

Administration d'Architecture Cloud Pod dans Horizon 7

MAR 2020

VMware Horizon 7 7.12

Vous trouverez la documentation technique la plus récente sur le site Web de VMware, à l'adresse :

<https://docs.vmware.com/fr/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

Copyright © 2020 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

Table des matières

Administration d'Architecture Cloud Pod dans Horizon 7 6

1 Présentation de Architecture Cloud Pod 7

- Présentation de Architecture Cloud Pod 7
 - Partage des données clés dans la couche de données globale 8
 - Envoi de messages entre des espaces 8
- Configuration et gestion d'un environnement Architecture Cloud Pod 9
- Limitations de Architecture Cloud Pod 9

2 Conception d'une topologie Architecture Cloud Pod 10

- Création de sites Architecture Cloud Pod 11
- Octroi de droits d'accès à des utilisateurs et à des groupes d'une fédération d'espaces 11
- Recherche et allocation de postes de travail et d'applications dans une fédération d'espaces 12
 - Présentation de la stratégie d'étendue 13
 - Comprendre la stratégie de sessions multiples par utilisateur pour les droits de poste de travail globaux 13
 - Utilisation des sites de base 13
- Considérations pour les utilisateurs non authentifiés 14
- Exemple de droit d'accès global 15
- Mise en œuvre des restrictions du Serveur de connexion pour les droits d'accès globaux 16
 - Correspondance de balise 16
 - Exigences et limitations pour les restrictions du Serveur de connexion 17
 - Exemple de restrictions du Serveur de connexion 18
- Mise en œuvre des restrictions du client pour les droits d'accès globaux 19
- Implémentation de la fonctionnalité de pré-lancement de session pour les droits d'application globaux 20
- Activation du mode de sessions multiples pour les droits applicatifs globaux 20
- Activation de la collaboration de session pour les droits de poste de travail globaux 21
- Implémentation des droits globaux de sauvegarde 22
- Éléments à prendre en compte pour les environnements hétérogènes 23
- Remarques relatives au mode Workspace ONE 23
- Considérations relatives à VMware Cloud on AWS 23
- Considérations relatives aux licences d'accès client aux services RDS par terminal 24
- Limites de la topologie Architecture Cloud Pod 24
- Configuration requise des ports pour Architecture Cloud Pod 25
- Considérations liées à la sécurité des topologies Architecture Cloud Pod 25

3 Configuration de Architecture Cloud Pod dans Horizon Console 27

Initialiser la fonctionnalité Architecture Cloud Pod dans Horizon Console	28
Joindre un espace à la fédération d'espaces dans Horizon Console	28
Affecter une balise à une instance du Serveur de connexion dans Horizon Console	30
Configuration des raccourcis pour les droits d'accès globaux	30
Feuille de calcul pour la configuration d'un droit d'accès global	32
Créer et configurer un droit global dans Horizon Console	38
Ajouter un pool à un droit global dans Horizon Console	40
Créer et configurer un site dans Horizon Console	41
Attribuer un site de base à un utilisateur ou à un groupe dans Horizon Console	42
Créer un remplacement du site de base dans Horizon Console	43
Tester une configuration d'Architecture Cloud Pod dans Horizon Client	44
Exemple : Paramétrage d'une configuration Architecture Cloud Pod de base	44
Conception de l'exemple de topologie	46
Initialisation de l'exemple de configuration	46
Jonction d'espaces dans l'exemple de configuration	47
Création de sites dans l'exemple de configuration	47
Création de droits de poste de travail globaux dans l'exemple de configuration	48
Création d'une URL pour l'exemple de configuration	49

4 Gestion d'un environnement Architecture Cloud Pod dans Horizon Console 50

Afficher une configuration d'Architecture Cloud Pod dans Horizon Console	50
Afficher l'intégrité d'une fédération d'espaces dans Horizon Console	52
Afficher les sessions de postes de travail et d'applications dans Horizon Console	53
Gestion des sites dans Horizon Console	55
Ajouter un espace à un site dans Horizon Console	55
Supprimer un site dans Horizon Console	55
Modifier un nom ou une description de site dans Horizon Console	56
Gestion des droits globaux dans Horizon Console	56
Supprimer un pool d'un droit global dans Horizon Console	56
Ajouter un utilisateur ou un groupe à un droit global dans Horizon Console	56
Supprimer un utilisateur ou un groupe d'un droit global dans Horizon Console	57
Modifier les attributs ou les stratégies d'un droit global dans Horizon Console	57
Supprimer un droit global dans Horizon Console	58
Gestion des sites de base dans Horizon Console	58
Modifier une attribution de site de base dans Horizon Console	59
Supprimer une attribution de site de base dans Horizon Console	59
Déterminer le site de base effectif d'un utilisateur dans Horizon Console	59
Modifier le remplacement du site de base dans Horizon Console	60
Supprimer le remplacement du site de base dans Horizon Console	60
Supprimer un espace de la fédération d'espaces dans Horizon Console	61
Annuler l'initialisation de la fonctionnalité Architecture Cloud Pod dans Horizon Console	61

5 Administration d'Architecture Cloud Pod avec Imvutil 63

Utilisation de la commande Imvutil	63
Authentification de la commande Imvutil	64
Sortie de la commande Imvutil	64
Options de la commande Imvutil	65
Initialisation de la fonctionnalité Architecture Cloud Pod.	67
Désactivation de la fonctionnalité Architecture Cloud Pod	68
Gestion d'une fédération d'espaces	69
Jonction d'un espace à la fédération d'espaces	69
Suppression d'un espace d'une fédération d'espaces	70
Modification du nom ou de la description d'un espace	70
Gestion des sites	71
Création d'un site	72
Affectation d'un espace à un site	72
Modification du nom ou de la description d'un site	73
Suppression d'un site	73
Gestion des droits d'accès globaux	74
Création d'un droit d'accès global	75
Modification d'un droit d'accès global	79
Suppression d'un droit d'accès global	83
Ajout d'un pool à un droit d'accès global	84
Suppression d'un pool d'un droit d'accès global	85
Ajout d'un utilisateur ou d'un groupe à un droit d'accès global	86
Suppression d'un utilisateur ou d'un groupe d'un droit global	87
Gestion des sites de base	88
Configuration d'un site de base	88
Suppression d'un site de base	89
Affichage d'une configuration Architecture Cloud Pod	90
Affichage de la liste des droits d'accès globaux	91
Affichage de la liste des pools d'un droit d'accès global	91
Affichage de la liste des utilisateurs ou des groupes d'un droit d'accès global	92
Affichage de la liste des sites de base d'un utilisateur ou d'un groupe	93
Affichage du site de base effectif d'un utilisateur	94
Affichage de la liste des attributions de pool de postes de travail dédiés	94
Affichage de la liste des espaces ou des sites dans une topologie Architecture Cloud Pod	95
Gestion des certificats SSL	96
Création d'un certificat en attente	96
Activation d'un certificat en attente	97

Administration d'Architecture Cloud Pod dans Horizon 7

Administration d'Architecture Cloud Pod dans Horizon 7 décrit comment configurer et gérer un environnement Architecture Cloud Pod dans VMware Horizon[®] 7.

Public cible

Ce document est destiné à des administrateurs système Windows ou Linux expérimentés familiarisés avec la technologie de machine virtuelle et les opérations de centre de données.

Présentation de Architecture Cloud Pod

1

La fonctionnalité Architecture Cloud Pod utilise les composants standard d'Horizon pour fournir l'administration de plusieurs centres de données, une correspondance globale et flexible des utilisateurs avec les postes de travail à haute disponibilité et des fonctionnalités de récupération d'urgence.

Ce chapitre contient les rubriques suivantes :

- [Présentation de Architecture Cloud Pod](#)
- [Configuration et gestion d'un environnement Architecture Cloud Pod](#)
- [Limitations de Architecture Cloud Pod](#)

Présentation de Architecture Cloud Pod

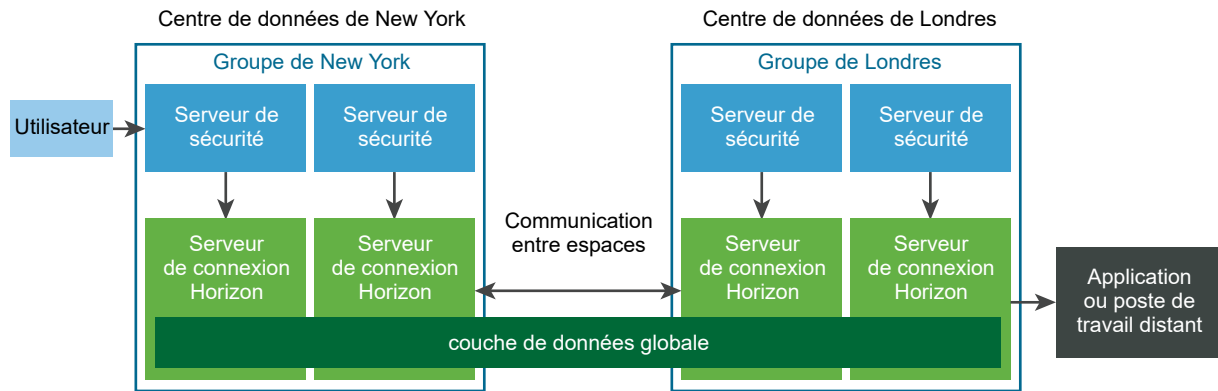
Avec la fonctionnalité Architecture Cloud Pod, vous pouvez lier plusieurs espaces ensemble afin de fournir un environnement unique et volumineux d'échange et de gestion de postes de travail et d'applications.

Un espace se compose d'un ensemble d'instances de Serveur de connexion, d'un stockage partagé, d'un serveur de base de données et des infrastructures vSphere et réseau requises pour héberger les pools de postes de travail et d'applications. Dans une implémentation Horizon traditionnelle, vous gérez chaque espace indépendamment. Avec la fonctionnalité Architecture Cloud Pod, vous pouvez joindre plusieurs espaces ensemble pour former une implémentation Horizon unique appelée fédération d'espaces.

Une fédération d'espaces peut s'étendre sur plusieurs sites et centres de données et ainsi simplifier l'effort d'administration requis pour gérer un déploiement d'Horizon à grande échelle.

Le graphique suivant présente un exemple d'une topologie Architecture Cloud Pod de base.

Figure 1-1. Topologie Architecture Cloud Pod de base



Dans l'exemple de topologie, deux espaces précédemment autonomes dans différents centres de données sont joints pour former une fédération d'espaces unique. Un utilisateur final de cet environnement peut se connecter à une instance du Serveur de connexion dans le centre de données de New York et recevoir un poste de travail ou une application dans le centre de données de Londres.

Partage des données clés dans la couche de données globale

Les instances du Serveur de connexion dans une fédération d'espaces utilisent la couche de données globale pour partager des données clés. Les données partagées incluent des informations sur la topologie de la fédération d'espaces, sur les droits d'accès d'utilisateur et de groupe, sur les stratégies, ainsi que d'autres informations de configuration Architecture Cloud Pod.

Dans un environnement Architecture Cloud Pod, les données partagées sont répliquées sur chaque instance du Serveur de connexion dans une fédération d'espaces. Les informations de configuration de droit d'accès et de topologie stockées dans la couche de données globale déterminent où et comment les postes de travail sont alloués dans la fédération d'espaces.

Horizon configure la couche de données globale sur chaque instance du Serveur de connexion dans une fédération d'espaces lorsque vous initialisez la fonctionnalité Architecture Cloud Pod.

