante (meilleure pratique, niveau)	Oui	Non	Non
Hiérarchisez les données froides vers le stockage cloud et libérez de l'espace de stockage	Oui	Oui	Non
Configurer des rappels	Oui	Oui	Oui

Fonctionnalité et action	Administrateur de stockage	Spécialiste de la santé du système	Visionneuse de stockage
Durabilité			
Afficher le tableau de bord et les recommandations	Oui	Oui	Oui
Télécharger les données du rapport	Oui	Oui	Oui
Modifier le pourcentage d'atténuation du carbone	Oui	Oui	Non
Recommandations de correction	Oui	Oui	Non
Reporter les recommandations	Oui	Oui	Non
Accès du gestionnaire système			
Peut saisir des informations d'identification	Oui	Oui	Non
Informations d'identification			
Informations d'identification de l'utilisateur	Oui	Oui	Non

Rôles des services de données

Rôles de NetApp Backup and Recovery dans la NetApp Console

Vous pouvez attribuer les rôles suivants aux utilisateurs pour leur donner accès à NetApp Backup and Recovery dans la console. Les rôles de sauvegarde et de récupération vous offrent la flexibilité d'attribuer aux utilisateurs un rôle spécifique aux tâches qu'ils doivent accomplir au sein de votre organisation. La manière dont vous attribuez les rôles dépend de votre propre entreprise et de vos pratiques de gestion du stockage.

Le service utilise les rôles suivants qui sont spécifiques à NetApp Backup and Recovery.

- **Super administrateur de sauvegarde et de récupération** : effectuez toutes les actions dans NetApp Backup and Recovery.
- **Administrateur de sauvegarde et de récupération de sauvegarde** : effectuez des sauvegardes sur des snapshots locaux, répliquez sur un stockage secondaire et sauvegardez sur des actions de stockage d'objets dans NetApp Backup and Recovery.
- **Administrateur de restauration de sauvegarde et de récupération** : Restaurez les charges de travail à l'aide de NetApp Backup and Recovery.
- **Administrateur de clonage de sauvegarde et de récupération** : Clonez des applications et des données à l'aide de NetApp Backup and Recovery.
- **Visionneuse de sauvegarde et de récupération** : affichez les informations dans NetApp Backup and Recovery, mais n'effectuez aucune action.

Pour plus de détails sur tous les rôles d'accès à la NetApp Console , consultez "la documentation de

configuration et d'administration de la console" .

Rôles utilisés pour les actions courantes

Le tableau suivant indique les actions que chaque rôle de NetApp Backup and Recovery peut effectuer pour toutes les charges de travail.

Fonctionnalité et action	Super administrateur de sauvegarde et de récupération	Sauvegarde et récupération de l'administrateur de sauvegarde	Administrateur de restauration de sauvegarde et de récupération	Administrateur de clone de sauvegarde et de récupération	Visionneuse de sauvegarde et de récupération
Ajouter, modifier ou supprimer des hôtes	Oui	Non	Non	Non	Non
Installer des plugins	Oui	Non	Non	Non	Non
Ajouter des informations d'identification (hôte, instance, vCenter)	Oui	Non	Non	Non	Non
Afficher le tableau de bord et tous les onglets	Oui	Oui	Oui	Oui	Oui
Démarrer un essai gratuit	Oui	Non	Non	Non	Non
Lancer la découverte des charges de travail	Non	Oui	Oui	Oui	Non
Afficher les informations de licence	Oui	Oui	Oui	Oui	Oui
Activer la licence	Oui	Non	Non	Non	Non
Voir les hôtes	Oui	Oui	Oui	Oui	Oui
Horaires:					
Activer les horaires	Oui	Oui	Oui	Oui	Non
Suspendre les horaires	Oui	Oui	Oui	Oui	Non
Politiques et protection:					
Voir les plans de protection	Oui	Oui	Oui	Oui	Oui

