Contrôle d'accès basé sur des rôles

ONTAP tools for VMware vSphere 10

NetApp
November 17, 2025

Sommaire

Contrôle d’accès basé sur des rôles

Découvrez les outils ONTAP pour VMware vSphere 10 RBAC

Le contrôle d’accès basé sur des rôles (RBAC) est un framework de sécurité qui permet de contrôler l’accès aux ressources au sein d’une entreprise. Le contrôle d’accès basé sur des rôles simplifie l’administration en définissant des rôles disposant de niveaux d’autorisation spécifiques pour effectuer des actions, au lieu d’attribuer des autorisations à des utilisateurs individuels. Les rôles définis sont attribués aux utilisateurs, ce qui permet de réduire le risque d’erreur et simplifie la gestion du contrôle d’accès dans l’ensemble de votre organisation.

Le modèle standard RBAC se compose de plusieurs technologies d’implémentation ou phases de plus en plus complexes. Il en résulte que les déploiements RBAC réels, basés sur les besoins des fournisseurs de logiciels et de leurs clients, peuvent différer et aller de relativement simple à très complexe.

Composants RBAC

À un niveau élevé, plusieurs composants sont généralement inclus dans chaque implémentation de RBAC. Ces composants sont liés de différentes manières dans le cadre de la définition des processus d’autorisation.

Privilèges

Un *privilège* est une action ou une capacité qui peut être autorisée ou refusée. Il peut s’agir d’une opération simple telle que la capacité de lire un fichier ou une opération plus abstraite spécifique à un système logiciel donné. Vous pouvez également définir Privileges pour limiter l’accès aux terminaux de l’API REST et aux commandes de l’interface de ligne de commande. Chaque implémentation de RBAC inclut une Privileges prédéfinie et peut également permettre aux administrateurs de créer une Privileges personnalisée.

Rôles

Un *role* est un conteneur qui inclut un ou plusieurs Privileges. Les rôles sont généralement définis en fonction de tâches ou de fonctions particulières. Lorsqu’un rôle est attribué à un utilisateur, tous les Privileges contenus dans le rôle lui sont attribués. Comme avec Privileges, les implémentations incluent des rôles prédéfinis et permettent généralement de créer des rôles personnalisés.

Objets

Un *objet* représente une ressource réelle ou abstraite identifiée dans l’environnement RBAC. Les actions définies via la Privileges sont effectuées sur ou avec les objets associés. Selon l’implémentation, Privileges peut être accordé à un type d’objet ou à une instance d’objet spécifique.

Utilisateurs et groupes

Users sont affectés ou associés à un rôle appliqué après l’authentification. Certaines implémentations RBAC ne permettent d’attribuer qu’un seul rôle à un utilisateur, tandis que d’autres autorisent plusieurs rôles par utilisateur, peut-être avec un seul rôle actif à la fois. L’attribution de rôles à des *groupes* peut simplifier davantage l’administration de la sécurité.

Autorisations

Une *permission* est une définition qui lie un utilisateur ou un groupe avec un rôle à un objet. Les autorisations peuvent être utiles avec un modèle d’objet hiérarchique dans lequel elles peuvent éventuellement être héritées par les enfants de la hiérarchie.

Deux environnements RBAC

Il existe deux environnements RBAC distincts que vous devez prendre en compte lorsque vous utilisez les outils ONTAP pour VMware vSphere 10.

Serveur VMware vCenter

L'implémentation RBAC dans VMware vCenter Server permet de restreindre l'accès aux objets exposés via l'interface utilisateur du client vSphere. Dans le cadre de l'installation des outils ONTAP pour VMware vSphere 10, l'environnement RBAC est étendu pour inclure des objets supplémentaires représentant les fonctionnalités des outils ONTAP. L'accès à ces objets est fourni via le plug-in distant. Pour plus d'informations, reportez-vous à la section."Environnement RBAC du serveur vCenter"

Groupe ONTAP

Les outils ONTAP pour VMware vSphere 10 se connectent à un cluster ONTAP via l'API REST ONTAP pour effectuer des opérations de stockage. L'accès aux ressources de stockage est contrôlé via un rôle ONTAP associé à l'utilisateur ONTAP lors de l'authentification. Voir "Environnement ONTAP RBAC" pour plus d'informations.