Envoi de messages entre des espaces

Les instances du Serveur de connexion communiquent dans un environnement Architecture Cloud Pod à l'aide d'un protocole de communication entre espaces appelé VIPA (View InterPod API).

Les instances du Serveur de connexion utilisent le canal de communication VIPA pour lancer de nouveaux postes de travail, rechercher des postes de travail existants et partager des données d'état de santé ainsi que d'autres informations. Horizon configure le canal de communication VIPA lorsque vous initialisez la fonctionnalité Architecture Cloud Pod.

Configuration et gestion d'un environnement Architecture Cloud Pod

Vous utilisez Horizon Console ou l'interface de ligne de commande `lmvutil` pour configurer et gérer un environnement Architecture Cloud Pod. `lmvutil` est installé au cours de l'installation d'Horizon. Vous pouvez également utiliser Horizon Console pour afficher l'intégrité de l'espace et les informations de session.

Limitations de Architecture Cloud Pod

La fonctionnalité Architecture Cloud Pod comporte certaines restrictions.

- La fonction Architecture Cloud Pod n'est pas prise en charge dans un environnement IPv6.
- Les clients en mode kiosque ne sont pas pris en charge dans une implémentation d'Architecture Cloud Pod, sauf si vous implémentez une solution. Pour plus d'instructions, consultez l'article [2148888](#) de la base de connaissances de VMware.

Conception d'une topologie Architecture Cloud Pod

2

Avant de configurer la fonctionnalité Architecture Cloud Pod, vous devez prendre des décisions concernant votre topologie Architecture Cloud Pod. Les topologies Architecture Cloud Pod peuvent varier en fonction de vos objectifs, des besoins de vos utilisateurs et de votre implémentation existante d'Horizon. Si vous joignez des espaces Horizon existants à une fédération d'espaces, votre topologie Architecture Cloud Pod est généralement basée sur votre topologie réseau existante.

Ce chapitre contient les rubriques suivantes :

- [Création de sites Architecture Cloud Pod](#)
- [Octroi de droits d'accès à des utilisateurs et à des groupes d'une fédération d'espaces](#)
- [Recherche et allocation de postes de travail et d'applications dans une fédération d'espaces](#)
- [Considérations pour les utilisateurs non authentifiés](#)
- [Exemple de droit d'accès global](#)
- [Mise en œuvre des restrictions du Serveur de connexion pour les droits d'accès globaux](#)
- [Mise en œuvre des restrictions du client pour les droits d'accès globaux](#)
- [Implémentation de la fonctionnalité de pré-lancement de session pour les droits d'application globaux](#)
- [Activation du mode de sessions multiples pour les droits applicatifs globaux](#)
- [Activation de la collaboration de session pour les droits de poste de travail globaux](#)
- [Implémentation des droits globaux de sauvegarde](#)
- [Éléments à prendre en compte pour les environnements hétérogènes](#)
- [Remarques relatives au mode Workspace ONE](#)
- [Considérations relatives à VMware Cloud on AWS](#)
- [Considérations relatives aux licences d'accès client aux services RDS par terminal](#)
- [Limites de la topologie Architecture Cloud Pod](#)
- [Configuration requise des ports pour Architecture Cloud Pod](#)

■ Considérations liées à la sécurité des topologies Architecture Cloud Pod

Création de sites Architecture Cloud Pod

Dans un environnement Architecture Cloud Pod, un site est un ensemble d'espaces bien connectés situés dans un même emplacement physique, généralement un centre de données unique. La fonctionnalité Architecture Cloud Pod traite tous les espaces d'un même site de la même manière.

Lorsque vous initialisez la fonctionnalité Architecture Cloud Pod, celle-ci place tous les espaces dans un site par défaut nommé Premier site par défaut. Si vous disposez d'une implémentation de grande taille, vous pouvez créer des sites supplémentaires pour y ajouter des espaces.

La fonctionnalité Architecture Cloud Pod part du principe que les espaces d'un même site se trouvent sur le même réseau local, et que les espaces de sites différents se trouvent sur des réseaux locaux différents. Dans la mesure où les espaces connectés à un réseau étendu ont des performances réseau plus lentes, la fonctionnalité Architecture Cloud Pod privilégie les postes de travail et les applications qui se trouvent dans l'espace ou le site local lorsqu'elle alloue des postes de travail et des applications aux utilisateurs.

Les sites peuvent être un élément utile d'une solution de récupération d'urgence. Par exemple, vous pouvez affecter des espaces de différents centres de données à différents sites, puis autoriser des utilisateurs et des groupes à accéder à des pools qui se trouvent sur ces sites. Si un centre de données d'un site devient indisponible, vous pouvez utiliser les postes de travail et les applications du site disponible afin de répondre aux demandes des utilisateurs.

Octroi de droits d'accès à des utilisateurs et à des groupes d'une fédération d'espaces

Dans un environnement Horizon traditionnel, vous utilisez Horizon Console pour créer des droits locaux. Ces droits locaux autorisent des utilisateurs et des groupes à accéder à un pool de postes de travail ou d'applications spécifique sur une instance du Serveur de connexion.

Dans un environnement Architecture Cloud Pod, vous créez des droits d'accès globaux pour autoriser des utilisateurs ou des groupes à accéder à plusieurs postes de travail ou applications dans plusieurs espaces d'une fédération d'espaces. Lorsque vous utilisez des droits d'accès globaux, vous n'avez pas besoin de configurer et de gérer les droits d'accès locaux. Les droits d'accès globaux simplifient l'administration, même dans une fédération d'espaces qui ne contient qu'un seul espace.

Les droits globaux sont stockés dans la couche de données globale. Dans la mesure où les droits globaux sont des données partagées, les informations les concernant sont disponibles sur toutes les instances du Serveur de connexion de la fédération d'espaces.

Vous autorisez des utilisateurs et des groupes à accéder à des postes de travail en créant des droits de poste de travail globaux. Chaque droit de poste de travail global contient une liste des utilisateurs ou des groupes membres, une liste des pools de postes de travail pouvant fournir des postes de travail aux utilisateurs autorisés et une stratégie d'étendue. Les pools de postes de travail d'un droit d'accès global peuvent être des pools flottants ou dédiés. C'est vous qui spécifiez si un droit d'accès global est flottant ou dédié lors de la création des droits d'accès globaux.

Vous autorisez des utilisateurs et des groupes à accéder à des applications en créant des droits d'application globaux. Chaque droit d'application global contient une liste des utilisateurs ou des groupes membres, une liste des pools d'applications pouvant fournir des applications aux utilisateurs autorisés et une stratégie d'étendue.

La stratégie d'étendue d'un droit global spécifie l'emplacement dans lequel Horizon recherche les postes de travail ou applications lorsqu'il alloue des postes de travail ou des applications aux utilisateurs de ce droit global. Elle détermine également si Horizon doit rechercher des postes de travail ou des applications dans n'importe quel espace de la fédération d'espaces, dans des espaces résidant sur le même site ou uniquement dans l'espace auquel l'utilisateur est connecté.

Nous vous recommandons de ne pas configurer les droits d'accès locaux et globaux dans un même pool de postes de travail. Par exemple, si vous créez des droits d'accès locaux et globaux dans le même pool de postes de travail, le même poste de travail peut figurer en tant que droit d'accès local et global dans la liste des postes de travail et des applications qu'Horizon Client présente à l'utilisateur autorisé. De la même façon, vous ne devez pas configurer des droits d'accès locaux et globaux pour des pools d'applications créés à partir de la même batterie de serveurs.

Recherche et allocation de postes de travail et d'applications dans une fédération d'espaces

Dans un environnement Architecture Cloud Pod, les instances du Serveur de connexion utilisent les informations de configuration partagées de la couche de données globale concernant les droits globaux et la topologie pour déterminer où effectuer une recherche et comment allouer des postes de travail et des applications dans une fédération d'espaces.

Lorsqu'un utilisateur demande un poste de travail ou une application à partir d'un droit global, Horizon recherche un poste de travail ou une application disponible dans les pools associés à ce droit global. Par défaut, Horizon donne la préférence d'abord à l'espace local, puis au site local et enfin aux espaces des autres sites.

Pour les droits de poste de travail globaux contenant des pools de postes de travail dédiés, Horizon utilise uniquement le comportement de recherche par défaut la première fois qu'un utilisateur demande un poste de travail. Dès qu'Horizon a alloué un poste de travail dédié, il renvoie l'utilisateur directement à ce même poste de travail.

Vous pouvez modifier le comportement de recherche et d'allocation pour des droits d'accès globaux individuels en définissant la stratégie d'étendue et en configurant les sites de base.

Présentation de la stratégie d'étendue

Lorsque vous créez un droit de poste de travail global ou un droit d'application global, vous devez spécifier sa stratégie d'étendue. La stratégie d'étendue détermine l'étendue de la recherche lorsqu'Horizon recherche des postes de travail ou des applications pour satisfaire une demande du droit global.

Vous pouvez définir la stratégie d'étendue pour qu'Horizon recherche uniquement dans l'espace auquel l'utilisateur est connecté, uniquement dans les espaces se trouvant sur le même site que l'espace de l'utilisateur ou dans tous les espaces de la fédération d'espaces.

Pour les droits de poste de travail globaux qui contiennent des pools dédiés, la stratégie d'étendue détermine l'emplacement dans lequel Horizon recherche des postes de travail la première fois qu'un utilisateur demande un poste de travail dédié. Dès qu'Horizon a alloué un poste de travail dédié, il renvoie l'utilisateur directement à ce même poste de travail.

Comprendre la stratégie de sessions multiples par utilisateur pour les droits de poste de travail globaux

Lorsque vous créez un droit de poste de travail global, vous pouvez spécifier si des utilisateurs peuvent initier des sessions de poste de travail distinctes à partir de périphériques clients différents. La stratégie de sessions multiples par utilisateur ne s'applique qu'aux droits de poste de travail globaux qui contiennent des pools de postes de travail flottants.

Lorsque vous activez la stratégie de sessions multiples par utilisateur, les utilisateurs qui se connectent au droit de poste de travail global depuis différents périphériques clients reçoivent des sessions de poste de travail différentes. Pour se reconnecter à une session de poste de travail existante, les utilisateurs doivent utiliser le périphérique sur lequel cette session a été initiée. Si vous n'activez pas cette stratégie, les utilisateurs sont toujours reconnectés à leurs sessions de poste de travail existantes, quel que soit le périphérique client qu'ils utilisent.

Si vous activez la stratégie de sessions multiples par utilisateur pour un droit de poste de travail global, tous les pools de postes de travail associés au droit de poste de travail global doivent également prendre en charge plusieurs utilisateurs par session.

Utilisation des sites de base

Un site de base correspond à une relation existant entre un utilisateur ou un groupe et un site Architecture Cloud Pod. Avec les sites de base, Horizon effectue une recherche des postes de travail et des applications sur un site spécifique plutôt qu'une recherche basée sur l'emplacement actuel de l'utilisateur.

Si le site de base n'est pas disponible ou n'a pas de ressources pour satisfaire la demande de l'utilisateur, Horizon continue de rechercher d'autres sites en fonction de la stratégie d'étendue définie pour le droit global.

Pour les droits de poste de travail globaux qui contiennent des pools dédiés, le site de base détermine l'emplacement dans lequel Horizon recherche des postes de travail la première fois qu'un utilisateur demande un poste de travail dédié. Dès qu'Horizon a alloué un poste de travail dédié, il renvoie l'utilisateur directement à ce même poste de travail.