Fonctionnalité et action	Super administrateur de sauvegarde et de récupération	Sauvegarde et récupération de l'administrateur de sauvegarde	Administrateur de restauration de sauvegarde et de récupération	Administrateur de clone de sauvegarde et de récupération	Visionneuse de sauvegarde et de récupération
Créer, modifier ou supprimer des plans de protection	Oui	Oui	Non	Non	Non
Restaurer les charges de travail	Oui	Non	Oui	Non	Non
Créer, diviser ou supprimer des clones	Oui	Non	Non	Oui	Non
Créer, modifier ou supprimer une politique	Oui	Oui	Non	Non	Non
Rapports:					
Afficher les rapports	Oui	Oui	Oui	Oui	Oui
Créer des rapports	Oui	Oui	Oui	Oui	Non
Supprimer les rapports	Oui	Non	Non	Non	Non
Importer depuis SnapCenter et gérer l'hôte:					
Afficher les données SnapCenter importées	Oui	Oui	Oui	Oui	Oui
Importer des données depuis SnapCenter	Oui	Oui	Non	Non	Non
Gérer (migrer) l'hôte	Oui	Oui	Non	Non	Non
Configurer les paramètres:					
Configurer le répertoire des journaux	Oui	Oui	Oui	Non	Non
Associer ou supprimer les informations d'identification d'instance	Oui	Oui	Oui	Non	Non
Seaux:					

Fonctionnalité et action	Super administrateur de sauvegarde et de récupération	Sauvegarde et récupération de l'administrateur de sauvegarde	Administrateur de restauration de sauvegarde et de récupération	Administrateur de clone de sauvegarde et de récupération	Visionneuse de sauvegarde et de récupération
Afficher les seaux	Oui	Oui	Oui	Oui	Oui
Créer, modifier ou supprimer un bucket	Oui	Oui	Non	Non	Non

Rôles utilisés pour les actions spécifiques à la charge de travail

Le tableau suivant indique les actions que chaque rôle NetApp Backup and Recovery peut effectuer pour des charges de travail spécifiques.

Charges de travail Kubernetes

Ce tableau indique les actions que chaque rôle de NetApp Backup and Recovery peut effectuer pour les actions spécifiques aux charges de travail Kubernetes.

Fonctionnalité et action	Super administrateur de sauvegarde et de récupération	Sauvegarde et récupération de l'administrateur de sauvegarde	Administrateur de restauration de sauvegarde et de récupération	Visionneuse de sauvegarde et de récupération
Afficher les clusters, les espaces de noms, les classes de stockage et les ressources API	Oui	Oui	Oui	Oui
Ajouter de nouveaux clusters Kubernetes	Oui	Oui	Non	Non
Mettre à jour les configurations de cluster	Oui	Non	Non	Non
Supprimer les clusters de la gestion	Oui	Non	Non	Non
Voir les candidatures	Oui	Oui	Oui	Oui
Créer et définir de nouvelles applications	Oui	Oui	Non	Non
Mettre à jour les configurations des applications	Oui	Oui	Non	Non
Supprimer les applications de la gestion	Oui	Oui	Non	Non

Fonctionnalité et action	Super administrateur de sauvegarde et de récupération	Sauvegarde et récupération de l'administrateur de sauvegarde	Administrateur de restauration de sauvegarde et de récupération	Visionneuse de sauvegarde et de récupération
Afficher les ressources protégées et l'état de la sauvegarde	Oui	Oui	Oui	Oui
Créez des sauvegardes et protégez les applications avec des politiques	Oui	Oui	Non	Non
Déprotégez les applications et supprimez les sauvegardes	Oui	Oui	Non	Non
Afficher les points de récupération et les résultats de la visionneuse de ressources	Oui	Oui	Oui	Oui
Restaurer les applications à partir des points de récupération	Oui	Non	Oui	Non
Afficher les politiques de sauvegarde Kubernetes	Oui	Oui	Oui	Oui
Créer des politiques de sauvegarde Kubernetes	Oui	Oui	Oui	Non
Mettre à jour les politiques de sauvegarde	Oui	Oui	Oui	Non
Supprimer les politiques de sauvegarde	Oui	Oui	Oui	Non
Afficher les hooks d'exécution et les sources des hooks	Oui	Oui	Oui	Oui
Créer des hooks d'exécution et des sources de hook	Oui	Oui	Oui	Non
Mettre à jour les hooks d'exécution et les sources des hooks	Oui	Oui	Oui	Non
Supprimer les hooks d'exécution et les sources de hook	Oui	Oui	Oui	Non
Afficher les modèles de hook d'exécution	Oui	Oui	Oui	Oui