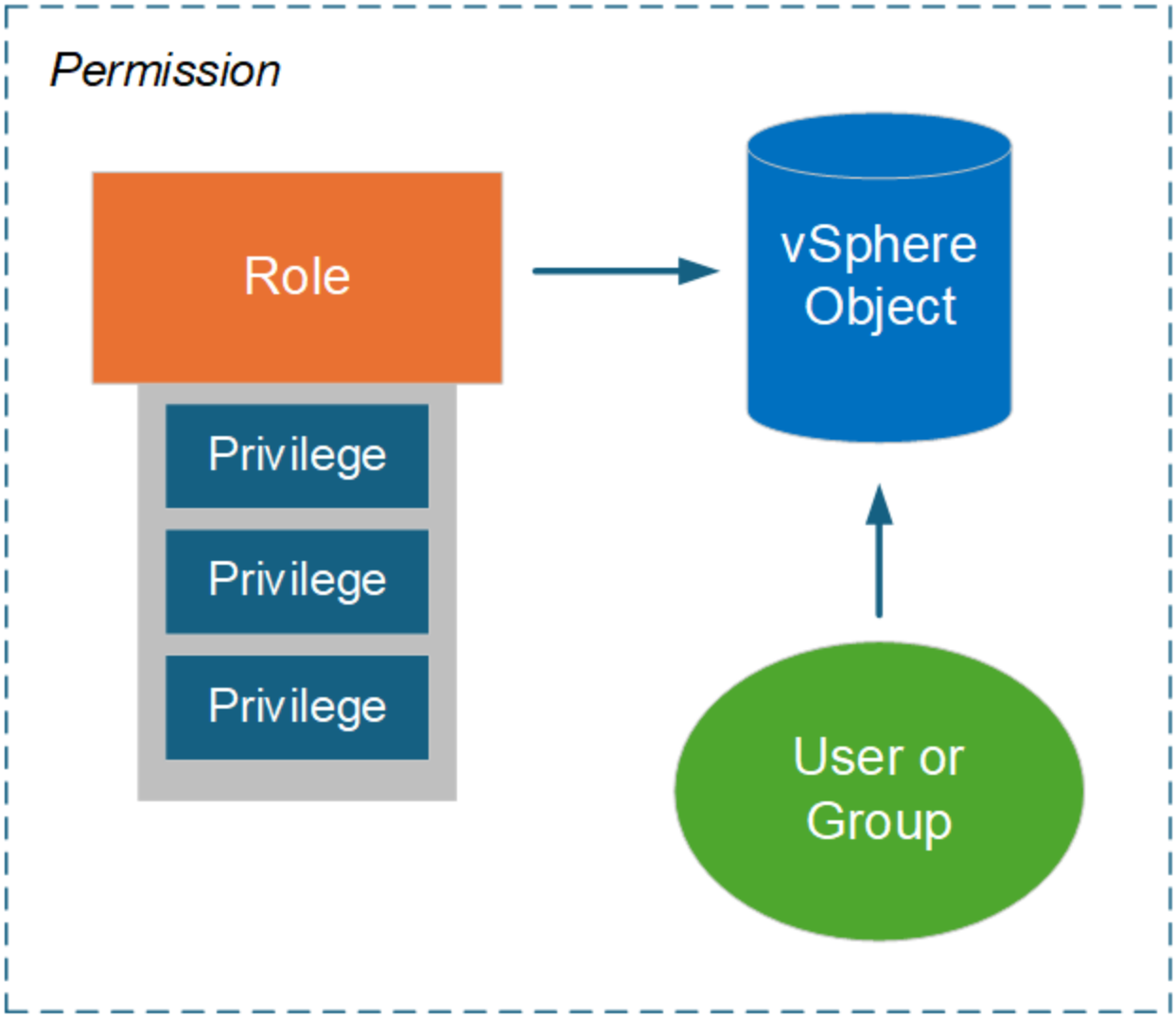
RBAC avec VMware vSphere

Environnement RBAC du serveur vCenter avec les outils ONTAP pour VMware vSphere 10

VMware vCenter Server propose une fonctionnalité RBAC qui vous permet de contrôler l'accès aux objets vSphere. Il s'agit d'une partie importante des services de sécurité d'authentification et d'autorisation centralisés vCenter.