La fonctionnalité Architecture Cloud Pod inclut les types suivants d'attributions de sites de base.

Site de base global

Un site de base affecté à un utilisateur ou un groupe.

Si un utilisateur qui dispose d'un site de base appartient à un groupe associé à un autre site de base, le site de base associé à l'utilisateur a priorité sur l'attribution du site de base du groupe.

Les sites de base globaux sont utiles pour contrôler l'emplacement dans lequel les utilisateurs itinérants reçoivent des postes de travail et des applications. Par exemple, si un utilisateur a un site de base à New York, mais se trouve actuellement à Londres, Horizon commence à rechercher sur le site de New York pour répondre à la demande de poste de travail de l'utilisateur plutôt que d'allouer un poste de travail situé à proximité de l'utilisateur. Les attributions de sites de base globaux s'appliquent à tous les droits d'accès globaux.

Important Les droits d'accès globaux ne reconnaissent pas les sites de base par défaut. Pour faire en sorte qu'un droit d'accès global utilise des sites de base, vous devez sélectionner l'option **Utiliser le site d'accueil** lors de la création ou de la modification du droit d'accès global.

Site de base par droit global (remplacement du site de base)

Un site de base associé à un droit d'accès global.

Les sites de base par droit global remplacent les attributions de sites de base globaux. Pour cette raison, les sites de base par droit global sont également appelés remplacements du site de base.

Par exemple, si un utilisateur qui a un site de base à New York accède à un droit global qui associe cet utilisateur au site de base de Londres, Horizon commence à rechercher sur le site de Londres pour répondre à la demande d'application de l'utilisateur plutôt que d'allouer une application à partir du site de New York.

La configuration de sites de base est facultative. Si un utilisateur ne dispose pas d'un site de base, Horizon recherche et alloue des postes de travail et des applications de la manière décrite dans [Recherche et allocation de postes de travail et d'applications dans une fédération d'espaces](#).

Considérations pour les utilisateurs non authentifiés

Un administrateur Horizon peut créer des utilisateurs pour un accès non authentifié à des applications publiées sur une instance du Serveur de connexion. Dans un environnement

Architecture Cloud Pod, vous pouvez autoriser ces utilisateurs non authentifiés à accéder à des applications dans la fédération d'espaces en les ajoutant à des droits d'application globaux.

Voici les considérations pour les utilisateurs non authentifiés dans un environnement Architecture Cloud Pod.

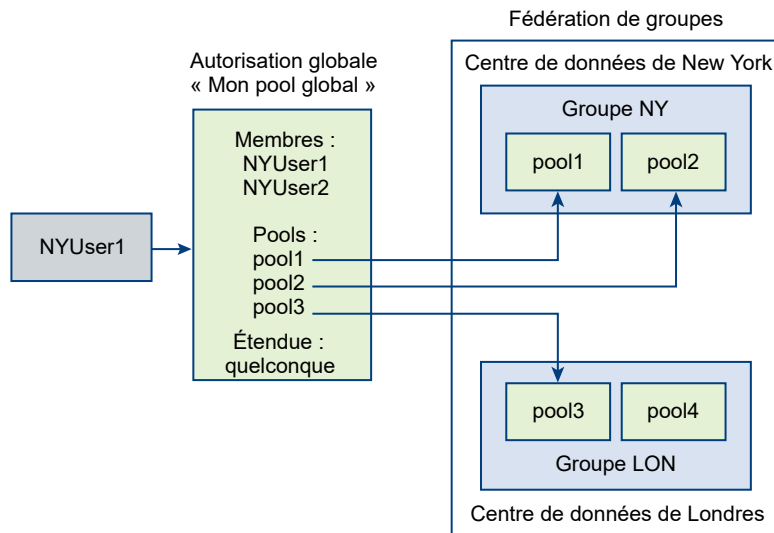
- Les utilisateurs non authentifiés ne peuvent disposer que de droits d'application globaux. Si un utilisateur non authentifié est inclus dans un droit de poste de travail global, une icône d'avertissement s'affiche en regard du nom dans l'onglet **Utilisateurs et groupes** du droit de poste de travail global dans Horizon Console.
- Lorsque vous joignez un espace à la fédération d'espaces, les données des utilisateurs non authentifiés sont migrées vers la couche de données globale. Si vous annulez la jonction ou éjectez un espace qui contient des utilisateurs non authentifiés de la fédération d'espaces, les données des utilisateurs non authentifiés pour cet espace sont supprimées de la couche de données globale.
- Vous ne pouvez avoir qu'un seul utilisateur non authentifié pour chaque utilisateur Active Directory. Si le même alias d'utilisateur est mappé à plusieurs utilisateurs Active Directory, Horizon Console affiche un message d'erreur dans l'onglet **Accès non authentifié** dans le volet Utilisateurs et groupes.
- Vous pouvez attribuer des sites de base à des utilisateurs non authentifiés.
- Les utilisateurs non authentifiés peuvent disposer de plusieurs sessions.
- Les utilisateurs d'accès non authentifiés ne sont pas autorisés à accéder aux droits d'application globaux prévoyant la publication des applications à partir d'un pool de postes de travail.

Pour plus d'informations sur la configuration des utilisateurs non authentifiés, consultez le document *Administration d'Horizon 7*.

Exemple de droit d'accès global

Dans cet exemple, NYUser1 est membre du droit de poste de travail global nommé My Global Pool (Mon pool global). Mon pool global fournit un droit d'accès à trois pools de postes de travail flottants, appelés pool1, pool2 et pool3. pool1 et pool2 se trouvent dans un espace nommé NY Pod dans le centre de données New York et pool3 et pool4 sont situés dans un espace appelé LDN Pod dans le centre de données Londres.

Figure 2-1. Exemple de droit global



Étant donné que My Global Pool a une stratégie d'étendue ANY, la fonctionnalité Architecture Cloud Pod recherche des postes de travail dans NY Pod et LDN Pod lorsque NYUser1 demande un poste de travail. La fonctionnalité Architecture Cloud Pod ne tente pas d'allouer un poste de travail à partir de pool4, car pool4 ne fait pas partie de My Global Pool.

Si NYUser1 se connecte à NY Pod, la fonctionnalité Architecture Cloud Pod alloue un poste de travail à partir de pool1 ou de pool2, si un poste est disponible. Si aucun poste de travail n'est disponible dans pool1 ou pool2, la fonctionnalité Architecture Cloud Pod alloue un poste de travail à partir de pool3.

Pour voir un exemple de droits globaux limités, consultez [Exemple de restrictions du Serveur de connexion](#).

Mise en œuvre des restrictions du Serveur de connexion pour les droits d'accès globaux

Vous pouvez limiter l'accès aux droits globaux en fonction de l'instance du Serveur de connexion à laquelle les utilisateurs se connectent au départ lorsqu'ils sélectionnent des droits globaux.

La fonctionnalité de restrictions du Serveur de connexion vous permet d'attribuer une ou plusieurs balises à une instance du Serveur de connexion. Ensuite, lorsque vous configurez un droit global, vous spécifiez les balises des instances du Serveur de connexion que vous voulez rendre capables d'accéder au droit global.

Vous pouvez ajouter des balises à des droits de poste de travail globaux et à des droits d'application globaux.

Correspondance de balise

La fonctionnalité de restrictions du Serveur de connexion utilise la correspondance de balise pour déterminer si une instance du Serveur de connexion peut accéder à un droit global particulier.

Au niveau le plus basique, la correspondance de balise détermine qu'une instance du Serveur de connexion avec une balise spécifique peut accéder à un droit global qui a la même balise.

L'absence d'attributions de balise peut également avoir une incidence sur la possibilité ou non des utilisateurs qui se connectent à une instance du Serveur de connexion d'accéder à un droit global. Par exemple, des instances du Serveur de connexion qui ne contiennent aucune balise ne peuvent accéder qu'à des droits globaux qui ne contiennent aucune balise.

Tableau 2-1. Règles de correspondance de balise indique comment la correspondance de balise détermine le moment où une instance du Serveur de connexion peut accéder à un droit global.

Tableau 2-1. Règles de correspondance de balise

Serveur de connexion	Autorisation globale	Accès autorisé ?
Pas de balise	Pas de balise	Oui
Pas de balise	Une ou plusieurs balises	Non
Une ou plusieurs balises	Pas de balise	Oui
Une ou plusieurs balises	Une ou plusieurs balises	Uniquement quand les balises correspondent

La fonctionnalité de restrictions du Serveur de connexion applique uniquement la correspondance de balise. Vous devez concevoir votre topologie de réseau pour forcer certains clients à se connecter via une instance du Serveur de connexion particulière.

Exigences et limitations pour les restrictions du Serveur de connexion

Avant de mettre en œuvre des restrictions du Serveur de connexion pour les droits d'accès globaux, vous devez connaître certaines exigences et limitations.

- Une instance du Serveur de connexion ou un droit global peut contenir plusieurs balises.
- Plusieurs instances du Serveur de connexion et droits globaux peuvent contenir la même balise.
- N'importe quelle instance du Serveur de connexion peut accéder à un droit global ne contenant aucune balise.
- Des instances du Serveur de connexion qui ne contiennent aucune balise ne peuvent accéder qu'à des droits globaux qui ne contiennent aucune balise.
- Si vous utilisez un serveur de sécurité, vous devez configurer des restrictions sur l'instance du Serveur de connexion à laquelle le serveur de sécurité est couplé. Vous ne pouvez pas configurer des restrictions sur un serveur de sécurité.
- Les restrictions du Serveur de connexion sont prioritaires sur les autres droits d'accès ou attributions. Par exemple, même si un utilisateur est attribué à une machine particulière, il ne peut pas accéder à cette machine si la balise attribuée au droit global ne correspond pas à celle attribuée à l'instance du Serveur de connexion à laquelle il est connecté.

- Si vous prévoyez de fournir un accès à vos droits globaux via VMware Identity Manager et si vous configurez des limitations du Serveur de connexion, il est possible que l'application VMware Identity Manager affiche les droits globaux aux utilisateurs alors que ces droits globaux sont en réalité limités. Lorsqu'un utilisateur VMware Identity Manager tente de se connecter à un droit global, le poste de travail ou l'application ne démarre pas si la balise attribuée au droit global ne correspond pas à celle attribuée à l'instance du Serveur de connexion à laquelle l'utilisateur est connecté.

Exemple de restrictions du Serveur de connexion

Cet exemple montre un environnement Architecture Cloud Pod qui inclut deux espaces. Les deux espaces contiennent deux instances du Serveur de connexion. La première instance du Serveur de connexion prend en charge les utilisateurs internes et la seconde instance est couplée avec un serveur de sécurité et prend en charge les utilisateurs externes.