Fonctionnalité et action	Super administrateur de sauvegarde et de récupération	Sauvegarde et récupération de l'administrateur de sauvegarde	Administrateur de restauration de sauvegarde et de récupération	Visionneuse de sauvegarde et de récupération
Créer des modèles de hook d'exécution	Oui	Oui	Oui	Non
Mettre à jour les modèles de hook d'exécution	Oui	Oui	Oui	Non
Supprimer les modèles de hook d'exécution	Oui	Oui	Oui	Non
Afficher les tableaux de bord récapitulatifs et analytiques de la charge de travail	Oui	Oui	Oui	Oui
Afficher les buckets et les cibles de stockage StorageGRID	Oui	Oui	Oui	Oui

Rôles de NetApp Disaster Recovery dans la NetApp Console

Vous pouvez attribuer les rôles suivants aux utilisateurs pour leur donner accès à NetApp Disaster Recovery dans la console. Les rôles de reprise après sinistre vous offrent la flexibilité d'attribuer aux utilisateurs un rôle spécifique aux tâches qu'ils doivent accomplir au sein de votre organisation. La manière dont vous attribuez les rôles dépend de votre propre entreprise et de vos pratiques de gestion du stockage.

La reprise après sinistre utilise les rôles suivants :

- **Administrateur de reprise après sinistre** : Effectuez toutes les actions.
- **Administrateur de basculement de reprise après sinistre** : Effectuer le basculement et les migrations.
- **Administrateur d'application de récupération après sinistre** : Créer des plans de réplication. Modifier les plans de réplication. Démarrer les tests de basculement.
- **Visionneuse de récupération après sinistre** : Afficher uniquement les informations.

Le tableau suivant indique les actions que chaque rôle peut effectuer.

Fonctionnalité et action	Administrateur de reprise après sinistre	Administrateur de basculement de reprise après sinistre	Administrateur d'application de reprise après sinistre	Visionneuse de reprise après sinistre
Afficher le tableau de bord et tous les onglets	Oui	Oui	Oui	Oui
Démarrer un essai gratuit	Oui	Non	Non	Non

Fonctionnalité et action	Administrateur de reprise après sinistre	Administrateur de basculement de reprise après sinistre	Administrateur d'application de reprise après sinistre	Visionneuse de reprise après sinistre
Lancer la découverte des charges de travail	Oui	Non	Non	Non
Afficher les informations de licence	Oui	Oui	Oui	Oui
Activer la licence	Oui	Non	Oui	Non
Dans l'onglet Sites :				
Voir les sites	Oui	Oui	Oui	Oui
Ajouter, modifier ou supprimer des sites	Oui	Non	Non	Non
Dans l'onglet Plans de réplication :				
Afficher les plans de réplication	Oui	Oui	Oui	Oui
Afficher les détails du plan de réplication	Oui	Oui	Oui	Oui
Créer ou modifier des plans de réplication	Oui	Oui	Oui	Non
Créer des rapports	Oui	Non	Non	Non
Voir les instantanés	Oui	Oui	Oui	Oui
Effectuer des tests de basculement	Oui	Oui	Oui	Non
Effectuer des basculements	Oui	Oui	Non	Non
Effectuer des restaurations automatiques	Oui	Oui	Non	Non
Effectuer des migrations	Oui	Oui	Non	Non
Dans l'onglet Groupes de ressources :				
Afficher les groupes de ressources	Oui	Oui	Oui	Oui
Créer, modifier ou supprimer des groupes de ressources	Oui	Non	Oui	Non
Dans l'onglet Suivi des tâches :				
Voir les offres d'emploi	Oui	Non	Oui	Oui