Illustration d'une autorisation vCenter Server

Une autorisation est la base de l'application du contrôle d'accès dans l'environnement vCenter Server. Elle est appliquée à un objet vSphere avec un utilisateur ou un groupe inclus dans la définition des autorisations. Vous trouverez une illustration de haut niveau d'une autorisation vCenter dans la figure ci-dessous.



Composants d'une autorisation vCenter Server

Une autorisation vCenter Server est un ensemble de plusieurs composants qui sont liés ensemble lors de la création de l'autorisation.

Objets vSphere

Les autorisations sont associées aux objets vSphere, tels que vCenter Server, les hôtes ESXi, les machines virtuelles, les datastores, les data centers et les dossiers. En fonction des autorisations attribuées à l'objet, vCenter Server détermine les actions ou les tâches pouvant être effectuées sur l'objet par chaque utilisateur ou groupe. Pour les tâches spécifiques aux outils ONTAP pour VMware vSphere, toutes les autorisations sont attribuées et validées au niveau du dossier racine ou racine du serveur vCenter. Voir "Utilisez RBAC avec le serveur vCenter" pour plus d'informations.

Privileges et rôles

Deux types de vSphere Privileges sont utilisés avec les outils ONTAP pour VMware vSphere 10. Pour simplifier l'utilisation du contrôle d'accès basé sur des rôles dans cet environnement, les outils ONTAP fournissent les rôles contenant le Privileges natif et personnalisé requis. Le Privileges comprend :

- Privilèges de serveur vCenter natif

  Il s'agit du Privileges fourni par vCenter Server.

- Privilèges spécifiques aux outils ONTAP

  Il s'agit d'une solution Privileges personnalisée propre aux outils ONTAP pour VMware vSphere.

Utilisateurs et groupes

Vous pouvez définir des utilisateurs et des groupes à l'aide d'Active Directory ou de l'instance vCenter Server locale. Associé à un rôle, vous pouvez créer une autorisation sur un objet dans la hiérarchie d'objets vSphere. L'autorisation accorde l'accès en fonction du Privileges dans le rôle associé. Notez que les rôles ne sont pas attribués directement aux utilisateurs isolés. Les utilisateurs et les groupes peuvent accéder à un objet via le rôle Privileges, dans le cadre de l'autorisation serveur vCenter plus importante.

Utilisez vCenter Server RBAC avec les outils ONTAP pour VMware vSphere 10

Il existe plusieurs aspects des outils ONTAP pour l'implémentation de VMware vSphere 10 RBAC avec vCenter Server que vous devez prendre en compte avant de l'utiliser dans un environnement de production.

Rôles vCenter et compte administrateur

Vous n'avez besoin de définir et d'utiliser les rôles de serveur vCenter personnalisés que si vous souhaitez limiter l'accès aux objets vSphere et aux tâches administratives associées. Si la limitation de l'accès n'est pas nécessaire, vous pouvez utiliser un compte d'administrateur. Chaque compte administrateur est défini avec le rôle Administrateur au niveau supérieur de la hiérarchie des objets. Vous bénéficiez ainsi d'un accès complet aux objets vSphere, y compris ceux ajoutés par les outils ONTAP pour VMware vSphere 10.

Hiérarchie des objets vSphere

L'inventaire des objets vSphere est organisé dans une hiérarchie. Par exemple, vous pouvez déplacer la hiérarchie vers le bas comme suit :

`vCenter Server` → `Datacenter` → `Cluster` → `Virtual Machine` → `ESXi host`

Toutes les autorisations sont validées dans la hiérarchie des objets vSphere, à l'exception des opérations du plug-in VAAI, qui sont validées par rapport à l'hôte ESXi cible.

Rôles inclus avec les outils ONTAP pour VMware vSphere 10

Pour simplifier l'utilisation du RBAC de vCenter Server, les outils ONTAP pour VMware vSphere fournissent des rôles prédéfinis adaptés à diverses tâches d'administration.

> Vous pouvez créer de nouveaux rôles personnalisés si nécessaire. Dans ce cas, vous devez cloner l'un des rôles d'outils ONTAP existants et le modifier si nécessaire. Après avoir modifié la configuration, les utilisateurs du client vSphere concernés doivent se déconnecter et se reconnecter pour activer les modifications.