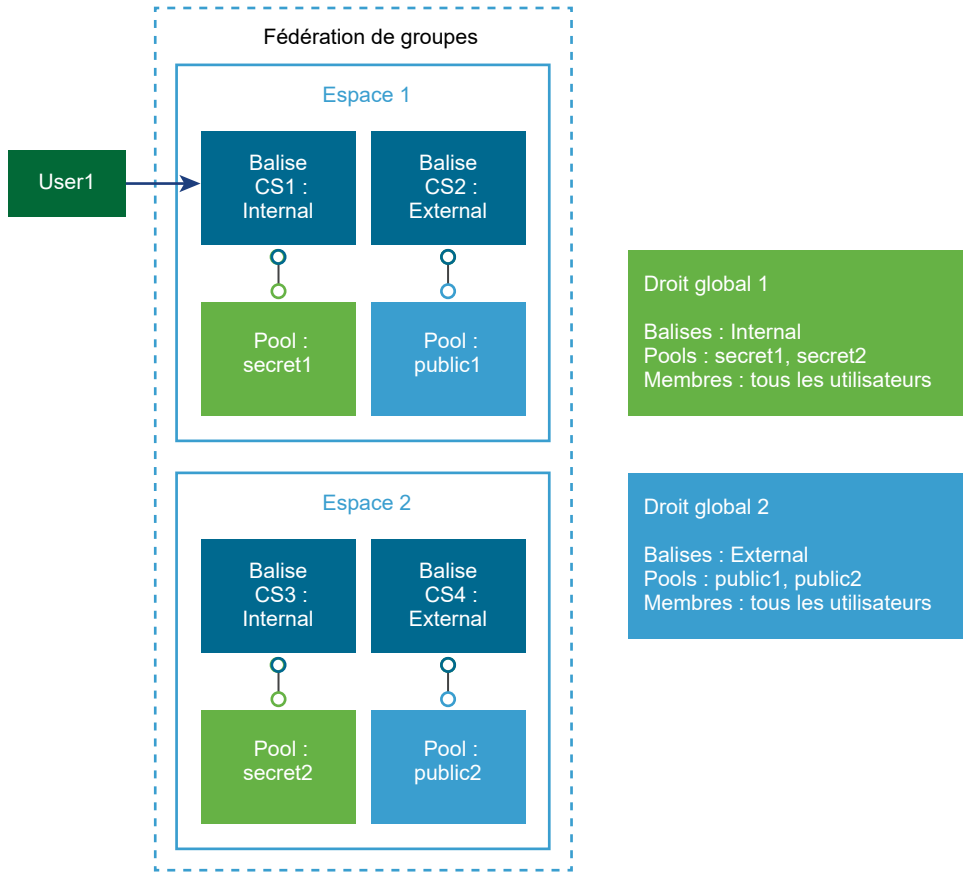
Pour empêcher les utilisateurs externes d'accéder à certains pools de postes de travail et d'applications, vous pouvez attribuer des balises comme suit :

- Attribuez la balise « Internal » à l'instance du Serveur de connexion qui prend en charge les utilisateurs internes.
- Attribuez la balise « External » aux instances du Serveur de connexion qui prennent en charge les utilisateurs externes.
- Attribuez la balise « Internal » aux droits globaux auxquels ne doivent accéder que les utilisateurs internes.
- Attribuez la balise « External » aux droits globaux auxquels ne doivent accéder que les utilisateurs externes.

Les utilisateurs externes ne peuvent pas voir les droits globaux qui portent la balise Internal, car ils sont connectés via les instances du Serveur de connexion qui portent des balises External. Les utilisateurs internes ne peuvent pas voir les droits globaux qui portent la balise External, car ils sont connectés via les instances du Serveur de connexion qui portent des balises Internal.

Dans le schéma suivant, User1 se connecte à l'instance du Serveur de connexion appelée CS1. Comme CS1 et le droit global 1 portent tous les deux une balise Internal, User1 ne peut voir que le droit global 1. Comme le droit global 1 contient des pools secret1 et secret2, User1 ne peut recevoir que des postes de travail ou des applications provenant des pools secret1 et secret2.

Figure 2-2. Exemple de restrictions du Serveur de connexion



Mise en œuvre des restrictions du client pour les droits d'accès globaux

Vous pouvez restreindre le droit global à des ordinateurs clients spécifiques. Pour limiter l'accès, ajoutez à un groupe de sécurité Active Directory les noms des ordinateurs clients auxquels vous voulez octroyer un droit global, puis ajoutez ce groupe aux utilisateurs et aux groupes du droit global.

Vous devez respecter certaines exigences et limitations pour utiliser les fonctionnalités de restrictions du client.

- Vous devez activer la stratégie de restrictions du client lorsque vous créez ou modifiez le droit d'accès global. Par défaut, la stratégie de restrictions du client est désactivée. Vous pouvez activer cette stratégie uniquement pour les droits de poste de travail flottants et les droits d'application globaux.
- Le paramètre de stratégie des restrictions du client pour les droits globaux remplace le paramètre de stratégie des restrictions du client au niveau du pool. Nous vous recommandons de ne pas activer la stratégie des restrictions du client sur les pools que contient le droit global si vous activez la stratégie de restrictions du client sur un droit global.

- Vous devez ajouter le groupe de sécurité Active Directory qui contient les noms des ordinateurs clients qui sont autorisés à accéder au droit global lorsque vous créez ou modifiez le droit global.
- La fonctionnalité de restrictions du client permet de restreindre les droits globaux à des ordinateurs clients spécifiques. Il ne permet pas aux utilisateurs de bénéficier des droits d'accès globaux. Par exemple, si un utilisateur ne bénéficie pas d'un droit d'accès global (en tant qu'utilisateur ou en tant que membre d'un groupe d'utilisateurs), il ne peut pas bénéficier du droit d'accès global, même si son ordinateur client bénéficie du droit d'accès global.
- Dans cette version, la fonctionnalité de restrictions du client est prise en charge uniquement par les ordinateurs clients Windows. Horizon Client 4.6 pour Windows ou version ultérieure doit être installé sur les ordinateurs clients.
- Lorsque la stratégie de restrictions du client est activée pour un droit d'accès global, les clients non-Windows, les clients Windows exécutant des versions antérieures à Horizon Client 4.6 pour Windows et les clients HTML Access ne peuvent pas bénéficier de ce droit d'accès global.

Implémentation de la fonctionnalité de préancement de session pour les droits d'application globaux

Avec la fonctionnalité de préancement de session, un administrateur Horizon peut configurer une application publiée pour que la session démarre avant qu'un utilisateur ouvre l'application dans Horizon Client. La fonctionnalité de préancement de session permet de démarrer plus rapidement des sessions pour les applications publiées fréquemment utilisées.

Vous pouvez activer la fonctionnalité de préancement de session pour un droit applicatif global en activant la stratégie de préancement lorsque vous créez ou modifiez le droit applicatif global. Tous les pools d'applications dans le droit d'application global doivent prendre en charge la fonctionnalité de préancement de session, et le délai d'expiration de session de préancement doit être le même pour toutes les batteries de serveurs.

Pour plus d'informations sur la configuration de pools d'applications et de batteries de serveurs pour utiliser la fonctionnalité de préancement de session, reportez-vous au document *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

La fonctionnalité de préancement de session n'est pas prise en charge pour les postes de travail distants.

Activation du mode de sessions multiples pour les droits applicatifs globaux

Lorsque vous créez un droit applicatif global, vous pouvez spécifier si les utilisateurs peuvent démarrer plusieurs sessions de la même application publiée sur différents périphériques clients. Cette fonctionnalité est appelée mode de sessions multiples.

Par exemple, si un utilisateur ouvre une application publiée en mode de sessions multiples sur le client A, puis qu'il ouvre la même application publiée sur le client B, elle reste ouverte sur le client A et une nouvelle session de l'application publiée s'ouvre sur le client B. En comparaison, si l'utilisateur ouvre une application publiée sur le client A en mode de sessions multiples, la session sur le client A est déconnectée et reconnectée sur le client B.

Lorsque vous activez le mode de sessions multiples, vous pouvez spécifier s'il est activé par défaut, désactivé par défaut ou appliqué.

- Lorsque le mode de sessions multiples est activé ou désactivé par défaut, les utilisateurs qui possèdent Horizon Client 4.10 ou version ultérieure peuvent désactiver ou activer le mode de sessions multiples en modifiant le paramètre **Lancements multiples** sur le client. Les utilisateurs qui disposent de versions antérieures d'Horizon Client ne peuvent pas modifier le paramètre par défaut.
- Lorsque le mode de sessions multiples est appliqué, il est toujours activé et les utilisateurs ne peuvent pas le désactiver dans Horizon Client.

Pour plus d'informations sur l'utilisation du paramètre **Lancements multiples**, consultez la documentation d'Horizon Client 4.10 ou version ultérieure.

La fonctionnalité de mode de sessions multiples présente les exigences et limites suivantes concernant les droits applicatifs globaux.

- Le paramètre de mode de sessions multiples que vous configurez pour le droit applicatif global doit correspondre au paramètre configuré pour les pools d'applications associés au droit applicatif global. Pour plus d'informations sur l'activation du mode de sessions multiples pour des pools d'applications, consultez le document *Configuration d'applications et de postes de travail publiés dans Horizon 7*.
- Vous ne pouvez pas activer la fonctionnalité de pré-lancement de session pour le droit applicatif global, ou les pools d'applications associés au droit applicatif global, lorsque le mode de sessions multiples est activé. La fonctionnalité de pré-lancement de session n'est pas prise en charge lorsque le mode de sessions multiples est activé.

Activation de la collaboration de session pour les droits de poste de travail globaux

Avec la fonctionnalité de collaboration de session, les utilisateurs finaux peuvent inviter d'autres utilisateurs à rejoindre une session de poste de travail distante existante.

Pour permettre aux utilisateurs de postes de travail distants de collaborer, un administrateur Horizon doit activer la fonctionnalité de collaboration de session pour le pool de postes de travail qui fournit le poste de travail distant. Pour les pools de postes de travail RDS, un administrateur Horizon doit activer la fonctionnalité de collaboration de session pour la batterie de serveurs sur laquelle repose le pool de postes de travail RDS.

Pour permettre aux utilisateurs invités de rejoindre des sessions à partir d'espaces autres que l'espace du propriétaire de la session, vous devez activer la stratégie de collaboration de session pour le droit de poste de travail global qui contient le pool de postes de travail lorsque vous créez ou modifiez le droit de poste de travail global.

Pour l'intégralité des exigences et des limitations relatives à la fonctionnalité de collaboration de session, notamment concernant la gestion des licences, reportez-vous à la section « Configuration de la session de collaboration » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

La collaboration de session n'est pas prise en charge pour les applications publiées.

Implémentation des droits globaux de sauvegarde

Lorsque vous modifiez un droit de poste de travail global ou un droit d'application global, vous pouvez sélectionner un droit global de sauvegarde. Un droit global de sauvegarde fournit des applications publiées ou des postes de travail distants lorsque le droit global principal ne parvient pas à démarrer une session en raison de problèmes tels qu'une capacité de pool insuffisante ou des espaces non disponibles. Un droit global de sauvegarde peut contenir des pools provenant de n'importe quel espace de la fédération d'espaces.

Les paramètres d'autorisation globale de sauvegarde suivants doivent correspondre à l'ensemble des paramètres de droits globaux principaux correspondants.

- Type d'affectation d'utilisateur
- Protocole d'affichage par défaut (uniquement si les utilisateurs ne sont pas autorisés à sélectionner le protocole d'affichage)
- Protocoles d'affichage pris en charge
- HTML Access
- Autoriser les utilisateurs à réinitialiser/redémarrer leurs machines
- Autoriser les utilisateurs à ouvrir des sessions séparées depuis différents périphériques clients
- Autoriser la collaboration de session

Le droit global de sauvegarde comporte les restrictions et limitations suivantes.

