



Rôles des services de données

NetApp Console setup and administration

NetApp

February 11, 2026

Sommaire

- Rôles des services de données 1
 - Rôles de NetApp Backup and Recovery dans la NetApp Console 1
 - Rôles utilisés pour les actions courantes 1
 - Rôles utilisés pour les actions spécifiques à la charge de travail 3
 - Rôles de NetApp Disaster Recovery dans la NetApp Console 6
 - Rôles d'accès à la résilience contre les ransomwares pour la NetApp Console 7
 - Rôles de base 8
 - Rôles de comportement des utilisateurs 10

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

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 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
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

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
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:					
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
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

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 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
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
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

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
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
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
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 <i>chiffrement</i>	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

Fonctionnalité et action	Administrateur de la résilience aux ransomwares	Visionneuse de résilience aux ransomwares
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 :		
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

Fonctionnalité et action	Administrateur de la résilience aux ransomwares	Visionneuse de résilience aux ransomwares
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

Fonctionnalité et action	Comportement utilisateur de Ransomware Resilience administrateur	Visualiseur de comportement utilisateur de Ransomware Resilience
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 <i>comportement utilisateur suspect</i>	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 :		
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

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.