Pour afficher les outils ONTAP pour les rôles VMware vSphere, sélectionnez **Menu** en haut du client vSphere et cliquez sur **Administration**, puis sur **rôles** à gauche. Il existe trois rôles prédéfinis, comme décrit ci-dessous.

Outils NetApp ONTAP pour VMware vSphere Administrator

Fournit tous les outils vCenter Server Privileges natifs et ONTAP spécifiques Privileges requis pour effectuer les tâches d'administration des principaux outils ONTAP pour VMware vSphere.

Outils NetApp ONTAP pour VMware vSphere en lecture seule

Accès en lecture seule aux outils ONTAP. Ces utilisateurs ne peuvent pas exécuter d'actions ONTAP Tools for VMware vSphere contrôlées par accès.

Outils NetApp ONTAP pour le provisionnement VMware vSphere

Fournit certains privilèges vCenter Server natifs et certains privilèges spécifiques aux outils ONTAP requis pour provisionner le stockage. Vous pouvez effectuer les tâches suivantes :

- Créer de nouveaux datastores
- Gérer les datastores

Objets vSphere et systèmes back-end de stockage ONTAP

Les deux environnements RBAC fonctionnent ensemble. Lors de l'exécution d'une tâche dans l'interface client vSphere, les rôles des outils ONTAP définis pour vCenter Server sont vérifiés en premier. Si l'opération est autorisée par vSphere, le Privileges de rôle ONTAP est examiné. Cette deuxième étape est effectuée en fonction du rôle ONTAP attribué à l'utilisateur au moment de la création et de la configuration du back-end de stockage.

Utilisation de vCenter Server RBAC

Vous devez tenir compte de quelques éléments lorsque vous travaillez avec vCenter Server Privileges et les autorisations.

Privilèges requis

Pour accéder à l'interface utilisateur des outils ONTAP pour VMware vSphere 10, vous devez disposer du privilège *View* spécifique aux outils ONTAP. Si vous vous connectez à vSphere sans ce privilège et que vous cliquez sur l'icône NetApp, ONTAP Tools for VMware vSphere affiche un message d'erreur et vous empêche d'accéder à l'interface utilisateur.

Le niveau d'affectation dans la hiérarchie des objets vSphere détermine les parties de l'interface utilisateur auxquelles vous pouvez accéder. L'attribution du privilège d'affichage à l'objet racine vous permet d'accéder aux outils ONTAP pour VMware vSphere en cliquant sur l'icône NetApp.

Vous pouvez à la place attribuer le privilège d'affichage à un autre niveau d'objet vSphere inférieur. Toutefois, cela limite les menus des outils ONTAP pour VMware vSphere auxquels vous pouvez accéder et utiliser.

Attribution d'autorisations

Vous devez utiliser les autorisations vCenter Server si vous souhaitez limiter l'accès aux objets et aux tâches vSphere. Lorsque vous attribuez des autorisations dans la hiérarchie d'objets vSphere, les outils ONTAP pour les tâches VMware vSphere 10 peuvent être utilisés par les utilisateurs.

À moins que vous n'ayez besoin de définir un accès plus restrictif, il est généralement recommandé d'attribuer des autorisations au niveau de l'objet racine ou du dossier racine.

Les autorisations disponibles avec les outils ONTAP pour VMware vSphere 10 s'appliquent aux objets non vSphere personnalisés, tels que les systèmes de stockage. Si possible, vous devez attribuer ces autorisations

aux outils ONTAP pour l'objet racine VMware vSphere car il n'y a pas d'objet vSphere auquel vous pouvez l'affecter. Par exemple, toute autorisation qui inclut un privilège « Ajout/modification/Suppression de systèmes de stockage » des outils ONTAP pour VMware vSphere doit être attribuée au niveau de l'objet racine.

Lors de la définition d'une autorisation à un niveau supérieur dans la hiérarchie d'objets, vous pouvez configurer l'autorisation de sorte qu'elle soit transmise et héritée par les objets enfants. Si nécessaire, vous pouvez attribuer des autorisations supplémentaires aux objets enfants qui remplacent les autorisations héritées du parent.

Vous pouvez modifier une autorisation à tout moment. Si vous modifiez l'une des Privileges dans le cadre d'une autorisation, les utilisateurs associés à cette autorisation doivent se déconnecter de vSphere et se reconnecter pour activer la modification.