- Pour les droits de postes de travail globaux, vous pouvez configurer un droit global de sauvegarde uniquement si la stratégie d'affectation d'utilisateur est définie sur Flottante.
- Après avoir configuré un droit global de sauvegarde, la fonctionnalité de modification, les droits des utilisateurs et le paramètre de remplacement de site de base pour le droit de sauvegarde global sont désactivés.
- Vous ne pouvez pas sélectionner un droit global principal ou de sauvegarde existant lorsque vous sélectionnez un droit global de sauvegarde.
- Un droit global de sauvegarde ne peut pas être géré par le cloud.

- Un droit global de sauvegarde ne peut pas être associé à des droits d'utilisateur ou de groupe.

Pour plus d'informations sur la modification d'un droit global, reportez-vous à la section [Modifier les attributs ou les stratégies d'un droit global dans Horizon Console](#).

Éléments à prendre en compte pour les environnements hétérogènes

Les environnements Architecture Cloud Pod à hétérogènes sont pris en charge à partir d'Horizon 7 version 7.4. Par exemple, une fédération de groupes peut inclure des espaces exécutant Horizon 7 version 7.4 et des espaces exécutant Horizon 6 version 6.x.

Les nouvelles fonctionnalités ne fonctionnent pas dans un environnement hétérogène. Par exemple, une nouvelle fonctionnalité qui est visible dans Horizon Administrator pour une instance du serveur de connexion Horizon 7 version 7.4 n'est pas visible dans Horizon Administrator pour une instance du serveur de connexion Horizon 6 version 6.x. VMware vous recommande de mettre à niveau tous les espaces à la même version d'Horizon 7.

Remarques relatives au mode Workspace ONE

Si un administrateur Horizon active le mode Workspace ONE pour une instance du Serveur de connexion, les utilisateurs Horizon Client peuvent être redirigés vers un serveur Workspace ONE pour lancer leurs droits d'accès.

Pendant la configuration du mode Workspace ONE, un administrateur Horizon spécifie le nom d'hôte du serveur Workspace ONE. Dans un environnement Architecture Cloud Pod, chaque espace de la fédération doit être configuré pour pointer vers le même serveur Workspace ONE.

Pour plus d'informations sur la configuration du mode Workspace ONE, consultez le document *Administration d'Horizon 7*.

Considérations relatives à VMware Cloud on AWS

Vous pouvez déployer Horizon 7 dans un environnement de cloud hybride lorsque vous utilisez Architecture Cloud Pod pour interconnecter Horizon 7 sur site et les espaces Horizon 7 sur VMware Cloud on AWS. Vous pouvez autoriser des utilisateurs à utiliser des postes de travail virtuels et des applications publiées sur site et sur VMware Cloud on AWS.

Pour plus d'informations, consultez la section sur la « restructuration d'Architecture Cloud Pod (CPA) dans Horizon 7 pour VMware Cloud on AWS » dans le document *Horizon 7 on VMware Cloud on AWS Deployment Guide* à l'adresse <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vmw-deploy-horizon-seven-on-vmware-cloud-on-aws.pdf>.

Considérations relatives aux licences d'accès client aux services RDS par terminal

Lorsqu'un terminal client se connecte à une application ou un poste de travail publié sur un hôte RDS, il reçoit une licence d'accès client aux services RDS par terminal, si le mode de licence par terminal est configuré sur l'hôte RDS. Par défaut, la licence d'accès client est stockée uniquement sur le terminal client.

À partir de Horizon Client pour Windows 4.9, si le terminal client dispose d'une licence, il présente toujours cette licence. Les clients Windows qui disposent d'une licence Horizon Client 4.8 ou une version antérieure présentent une licence uniquement s'ils disposent d'une licence pour l'espace spécifique. Si le terminal client ne présente pas de licence, la licence la plus récente qui peut se trouver sur n'importe quel espace impliqué dans le démarrage de l'application ou du poste de travail publié est utilisée. Si aucune licence n'est trouvée sur l'un des espaces impliqués dans le démarrage, l'ID du terminal client est présenté au serveur de licences et une licence est émise.

Important VMware recommande de procéder à la mise à niveau vers la dernière version du client Windows et du serveur logiciel pour une gestion optimale des licences RDS.

Pour plus d'informations, reportez-vous à la section « Comprendre la gestion des licences d'accès client aux services RDS par terminal dans Horizon 7 » dans le document *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

Limites de la topologie Architecture Cloud Pod

Une topologie Architecture Cloud Pod standard se compose d'au moins deux espaces qui sont reliés entre eux dans une fédération d'espaces.

Le tableau suivant indique le nombre total de sessions prises en charge dans cette version.

Tableau 2-2. Limites des fédérations d'espaces

Objet	Limite
Nombre total de sessions	250 000
Groupes	50
Sessions par espace	12 000
Sites	15
Instances du Serveur de connexion par espace	7
Nombre total d'instances du Serveur de connexion	350

Les limites concernant les espaces, les sites et le nombre total des instances du Serveur de connexion indiquent le nombre maximal pris en charge pour chaque composant de la fédération d'espaces. Tant que la configuration reste dans les limites indiquées, vous pouvez concevoir une topologie appropriée pour atteindre le nombre total de sessions.

Configuration requise des ports pour Architecture Cloud Pod

Certains ports réseau doivent être ouverts sur le pare-feu Windows pour que la fonctionnalité Architecture Cloud Pod soit active. Lorsque vous installez le Serveur de connexion, le programme d'installation peut éventuellement configurer les règles de pare-feu requises à votre place. Ces règles ouvrent les ports utilisés par défaut. Si vous modifiez les ports par défaut après l'installation ou s'il existe d'autres pare-feu sur votre réseau, vous devez configurer manuellement le pare-feu Windows.

Tableau 2-3. Ports ouverts lors de l'installation du Serveur de connexion

Protocole	Port TCP	Description
HTTP	22389	Utilisé pour la réplication LDAP de couche de données globale. Les données partagées sont répliquées sur chaque instance du Serveur de connexion d'une fédération d'espaces. Chaque instance du Serveur de connexion d'une fédération d'espaces exécute une deuxième instance LDAP pour stocker les données partagées.
HTTPS	22636	Utilisé pour la réplication LDAP sécurisée de couche de données globale.
HTTPS	8472	Utilisé pour la communication View Interpod API (VIPA). Les instances du Serveur de connexion utilisent le canal de communication VIPA pour lancer de nouveaux postes de travail et applications, rechercher des postes de travail existants et partager des données d'état de santé ainsi que d'autres informations.

Note Microsoft Windows Server requiert l'ouverture d'une plage dynamique de ports entre toutes les instances du Serveur de connexion. Ces ports sont requis par Microsoft Windows pour le fonctionnement normal de l'appel de procédure distante (RPC) et la réplication Active Directory. Pour plus d'informations sur la plage de ports dynamique, consultez la documentation de Microsoft Windows Server.

Considérations liées à la sécurité des topologies Architecture Cloud Pod

Pour utiliser Horizon Console ou la commande `lmvutil` pour configurer et gérer un environnement Architecture Cloud Pod, vous devez disposer du rôle Administrateurs. Les utilisateurs qui disposent du rôle Administrateurs sur le groupe d'accès racine sont des super utilisateurs.

Lorsqu'une instance du Serveur de connexion fait partie d'un groupe répliqué d'instances du Serveur de connexion, les droits des super utilisateurs sont étendus à d'autres instances du Serveur de connexion de l'espace. De même, lorsqu'un espace est joint à une fédération d'espaces, les droits des super utilisateurs sont étendus à toutes les instances du Serveur de connexion de tous les espaces de la fédération d'espaces. Ces droits sont nécessaires pour modifier les droits d'accès globaux et pour effectuer d'autres opérations sur la couche de données globale.

Si vous ne souhaitez pas que certains super utilisateurs puissent effectuer des opérations sur la couche de données globale, vous pouvez supprimer l'attribution du rôle Administrateurs et plutôt attribuer le rôle Administrateurs locaux. Les utilisateurs qui disposent du rôle Administrateurs locaux obtiennent des droits de super utilisateur uniquement sur leur instance locale du Serveur de connexion et sur toute instance du groupe répliqué.

Pour plus d'informations sur l'affectation de rôles, consultez le document *Administration d'Horizon 7*.

Configuration de Architecture Cloud Pod dans Horizon Console

3

La configuration d'un environnement Architecture Cloud Pod implique d'initialiser la fonctionnalité Architecture Cloud Pod, d'associer des espaces à la fédération d'espaces et de créer de droits d'accès globaux.

Vous devez créer et configurer au moins un droit d'accès global afin d'utiliser la fonctionnalité Architecture Cloud Pod. Vous pouvez, en option, créer des sites et attribuer des sites de base.

Ce chapitre explique comment configurer un environnement Architecture Cloud Pod dans Horizon Console. Pour plus d'informations sur l'utilisation de l'interface de ligne de commande `lmvutil`, reportez-vous à la section [Chapitre 5 Administration d'Architecture Cloud Pod avec `lmvutil`](#).

Ce chapitre contient les rubriques suivantes :

- [Initialiser la fonctionnalité Architecture Cloud Pod dans Horizon Console](#)
- [Joindre un espace à la fédération d'espaces dans Horizon Console](#)
- [Affecter une balise à une instance du Serveur de connexion dans Horizon Console](#)
- [Configuration des raccourcis pour les droits d'accès globaux](#)
- [Feuille de calcul pour la configuration d'un droit d'accès global](#)
- [Créer et configurer un droit global dans Horizon Console](#)
- [Ajouter un pool à un droit global dans Horizon Console](#)
- [Créer et configurer un site dans Horizon Console](#)
- [Attribuer un site de base à un utilisateur ou à un groupe dans Horizon Console](#)
- [Créer un remplacement du site de base dans Horizon Console](#)
- [Tester une configuration d'Architecture Cloud Pod dans Horizon Client](#)
- [Exemple : Paramétrage d'une configuration Architecture Cloud Pod de base](#)

Initialiser la fonctionnalité Architecture Cloud Pod dans Horizon Console

Avant de configurer un environnement Architecture Cloud Pod, vous devez initialiser la fonctionnalité Architecture Cloud Pod.

Vous devez initialiser la fonctionnalité Architecture Cloud Pod une seule fois sur le premier espace d'une fédération d'espaces. Pour ajouter des espaces à la fédération d'espaces, vous devez joindre les nouveaux espaces à l'espace initialisé.

Pendant le processus d'initialisation, Horizon configure la couche de données globale sur chaque instance du Serveur de connexion de l'espace, configure le canal de communication VIPA et établit un accord de réplication entre chaque instance du Serveur de connexion.

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de l'espace.
- 2 Sélectionnez **Paramètres > Architecture Cloud Pod**, puis cliquez sur **Initialiser la fonctionnalité Architecture Cloud Pod** et sur **OK** pour démarrer le processus d'initialisation.

Horizon Console affiche l'avancement du processus d'initialisation. Une fois la fonctionnalité Architecture Cloud Pod initialisée, la fédération d'espaces contient l'espace initialisé et un site unique. Le nom de la fédération d'espaces par défaut est Horizon Cloud Pod Federation. Le nom de l'espace par défaut est basé sur le nom d'hôte de l'instance du Serveur de connexion. Par exemple, si le nom d'hôte est CS1, le nom de l'espace par défaut est Cluster-CS1. Le nom du site par défaut est Default First Site.
- 3 (Facultatif) Pour modifier le nom par défaut de la fédération d'espaces, cliquez sur **Modifier**, tapez le nouveau nom dans la zone de texte **Nom** et cliquez sur **OK**.
- 4 (Facultatif) Pour modifier le nom par défaut de l'espace, sélectionnez **Paramètres > Sites**, sélectionnez l'espace, cliquez sur **Modifier**, tapez le nouveau nom dans la zone de texte **Nom** et cliquez sur **OK**.
- 5 (Facultatif) Pour modifier le nom par défaut du site, sélectionnez **Paramètres > Sites**, sélectionnez le site, cliquez sur **Modifier**, tapez le nouveau nom dans la zone de texte **Nom** et cliquez sur **OK**.