Fonctionnalité et action	Administrateur de reprise après sinistre	Administrateur de basculement de reprise après sinistre	Administrateur d'application de reprise après sinistre	Visionneuse de reprise après sinistre
Annuler les emplois	Oui	Oui	Oui	Non

Rôles d'accès à la résilience contre les ransomwares pour la NetApp Console

Les rôles Ransomware Resilience permettent aux utilisateurs d'accéder à NetApp Ransomware Resilience. Ransomware Resilience prend en charge les rôles suivants :

Rôles de base

- Administrateur de la résilience aux ransomwares : configurez les paramètres de résilience aux ransomwares ; examinez et répondez aux alertes de chiffrement.
- Visionneuse de résilience aux ransomwares : affichez les incidents de chiffrement, les rapports et les paramètres de découverte

Rôles d'activité de comportement de l'utilisateur"Détection d'activité utilisateur suspecte" les alertes offrent une visibilité sur les données telles que les événements d'activité des fichiers ; ces alertes incluent les noms de fichiers et les actions de fichiers (telles que la lecture, l'écriture, la suppression, le renommage) effectuées par l'utilisateur. Pour limiter la visibilité de ces données, seuls les utilisateurs disposant de ces rôles peuvent gérer ou visualiser ces alertes.

- Administrateur du comportement utilisateur de Ransomware Resilience - Activez la détection d'activité utilisateur suspecte, enquêtez et répondez aux alertes d'activité utilisateur suspecte
- Visualiseur de comportement utilisateur Ransomware Resilience : affichez les alertes d'activité utilisateur suspecte

Les rôles de comportement utilisateur ne sont pas des rôles autonomes ; ils sont conçus pour être ajoutés aux rôles d'administrateur ou de spectateur de Ransomware Resilience. Pour plus d'informations, voir Rôles de comportement des utilisateurs.

Consultez les tableaux suivants pour des descriptions détaillées de chaque rôle.

Rôles de base

Le tableau suivant décrit les actions disponibles pour les rôles d'administrateur et de visualiseur de Ransomware Resilience.

Fonctionnalité et action	Administrateur de la résilience aux ransomwares	Visionneuse de résilience aux ransomwares
Afficher le tableau de bord et tous les onglets	Oui	Oui
Sur le tableau de bord, mettre à jour le statut de la recommandation	Oui	Non
Démarrer un essai gratuit	Oui	Non

Fonctionnalité et action	Administrateur de la résilience aux ransomwares	Visionneuse de résilience aux ransomwares
Lancer la découverte des charges de travail	Oui	Non
Initier la redécouverte des charges de travail	Oui	Non
Dans l'onglet Protéger :		
Ajouter, modifier ou supprimer des plans de protection pour les politiques de *chiffrement*	Oui	Non
Protéger les charges de travail	Oui	Non
Identifier l'exposition aux données sensibles grâce à la classification des données	Oui	Non
Liste des plans de protection et des détails	Oui	Oui
Liste des groupes de protection	Oui	Oui
Afficher les détails du groupe de protection	Oui	Oui
Créer, modifier ou supprimer des groupes de protection	Oui	Non
Télécharger les données	Oui	Oui
Dans l'onglet Alertes :		
Afficher les alertes de chiffrement et les détails des alertes	Oui	Oui
Modifier le statut de l'incident de chiffrement	Oui	Non
Marquer l'alerte de chiffrement pour la récupération	Oui	Non
Afficher les détails de l'incident de chiffrement	Oui	Oui
Ignorer ou résoudre les incidents de chiffrement	Oui	Non
Obtenez la liste complète des fichiers impactés par l'événement de chiffrement	Oui	Non
Télécharger les données d'alertes d'événements de chiffrement	Oui	Oui
Bloquer l'utilisateur (avec la configuration de l'agent Workload Security)	Oui	Non
Dans l'onglet Récupérer :		