RBAC avec ONTAP

Environnement ONTAP RBAC avec les outils ONTAP pour VMware vSphere 10

ONTAP fournit un environnement RBAC robuste et extensible. Vous pouvez utiliser la fonctionnalité RBAC pour contrôler l'accès aux opérations du système et du stockage comme exposées via l'API REST et l'interface de ligne de commande. Il est utile de se familiariser avec l'environnement avant de l'utiliser avec les outils ONTAP pour le déploiement de VMware vSphere 10.

Présentation des options administratives

Plusieurs options sont disponibles lorsque vous utilisez ONTAP RBAC, en fonction de votre environnement et de vos objectifs. Un aperçu des principales décisions administratives est présenté ci-dessous. Voir également "Automatisation ONTAP : présentation de la sécurité RBAC" pour plus d'informations.

> ONTAP RBAC est adapté à un environnement de stockage et est plus simple que l'implémentation RBAC fournie avec vCenter Server. Avec ONTAP, vous attribuez un rôle directement à l'utilisateur. La configuration des autorisations explicites, telles que celles utilisées avec vCenter Server, n'est pas nécessaire avec ONTAP RBAC.

Types de rôles et de Privileges

Un rôle ONTAP est requis lors de la définition d'un utilisateur ONTAP. Il existe deux types de rôles ONTAP :

- REPOS

  Les rôles REST ont été introduits avec ONTAP 9.6 et sont généralement appliqués aux utilisateurs qui accèdent à ONTAP via l'API REST. Les Privileges incluses dans ces rôles sont définies en termes d'accès aux terminaux de l'API REST ONTAP et aux actions associées.

- Traditionnel

  Il s'agit des rôles hérités inclus avant ONTAP 9.6. Elles continuent d'être un aspect fondamental du RBAC. Les Privileges sont définies en termes d'accès aux commandes de l'interface de ligne de commandes ONTAP.

Alors que les AUTRES rôles ont été introduits plus récemment, les rôles traditionnels ont quelques avantages. Par exemple, des paramètres de requête supplémentaires peuvent être inclus de manière à ce que Privileges définisse plus précisément les objets auxquels ils sont appliqués.

Portée

Les rôles ONTAP peuvent être définis avec l'une des deux étendues différentes. Elles peuvent être appliquées à un SVM de données spécifique (niveau SVM) ou à l'ensemble du cluster ONTAP (niveau cluster).

Définitions de rôle

ONTAP fournit un ensemble de rôles prédéfinis au niveau du cluster et du SVM. Vous pouvez également définir des rôles personnalisés.

Utilisation des rôles REST ONTAP

Plusieurs considérations sont à prendre en compte lors de l'utilisation des rôles REST ONTAP inclus dans les outils ONTAP pour VMware vSphere 10.

Mappage de rôles

Que vous utilisiez un rôle classique ou REST, toutes les décisions d'accès à ONTAP sont basées sur la commande de l'interface de ligne de commande sous-jacente. Mais comme le Privileges dans un rôle REST est défini en termes de terminaux d'API REST, ONTAP doit créer un rôle *mappé* traditionnel pour chacun des rôles REST. Par conséquent, chaque rôle REST est associé à un rôle traditionnel sous-jacent. ONTAP peut ainsi prendre des décisions de contrôle d'accès de manière cohérente, quel que soit le type de rôle. Vous ne pouvez pas modifier les rôles mappés en parallèle.

Définition d'un rôle REST à l'aide de l'interface de ligne de commande Privileges

Comme ONTAP utilise toujours les commandes de l'interface de ligne de commande pour déterminer l'accès au niveau de base, il est possible d'exprimer un rôle REST en utilisant la commande de l'interface de ligne de commande Privileges à la place des terminaux REST. L'un des avantages de cette approche est la granularité supplémentaire disponible avec les rôles traditionnels.

Interface d'administration lors de la définition des rôles ONTAP

Vous pouvez créer des utilisateurs et des rôles à l'aide de l'interface de ligne de commandes et de l'API REST de ONTAP. Cependant, il est plus pratique d'utiliser l'interface System Manager et le fichier JSON disponible via le gestionnaire d'outils ONTAP. Voir "Utilisez ONTAP RBAC avec les outils ONTAP pour VMware vSphere 10" pour plus d'informations.