Étape suivante

Pour ajouter des espaces supplémentaires à la fédération d'espaces, reportez-vous à [Joindre un espace à la fédération d'espaces dans Horizon Console](#).

Joindre un espace à la fédération d'espaces dans Horizon Console

Au cours du processus d'initialisation de la fonctionnalité Architecture Cloud Pod, la fonctionnalité Architecture Cloud Pod crée une fédération d'espaces contenant un espace unique. Vous pouvez

utiliser Horizon Console pour joindre des espaces supplémentaires à la fédération d'espaces. La jonction d'espaces supplémentaires est facultative.

Important Vous ne devez ni arrêter ni démarrer une instance du Serveur de connexion pendant que vous la joignez à une fédération d'espaces. Le service Serveur de connexion risque de ne pas redémarrer correctement. Vous pouvez arrêter et démarrer le Serveur de connexion une fois qu'il a joint la fédération d'espaces.

Conditions préalables

- Assurez-vous que les instances du Serveur de connexion que vous souhaitez joindre portent des noms d'hôtes différents. Vous ne pouvez pas joindre des serveurs portant le même nom, même s'ils se trouvent dans des domaines différents.
- Initialisez la fonctionnalité Architecture Cloud Pod. Reportez-vous à la section [Initialiser la fonctionnalité Architecture Cloud Pod dans Horizon Console](#).

Procédure

- 1 Ouvrez une session sur l'interface utilisateur d'Horizon Console pour tout Serveur de connexion de l'espace que vous joignez à la fédération d'espaces.
- 2 Sélectionnez **Paramètres > Architecture Cloud Pod** et cliquez sur **Joindre la fédération d'espaces**.
- 3 Dans la zone de texte **Serveur de connexion (nom d'hôte ou adresse IP)**, tapez le nom d'hôte ou l'adresse IP d'une instance du Serveur de connexion de n'importe quel espace ayant été initialisé ou qui est déjà joint à la fédération d'espaces.
- 4 Dans la zone de texte **Nom d'utilisateur (domain/username)**, tapez le nom d'un administrateur Horizon sur l'espace déjà initialisé.

Utilisez le format *domain\username*.

- 5 Dans la zone de texte **Mot de passe**, tapez le mot de passe de l'administrateur Horizon.
- 6 Pour joindre l'espace à la fédération d'espaces, cliquez sur **OK**.

Horizon Console affiche l'avancement du processus de jonction. Le nom de l'espace par défaut est basé sur le nom d'hôte de l'instance du Serveur de connexion. Par exemple, si le nom d'hôte est CS1, le nom de l'espace par défaut est Cluster-CS1.

Résultats

Une fois l'espace joint à la fédération d'espaces, il commence à partager des données de santé. Vous pouvez consulter ces données d'intégrité sur le tableau de bord d'Horizon Console. Reportez-vous à la section [Afficher l'intégrité d'une fédération d'espaces dans Horizon Console](#).

Note Il peut s'écouler un court délai avant que les données d'intégrité ne soient disponibles dans Horizon Console.

Étape suivante

Vous pouvez répéter ces étapes pour joindre des espaces supplémentaires à la fédération d'espaces.

Affecter une balise à une instance du Serveur de connexion dans Horizon Console

Si vous envisagez de limiter l'accès au droit global en fonction de l'instance du Serveur de connexion à laquelle les utilisateurs se connectent au départ lorsqu'ils sélectionnent un droit global, vous devez d'abord affecter une ou plusieurs balises à l'instance du Serveur de connexion.

Conditions préalables

Vous devez vous familiariser avec la fonctionnalité Restrictions du Serveur de connexion. Reportez-vous à la section [Mise en œuvre des restrictions du client pour les droits d'accès globaux](#).

Procédure

- 1 Connectez-vous à l'interface utilisateur d'Horizon Console pour l'instance du Serveur de connexion.
- 2 Sélectionnez **Paramètres > Serveurs**.
- 3 Cliquez sur l'onglet **Serveurs de connexion**, sélectionnez l'instance du Serveur de connexion et cliquez sur **Modifier**.
- 4 Saisissez une ou plusieurs balises dans le champ **Balises**.
Séparez les balises avec une virgule ou un point-virgule.
- 5 Cliquez sur **OK** pour enregistrer vos modifications.
- 6 Répétez ces étapes pour chaque instance du Serveur de connexion à laquelle vous voulez attribuer des balises.

Étape suivante

Lorsque vous créez ou modifiez un droit d'accès global, sélectionnez les balises qui sont associées aux instances du Serveur de connexion que vous souhaitez laisser accéder au droit d'accès global. Reportez-vous à la section [Créer et configurer un droit global dans Horizon Console](#) ou [Modifier les attributs ou les stratégies d'un droit global dans Horizon Console](#).

Configuration des raccourcis pour les droits d'accès globaux

Vous pouvez configurer des raccourcis pour les droits d'accès globaux. Lorsqu'un utilisateur autorisé se connecte à une instance du Serveur de connexion dans la fédération d'espaces à partir d'un client Windows, Horizon Client pour Windows place ces raccourcis dans le menu Démarrer de Windows, sur le poste de travail, ou sur les deux, sur le périphérique client de

l'utilisateur. Vous pouvez configurer un raccourci lorsque vous créez ou modifiez un droit d'accès global.

Vous devez sélectionner un dossier de catégorie, ou le dossier racine (/), pendant la configuration du raccourci. Vous pouvez ajouter et nommer vos propres dossiers de catégorie. Vous pouvez configurer jusqu'à quatre niveaux de dossier. Par exemple, vous pourrez ajouter un dossier de catégorie nommé Office, puis le sélectionner pour toutes vos applications professionnelles, telles que Microsoft Office et Microsoft PowerPoint.

Pour les raccourcis du menu Démarrer, sur les périphériques clients Windows 7, Horizon Client place les raccourcis et les dossiers de catégorie dans le dossier Applications VMware du menu Démarrer. Si vous sélectionnez le dossier racine (/) pour créer un raccourci, Horizon Client place le raccourci directement dans le dossier Applications VMware. Sur les périphériques clients Windows 8 et Windows 10, Horizon Client place les raccourcis et les dossiers de catégorie dans la liste Applications. Si vous sélectionnez le dossier racine (/) pour créer un raccourci, Horizon Client place le raccourci directement dans la liste Applications.

Sur les clients Mac, si Horizon Client pour Mac est configuré pour exécuter les applications publiées à partir du dossier Applications et autoriser les raccourcis automatiques à partir du serveur, les dossiers de catégorie pour les droits applicatifs globaux s'affichent dans le dossier Applications sur le client Mac.

Lorsque vous avez créé un raccourci, une coche s'affiche dans la colonne Raccourci d'application pour le droit global sur la page Droits d'accès globaux dans Horizon Console.

Par défaut, Horizon Client pour Windows invite les utilisateurs autorisés à installer des raccourcis lors de leur première connexion à un serveur. Vous pouvez configurer Horizon Client pour Windows pour qu'il installe automatiquement des raccourcis, ou qu'il n'en installe jamais, en modifiant le paramètre de stratégie de groupe **Installer automatiquement des raccourcis s'ils sont configurés sur Horizon Server**. Pour plus d'informations, reportez-vous au document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.

Par défaut, les modifications que vous apportez aux raccourcis sont synchronisées sur le périphérique client Windows d'un utilisateur chaque fois que l'utilisateur se connecte au serveur. Les utilisateurs peuvent désactiver la fonctionnalité de synchronisation de raccourci dans Horizon Client pour Windows. Pour plus d'informations, reportez-vous au document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.

Pour les utilisateurs Windows, cette fonctionnalité nécessite qu'Horizon Client 4.6 pour Windows ou version ultérieure soit installé sur le système client. Pour les utilisateurs Mac, cette fonctionnalité nécessite qu'Horizon Client pour Mac 4.10 ou version ultérieure soit installé sur le système client.

Feuille de calcul pour la configuration d'un droit d'accès global

Lorsque vous créez un droit global dans Horizon Console, l'interface utilisateur vous invite à configurer certaines options. Utilisez cette feuille de calcul pour préparer vos options de configuration avant de créer le droit d'accès global.

Vous pouvez imprimer cette feuille de calcul et noter les valeurs que vous souhaitez spécifier lorsque vous ajoutez un droit global.

Tableau 3-1. Feuille de calcul : Options de configuration d'un droit d'accès global

Option	Description	Indiquez votre valeur ici
Nom	Nom du droit d'accès global. Le nom s'affiche dans la liste des postes de travail et des applications disponibles dans Horizon Client. Le nom peut contenir entre 1 et 64 caractères.	
Description	(Facultatif) Description du droit d'accès global. La description peut contenir entre 1 et 1 024 caractères.	
Restrictions du Serveur de connexion	(Facultatif) Associe les balises du Serveur de connexion au droit d'accès global pour limiter l'accès au droit d'accès global à partir d'instances spécifiques du Serveur de connexion. Note Vous pouvez sélectionner uniquement les balises attribuées aux instances du Serveur de connexion dans l'espace local. Pour sélectionner des balises attribuées à des instances du Serveur de connexion dans un autre espace, vous devez vous connecter à une instance du Serveur de connexion de l'autre espace et modifier le droit global. Pour plus d'informations, reportez-vous à la section Mise en œuvre des restrictions du Serveur de connexion pour les droits d'accès globaux .	

Tableau 3-1. Feuille de calcul : Options de configuration d'un droit d'accès global (suite)

Option	Description	Indiquez votre valeur ici
Dossier de catégorie	<p>(Facultatif) Crée un raccourci pour le droit d'accès global. Vous pouvez sélectionner un dossier de catégorie existant ou en créer un. Vous pouvez configurer jusqu'à quatre sous-dossiers. Vous pouvez configurer un raccourci du menu Démarrer de Windows, un raccourci sur le poste de travail, ou les deux.</p> <p>Un nom de dossier peut comprendre jusqu'à 64 caractères. Pour spécifier un sous-dossier, entrez une barre oblique inversée (\), par exemple, dir1\dir2\dir3\dir4. Vous pouvez entrer jusqu'à quatre niveaux de dossier. Vous ne pouvez pas commencer ni terminer un nom de dossier avec une barre oblique inversée, et vous ne pouvez pas combiner plusieurs barres obliques inversées. Par exemple, \dir1, dir1\dir2\, dir1\\dir2 et dir1\\dir2 ne sont pas valides. Vous ne pouvez pas entrer de mots clés réservés Windows.</p> <p>Pour plus d'informations, reportez-vous à la section Configuration des raccourcis pour les droits d'accès globaux.</p>	
Droit global de sauvegarde	<p>(Uniquement disponible lorsque vous modifiez un droit global) Un droit global de sauvegarde fournit des postes de travail distants ou des applications publiées lorsque le droit global principal ne peut pas démarrer une session. Pour connaître les conditions requises et les restrictions, reportez-vous à la section Implémentation des droits globaux de sauvegarde.</p>	
Affectation d'utilisateur	<p>(Droit de poste de travail global uniquement) Spécifie le type de pool de postes de travail que peut contenir le droit d'accès global. Vous pouvez configurer l'une des stratégies d'affectation d'utilisateur suivantes :</p> <ul style="list-style-type: none"> ■ Flottant : le droit d'accès global contient uniquement des pools de postes de travail flottants. ■ Dédié : le droit d'accès global contient uniquement des pools de postes de travail dédiés. 	