Fonctionnalité et action	Administrateur de la résilience aux ransomwares	Visionneuse de résilience aux ransomwares
Télécharger les fichiers impactés par l'événement de chiffrement	Oui	Non
Restaurer la charge de travail à partir d'un événement de chiffrement	Oui	Non
Télécharger les données de récupération à partir de l'événement de chiffrement	Oui	Oui
Télécharger les rapports d'événements de chiffrement	Oui	Oui
Dans l'onglet Paramètres :		
Ajouter ou modifier des destinations de sauvegarde	Oui	Non
Lister les destinations de sauvegarde	Oui	Oui
Afficher les cibles SIEM connectées	Oui	Oui
Ajouter ou modifier des cibles SIEM	Oui	Non
Configurer l'exercice de préparation	Oui	Non
Démarrer, réinitialiser ou modifier l'exercice de préparation	Oui	Non
Examen de l'état de préparation de l'exercice	Oui	Oui
Mettre à jour la configuration de la découverte	Oui	Non
Afficher la configuration de la découverte	Oui	Oui
Dans l'onglet Rapports :		
Télécharger les rapports	Oui	Oui

Rôles de comportement des utilisateurs

Pour configurer les paramètres de comportement utilisateur suspect et répondre aux alertes, un utilisateur doit disposer du rôle d'administrateur du comportement utilisateur Ransomware Resilience. Pour afficher uniquement les alertes de comportement utilisateur suspect, un utilisateur doit disposer du rôle d'observateur de comportement utilisateur Ransomware Resilience.

Les rôles de comportement des utilisateurs doivent être conférés aux utilisateurs disposant de privilèges d'administrateur ou de spectateur Ransomware Resilience existants qui ont besoin d'accéder à"paramètres et alertes d'activité utilisateur suspecte" . Un utilisateur disposant du rôle d'administrateur Ransomware Resilience, par exemple, doit recevoir le rôle d'administrateur du comportement utilisateur Ransomware Resilience pour configurer les agents d'activité utilisateur et bloquer ou débloquer les utilisateurs. Le rôle

d’administrateur du comportement utilisateur de Ransomware Resilience ne doit pas être conféré à un visualiseur de Ransomware Resilience.

Pour activer la détection d’activité utilisateur suspecte, vous devez disposer du rôle d’administrateur de l’organisation de la console.

Le tableau suivant décrit les actions disponibles pour les rôles d’administrateur et de spectateur du comportement utilisateur de Ransomware Resilience.

Fonctionnalité et action	Comportement utilisateur de Ransomware Resilience administrateur	Visualiseur de comportement utilisateur de Ransomware Resilience
Dans l’onglet Paramètres :		
Créer, modifier ou supprimer un agent d’activité utilisateur	Oui	Non
Créer ou supprimer un connecteur d’annuaire utilisateur	Oui	Non
Mettre en pause ou reprendre la collecte de données	Oui	Non
Exécuter un exercice de préparation aux violations de données	Oui	Non
Dans l’onglet Protéger :		
Ajouter, modifier ou supprimer des plans de protection pour les politiques de *comportement utilisateur suspect*	Oui	Non
Dans l’onglet Alertes :		
Afficher les alertes d’activité des utilisateurs et les détails des alertes	Oui	Oui
Modifier le statut de l’incident d’activité de l’utilisateur	Oui	Non
Marquer l’alerte d’activité de l’utilisateur pour la récupération	Oui	Non
Afficher les détails des incidents liés à l’activité de l’utilisateur	Oui	Oui
Rejeter ou résoudre les incidents d’activité des utilisateurs	Oui	Non
Obtenez la liste complète des fichiers impactés par l’utilisateur suspect	Oui	Oui
Télécharger les données d’alertes d’événements d’activité utilisateur	Oui	Oui
Bloquer ou débloquer l’utilisateur	Oui	Non
Dans l’onglet Récupérer :		

Fonctionnalité et action	Comportement utilisateur de Ransomware Resilience administrateur	Visualiseur de comportement utilisateur de Ransomware Resilience
Télécharger les fichiers impactés par l'événement d'activité utilisateur	Oui	Non
Restaurer la charge de travail à partir d'un événement d'activité utilisateur	Oui	Non
Télécharger les données de récupération à partir de l'événement d'activité de l'utilisateur	Oui	Oui
Télécharger les rapports d'événements d'activité utilisateur	Oui	Oui