Utilisez ONTAP RBAC avec les outils ONTAP pour VMware vSphere 10

Il existe plusieurs aspects des outils ONTAP pour l'implémentation de VMware vSphere 10 RBAC avec ONTAP que vous devez prendre en compte avant de l'utiliser dans un environnement de production.

Présentation du processus de configuration

Les outils ONTAP pour VMware vSphere 10 incluent la prise en charge de la création d'un utilisateur ONTAP avec un rôle personnalisé. Ces définitions sont fournies dans un fichier JSON que vous pouvez télécharger vers le cluster ONTAP. Vous pouvez créer l'utilisateur et adapter le rôle à vos besoins en matière d'environnement et de sécurité.

Les principales étapes de configuration sont décrites ci-dessous à un niveau élevé. Voir "Configurer les rôles et privilèges des utilisateurs ONTAP"pour plus de détails.

1. Préparation

Vous devez disposer d'informations d'identification d'administration pour le gestionnaire d'outils ONTAP et le cluster ONTAP.

2. Téléchargez le fichier de définition JSON

Une fois connecté à l'interface utilisateur du Gestionnaire d'outils ONTAP, vous pouvez télécharger le fichier JSON contenant les définitions RBAC.

3. Créez un utilisateur ONTAP avec un rôle

Une fois connecté à System Manager, vous pouvez créer l'utilisateur et le rôle :

1. Sélectionnez **Cluster** sur la gauche, puis **Settings**.
2. Faites défiler jusqu'à **utilisateurs et rôles** et cliquez sur −→.
3. Sélectionnez **Ajouter** sous **utilisateurs** et sélectionnez **produits de virtualisation**.
4. Sélectionnez le fichier JSON sur votre poste de travail local et chargez-le.

4. Configurez le rôle

Dans le cadre de la définition du rôle, vous devez prendre plusieurs décisions administratives. Voir Configurez le rôle à l'aide de System Manager pour plus de détails.

Configurez le rôle à l'aide de System Manager

Une fois que vous avez commencé à créer un utilisateur et un rôle avec System Manager et que vous avez téléchargé le fichier JSON, vous pouvez personnaliser le rôle en fonction de votre environnement et de vos besoins.

Configuration de l'utilisateur principal et du rôle

Les définitions RBAC sont packagées sous la forme de plusieurs fonctionnalités, dont une combinaison de VSC, VASA Provider et SRA. Vous devez sélectionner l'environnement ou les environnements dans lesquels vous avez besoin de la prise en charge de RBAC. Par exemple, si vous souhaitez que les rôles prennent en charge la fonctionnalité de plug-in à distance, sélectionnez VSC. Vous devez également choisir le nom d'utilisateur et le mot de passe associé.

Privilèges

Les Privileges de rôle sont organisés en quatre ensembles en fonction du niveau d'accès requis au stockage ONTAP. Le Privileges sur lequel sont basés les rôles comprend :

- Détection

  Il permet donc d'ajouter des systèmes de stockage.

- Créer du stockage

  Grâce à ce rôle, vous pouvez créer du stockage. Il inclut également toutes les Privileges associées au rôle de découverte.

- Modifier le stockage

  Ce rôle vous permet de modifier le stockage. Il inclut également toutes les Privileges associées à la détection et crée des rôles de stockage.

- Détruire le stockage

  Vous pouvez ainsi détruire le stockage. Elle inclut également toutes les Privileges associées à la détection, la création du stockage et la modification des rôles de stockage.

Générer l’utilisateur avec un rôle

Après avoir sélectionné les options de configuration pour votre environnement, cliquez sur **Ajouter** et ONTAP crée l’utilisateur et le rôle. Le nom du rôle généré est une concaténation des valeurs suivantes :

- Valeur de préfixe constante définie dans le fichier JSON (par exemple « OTV_10 »)
- Fonctionnalité de produit que vous avez sélectionnée
- Liste des jeux de privilèges.

Exemple

```
OTV_10_VSC_Discovery_Create
```

Le nouvel utilisateur sera ajouté à la liste de la page "utilisateurs et rôles". Notez que les méthodes de connexion utilisateur HTTP et ONTAPI sont prises en charge.

Informations sur le copyright

Informations sur les marques commerciales