Tableau 3-1. Feuille de calcul : Options de configuration d'un droit d'accès global (suite)

Option	Description	Indiquez votre valeur ici
Étendue	<p>Spécifie où rechercher des postes de travail ou des applications pour répondre à une demande provenant du droit d'accès global. Vous pouvez configurer l'une des stratégies d'étendue suivantes :</p> <ul style="list-style-type: none"> ■ Tous les sites : recherchez des postes de travail ou des applications dans n'importe quel espace de la fédération d'espaces. ■ Dans le site : recherchez des postes de travail ou des applications uniquement dans les espaces se trouvant dans le même site que l'espace auquel l'utilisateur est connecté. ■ Dans l'espace : recherchez des postes de travail ou des applications uniquement dans l'espace auquel l'utilisateur est connecté. <p>Pour plus d'informations, reportez-vous à la section Présentation de la stratégie d'étendue.</p>	
Options Utiliser le site de base et L'utilisateur autorisé doit disposer d'un site de base	<p>(Facultatif) Si les utilisateurs disposent de sites de base, configurez une stratégie de site de base pour le droit d'accès global. Vous pouvez configurer les stratégies de site de base suivantes :</p> <ul style="list-style-type: none"> ■ Utiliser le site de base : commencer par rechercher des postes de travail ou des applications dans le site de base de l'utilisateur. Si l'utilisateur ne dispose pas d'un site de base et que l'option L'utilisateur autorisé doit disposer d'un site de base n'est pas sélectionnée, le site auquel l'utilisateur est connecté est considéré comme le site de base. ■ L'utilisateur autorisé doit disposer d'un site de base : rend le droit d'accès global disponible uniquement si l'utilisateur dispose d'un site de base. Cette option est disponible uniquement si l'option Utiliser le site de base est sélectionnée. <p>Pour plus d'informations, reportez-vous à la section Utilisation des sites de base.</p>	
Nettoyage automatique des sessions redondantes	<p>(Facultatif) Spécifie s'il faut nettoyer les sessions redondantes.</p> <p>Plusieurs sessions peuvent être établies lorsqu'un espace contenant une session se déconnecte, lorsque l'utilisateur se reconnecte et démarre une autre session, et lorsque l'espace problématique revient en ligne avec la session d'origine. Lorsque plusieurs sessions sont établies, Horizon Client demande à l'utilisateur de sélectionner une session. Cette option détermine ce qu'il advient des sessions que l'utilisateur ne sélectionne pas. Si vous ne sélectionnez pas cette option, les utilisateurs doivent manuellement fermer leurs propres sessions supplémentaires en se déconnectant de Horizon Client ou en ouvrant les sessions, puis en les fermant.</p>	

Tableau 3-1. Feuille de calcul : Options de configuration d'un droit d'accès global (suite)

Option	Description	Indiquez votre valeur ici
Protocole d'affichage par défaut	Spécifie le protocole d'affichage par défaut pour les postes de travail ou les applications du droit global. Vous pouvez configurer PCoIP ou VMware Blast .	
Autoriser les utilisateurs à choisir un protocole	Lorsque vous activez cette stratégie, les utilisateurs peuvent remplacer le protocole d'affichage par défaut.	
Autoriser les utilisateurs à réinitialiser/redémarrer leurs machines	(Droit de travail global uniquement) Lorsque vous activez cette stratégie, les utilisateurs peuvent réinitialiser et redémarrer les postes de travail dans le droit de poste de travail global.	
HTML Access	<p>Lorsque vous activez cette stratégie, les utilisateurs peuvent utiliser un navigateur Web pour se connecter à des applications et des postes de travail distants et n'ont pas besoin d'installer un logiciel client sur leurs systèmes locaux.</p> <p>Pour plus d'informations, reportez-vous au document <i>Guide de l'utilisateur de VMware Horizon HTML Access</i>.</p>	
Prélancement	<p>(Droit applicatif global uniquement) Lorsque vous activez cette stratégie, les utilisateurs peuvent démarrer plus rapidement le droit d'application global.</p> <p>Note Si vous activez cette stratégie, tous les pools d'applications dans le droit d'application global doivent aussi prendre en charge la fonctionnalité de prélancement de session, et le délai d'expiration de session de prélancement doit être le même pour toutes les batteries de serveurs.</p>	
Autoriser la collaboration de session	<p>Lorsque vous activez cette stratégie, les utilisateurs peuvent inviter d'autres utilisateurs à rejoindre leurs sessions de poste de travail distantes.</p> <p>Note Si vous activez cette stratégie, tous les pools de postes de travail dans le droit de poste de travail global doivent également prendre en charge la fonctionnalité de collaboration de session. Pour les pools de postes de travail RDS, la fonctionnalité de collaboration de session est activée au niveau de la batterie de serveurs.</p> <p>Pour plus d'informations, reportez-vous à la section Activation de la collaboration de session pour les droits de poste de travail globaux.</p>	

Tableau 3-1. Feuille de calcul : Options de configuration d'un droit d'accès global (suite)

Option	Description	Indiquez votre valeur ici
Autoriser l'utilisateur à ouvrir des sessions séparées depuis différents périphériques clients	<p>(Droit de poste de travail global uniquement) Lorsque vous activez ce paramètre, les utilisateurs qui se connectent au droit global depuis différents périphériques clients reçoivent des sessions de poste de travail différentes. Pour se reconnecter à une session de poste de travail existante, les utilisateurs doivent utiliser le périphérique sur lequel cette session a été initiée. Si vous n'activez pas cette stratégie, les utilisateurs sont toujours reconnectés à leurs sessions de poste de travail existantes, quel que soit le périphérique client qu'ils utilisent. Vous pouvez activer cette stratégie uniquement pour les droits de poste de travail flottants.</p> <p>Note Si vous activez cette stratégie, tous les pools de postes de travail dans le droit d'accès global doivent également prendre en charge plusieurs sessions par utilisateur.</p> <p>Pour plus d'informations, reportez-vous à la section Comprendre la stratégie de sessions multiples par utilisateur pour les droits de poste de travail globaux.</p>	
Restrictions du client	<p>Lorsque vous activez cette stratégie, l'accès au droit global est limité à des ordinateurs clients spécifiques. Vous pouvez activer cette stratégie uniquement pour les droits de poste de travail flottants et les droits d'application globaux.</p> <p>Vous devez ajouter les noms des ordinateurs dotés du droit d'accès global dans un groupe de sécurité d'Active Directory. Vous pouvez sélectionner ce groupe de sécurité lorsque vous ajoutez des utilisateurs ou des groupes pour leur octroyer un droit d'accès global.</p> <p>Pour plus d'informations, reportez-vous à la section Mise en œuvre des restrictions du client pour les droits d'accès globaux.</p>	

Tableau 3-1. Feuille de calcul : Options de configuration d'un droit d'accès global (suite)

Option	Description	Indiquez votre valeur ici
Mode de sessions multiples	<p>(Droit applicatif global uniquement) Utilisez cette stratégie pour configurer la fonctionnalité de mode de sessions multiples pour un droit applicatif global. Les valeurs valides sont les suivantes.</p> <ul style="list-style-type: none"> ■ Désactivé : le mode de sessions multiples n'est pas pris en charge. ■ Activé (désactivé par défaut) : le mode de sessions multiples est pris en charge, mais il est désactivé par défaut. Pour utiliser le mode de sessions multiples, les utilisateurs doivent activer le paramètre Lancements multiples dans Horizon Client 4.10 ou version ultérieure. Pour les utilisateurs disposant d'une version antérieure d'Horizon Client, l'application est toujours démarrée en mode de session unique. ■ Activé (activé par défaut) : le mode de sessions multiples est pris en charge et il est activé par défaut. Les utilisateurs peuvent désactiver le mode de sessions multiples en désactivant le paramètre Lancements multiples dans Horizon Client 4.10 ou version ultérieure. Pour les utilisateurs disposant d'une version antérieure d'Horizon Client, l'application est toujours démarrée en mode de session unique. ■ Activé (appliqué) : le mode de sessions multiples est pris en charge et l'application est toujours démarrée en mode de sessions multiples. Les utilisateurs ne peuvent pas désactiver le mode de sessions multiples en désactivant le paramètre Lancements multiples dans Horizon Client 4.10 ou version ultérieure. Les utilisateurs qui disposent d'une version antérieure d'Horizon Client reçoivent un message d'erreur indiquant que le mode de démarrage demandé n'est pas pris en charge. <p>Pour plus d'informations, reportez-vous à la section Activation du mode de sessions multiples pour les droits applicatifs globaux.</p>	
Afficher le nom de la machine attribuée	<p>(Droit d'autorisation de poste de travail global uniquement) Affiche le nom d'hôte de la machine attribuée au lieu du nom du droit d'autorisation globale lorsqu'un utilisateur se connecte à Horizon Client.</p>	

Tableau 3-1. Feuille de calcul : Options de configuration d'un droit d'accès global (suite)

Option	Description	Indiquez votre valeur ici
	<p>Si aucune machine n'est attribuée à l'utilisateur, « nom du droit (aucune machine attribuée) » s'affiche pour le droit d'autorisation globale lorsque l'utilisateur se connecte à Horizon Client.</p> <hr/> <p>Note Si l'espace qui contient la machine n'est pas disponible ou ne répond pas dans les temps, le serveur de connexion ne peut pas obtenir le nom de la machine attribuée. Dans ce cas, « nom du droit (impossible d'obtenir le nom de la machine) » s'affiche à la place du nom du droit d'autorisation global lorsque l'utilisateur se connecte à Horizon Client.</p> <hr/> <p>Cette option n'est disponible que si vous sélectionnez Dédié dans Attributions d'utilisateur.</p>	

Créer et configurer un droit global dans Horizon Console

Vous pouvez utiliser Horizon Console pour créer et configurer des droits globaux. Vous utilisez des droits globaux pour permettre à des utilisateurs et des groupes d'accéder aux postes de travail et aux applications dans un environnement Architecture Cloud Pod. Les droits globaux font le lien entre les utilisateurs et leurs postes de travail et applications, quel que soit l'emplacement de ces postes de travail et applications dans la fédération d'espaces.

Un droit d'accès global contient une liste d'utilisateurs ou de groupes membres, un ensemble de stratégies et une liste des pools pouvant fournir des postes de travail ou des applications aux utilisateurs autorisés. Vous pouvez ajouter à un droit d'accès global des utilisateurs et des groupes, uniquement des utilisateurs ou uniquement des groupes.

Conditions préalables

- Initialisez la fonctionnalité Architecture Cloud Pod. Reportez-vous à la section [Initialiser la fonctionnalité Architecture Cloud Pod dans Horizon Console](#).
- Choisissez le type de droit de poste de travail global à créer, ainsi que les utilisateurs et groupes à inclure dans le droit d'accès global. Reportez-vous à la section [Octroi de droits d'accès à des utilisateurs et à des groupes d'une fédération d'espaces](#).
- Choisissez les options à configurer pour le droit d'accès global. Reportez-vous à la section [Feuille de calcul pour la configuration d'un droit d'accès global](#).

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Sélectionnez **Inventaire > Droits globaux** et cliquez sur **Ajouter**.

3 Sélectionnez le type de droit d'accès global à ajouter.

Option	Description
Autorisation de poste de travail	Ajoute un droit de poste de travail global.
Autorisation d'application	Ajoute un droit d'application global.

4 Cliquez sur **Suivant** et suivez les invites pour configurer le droit d'accès global.

Utilisez les informations de configuration que vous avez collectées dans la feuille de calcul de configuration de droit global.

5 Cliquez sur **Suivant** et ajoutez des utilisateurs ou des groupes au droit d'accès global.

a Pour filtrer des utilisateurs ou des groupes en fonction de vos critères de recherche, cliquez sur **Ajouter**, sélectionnez un ou plusieurs critères de recherche, puis cliquez sur **Rechercher**.

b Sélectionnez l'utilisateur ou le groupe à ajouter au droit global et cliquez sur **OK**.

Vous pouvez appuyer sur les touches Ctrl et Maj pour sélectionner plusieurs utilisateurs et groupes.

Pour restreindre le droit global à des ordinateurs clients spécifiques, sélectionnez le groupe de sécurité Active Directory contenant les noms des ordinateurs auxquels vous voulez octroyer ce droit.

Vous pouvez cocher la case **Utilisateurs non authentifiés** pour rechercher et ajouter des utilisateurs ne disposant pas d'un accès authentifié à des droits d'application globaux. Vous ne pouvez pas ajouter des utilisateurs ne disposant pas d'un accès authentifié à des droits de poste de travail globaux.

6 Pour créer l'autorisation globale, cliquez sur **Suivant**, vérifiez la configuration du droit global, puis cliquez sur **Terminer**.

Le droit d'accès global s'affiche sur la page Droits d'accès globaux.

Résultats

La fonctionnalité Architecture Cloud Pod stocke le droit global dans la couche de données globale qui réplique le droit global sur chaque espace de la fédération d'espaces.

Étape suivante

Sélectionnez les pools pouvant fournir des postes de travail ou des applications aux utilisateurs dans le droit global que vous avez créé. Reportez-vous à la section [Ajouter un pool à un droit global dans Horizon Console](#).

Ajouter un pool à un droit global dans Horizon Console

Vous pouvez utiliser Horizon Console pour ajouter un pool de postes de travail à une autorisation globale de poste de travail existante ou pour ajouter un pool d'applications à un droit applicatif existant.

Vous pouvez ajouter plusieurs pools à un droit global, mais vous ne pouvez ajouter un pool spécifique qu'à un seul droit global.

Si vous ajoutez plusieurs pools d'applications à un droit d'application global, vous devez ajouter la même application. Par exemple, n'ajoutez pas la Calculatrice et Microsoft Office PowerPoint au même droit d'application global. Si vous ajoutez différentes applications au même droit d'application global, les utilisateurs autorisés peuvent recevoir différentes applications à des moments différents.

Note Si un administrateur Horizon modifie la stratégie de protocole d'affichage ou de remplacement de protocole au niveau du pool après qu'un pool de postes de travail a été associé à un droit de poste de travail global, les utilisateurs peuvent recevoir une erreur de lancement du poste de travail quand ils sélectionnent le droit de poste de travail global. Si un administrateur Horizon modifie la stratégie de réinitialisation de machine virtuelle au niveau du pool après qu'un pool de postes de travail a été associé au droit de poste de travail global, les utilisateurs peuvent recevoir une erreur s'ils tentent de réinitialiser le poste de travail.

Conditions préalables

- Créez et configurez un droit d'accès global. Reportez-vous à la section [Créer et configurer un droit global dans Horizon Console](#).
- Créez le pool de postes de travail ou d'applications à ajouter au droit d'accès global. Reportez-vous au document *Configuration des postes de travail virtuels dans Horizon 7* ou *Configuration d'applications et de postes de travail publiés dans Horizon 7*.

Procédure

- 1 Ouvrez une session sur l'interface utilisateur d'Horizon Console pour toutes les instances du Serveur de connexion de l'espace contenant le pool à ajouter au droit global.
- 2 Sélectionnez **Inventaire > Droits globaux**.
- 3 Cliquez sur le nom du droit global.
- 4 Dans l'onglet **Pools locaux**, cliquez sur **Ajouter**, sélectionnez le pool de postes de travail ou d'applications à ajouter, puis cliquez sur **Ajouter**.

Vous pouvez appuyer sur les touches Ctrl et Maj pour sélectionner plusieurs pools.

Note Les pools déjà associés à un droit d'accès global ou qui ne répondent pas aux critères des stratégies de droit d'accès global sélectionnées ne sont pas affichés. Par exemple, si vous avez activé la stratégie HTML Access, vous ne pouvez pas sélectionner des pools qui n'autorisent pas HTML Access.

- 5 Répétez ces étapes sur une instance du Serveur de connexion dans chaque espace qui contient un pool à ajouter au droit global.

Résultats

Lorsqu'un utilisateur autorisé utilise Horizon Client pour se connecter à une instance du Serveur de connexion dans la fédération d'espaces, le nom du droit global apparaît dans la liste de postes de travail et d'applications disponibles.

Créer et configurer un site dans Horizon Console

Si votre topologie Architecture Cloud Pod contient plusieurs espaces, vous pouvez regrouper ces espaces dans des sites distincts. La fonctionnalité Architecture Cloud Pod traite tous les espaces d'un même site de la même manière.

Conditions préalables

- Décidez si votre topologie Architecture Cloud Pod doit inclure des sites. Reportez-vous à la section [Création de sites Architecture Cloud Pod](#).
- Initialisez la fonctionnalité Architecture Cloud Pod. Reportez-vous à la section [Initialiser la fonctionnalité Architecture Cloud Pod dans Horizon Console](#).

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Créez le site.
 - a Dans Horizon Console, sélectionnez **Paramètres > Sites** et cliquez sur **Ajouter**.
 - b Attribuez un nom au site dans la zone de texte **Nom**.
Le nom du site peut contenir entre 1 et 64 caractères.
 - c (Facultatif) Donnez une description du site dans la zone de texte **Description**.
Le nom du site peut contenir entre 1 et 1 024 caractères.
 - d Pour créer le site, cliquez sur **OK**.
- 3 Ajoutez un espace au site.
Répétez cette étape pour chaque espace à ajouter au site.
 - a Dans Horizon Console, sélectionnez **Paramètres > Sites**.
 - b Sélectionnez le site contenant actuellement l'espace à ajouter au site.
 - c Sélectionnez l'espace à ajouter au site et cliquez sur **Modifier**.
 - d Sélectionnez le site dans le menu déroulant **Site** et cliquez sur **OK**.

Attribuer un site de base à un utilisateur ou à un groupe dans Horizon Console

Un site de base correspond à la relation existant entre un utilisateur ou un groupe et un site Architecture Cloud Pod. Avec les sites de base, Horizon 7 effectue une recherche des postes de travail et des applications sur un site spécifique plutôt qu'une recherche basée sur l'emplacement actuel de l'utilisateur. L'attribution des sites de base est facultative.

Vous pouvez associer un droit global à un site de base pour que le site de base du droit global remplace le propre site de base d'un utilisateur lorsque ce dernier sélectionne le droit global. Pour plus d'informations, reportez-vous à la section [Créer un remplacement du site de base dans Horizon Console](#).

Conditions préalables

- Déterminez s'il convient d'attribuer des sites de base à des utilisateurs ou à des groupes dans votre environnement Architecture Cloud Pod. Reportez-vous à la section [Utilisation des sites de base](#).
- Regroupez les espaces de votre fédération d'espaces en sites. Reportez-vous à la section [Créer et configurer un site dans Horizon Console](#).
- Les droits d'accès globaux n'utilisent pas de sites de base par défaut. Lorsque vous créez un droit d'accès global, vous devez sélectionner l'option **Utiliser le site d'accueil** pour que Horizon 7 utilise le site de base d'un utilisateur lors de l'allocation de postes de travail à partir de ce droit d'accès global. Reportez-vous à la section [Créer et configurer un droit global dans Horizon Console](#).
- Initialisez la fonctionnalité Architecture Cloud Pod. Reportez-vous à la section [Initialiser la fonctionnalité Architecture Cloud Pod dans Horizon Console](#).

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Sélectionnez **Utilisateurs et groupes**, puis cliquez sur l'onglet **Attribution de site de base** et sur **Ajouter**.
- 3 Pour filtrer les utilisateurs ou les groupes en fonction de vos critères de recherche, sélectionnez un ou plusieurs critères de recherche, puis cliquez sur **Rechercher**.

Vous pouvez cocher la case **Utilisateurs non authentifiés** pour rechercher des utilisateurs ne disposant pas d'un accès authentifié dans la fédération d'espaces.

- 4 Sélectionnez un utilisateur ou un groupe et cliquez sur **Suivant**.
- 5 Sélectionnez le site de base à attribuer à l'utilisateur ou au groupe dans le menu déroulant **Site de base** et cliquez sur **Envoyer**.

Créer un remplacement du site de base dans Horizon Console

Vous pouvez associer un droit global à un site de base pour que le site de base du droit global remplace le propre site de base d'un utilisateur lorsque ce dernier sélectionne le droit global.

Pour créer un remplacement du site de base, vous associez un site de base à un droit global et un utilisateur ou un groupe particulier. Lorsque l'utilisateur (ou un utilisateur dans le groupe sélectionné) accède au droit global, le site de base de ce droit remplace le site de base de l'utilisateur.

Par exemple, si un utilisateur qui a un site de base à New York accède à un droit global qui associe cet utilisateur au site de base de Londres, Horizon recherche sur le site de Londres pour répondre à la demande d'application de l'utilisateur plutôt que d'allouer une application à partir du site de New York.

Conditions préalables

- Vérifiez que la stratégie **Utiliser le site de base** est activée sur le droit global. Pour plus d'informations, reportez-vous à la section [Modifier les attributs ou les stratégies d'un droit global dans Horizon Console](#).
- Vérifiez que l'utilisateur ou le groupe est inclus dans le droit global. Pour plus d'informations, reportez-vous à la section [Ajouter un utilisateur ou un groupe à un droit global dans Horizon Console](#).

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Sélectionnez **Inventaire > Droits globaux**.
- 3 Sélectionnez le nom du droit global à associer à un site de base, puis cliquez sur l'onglet **Remplacement du site de base**.
- 4 Cliquez sur **Ajouter**.

Le bouton **Ajouter** n'est pas disponible si la stratégie **Utiliser le site de base** n'est pas activée pour le droit global.

- 5 Sélectionnez un ou plusieurs critères de recherche et cliquez sur **Rechercher** pour filtrer des utilisateurs et des groupes Active Directory en fonction de vos critères de recherche.
- 6 Sélectionnez l'utilisateur ou le groupe Active Directory qui dispose d'un site de base que vous voulez remplacer et cliquez sur **Suivant**.

L'utilisateur ou le groupe doit déjà être inclus dans le droit global que vous avez sélectionné.

- 7 Sélectionnez le site de base à associer au droit global dans le menu déroulant **Remplacement du site de base** et cliquez sur **Soumettre**.

Tester une configuration d'Architecture Cloud Pod dans Horizon Client

Après avoir initialisé et configuré un environnement Architecture Cloud Pod, effectuez certaines étapes pour vérifier que votre environnement est correctement installé.

Conditions préalables

- Installez la dernière version de Horizon Client sur un ordinateur ou un appareil mobile pris en charge.
- Vérifiez que vous disposez des informations d'identification pour un utilisateur dans l'un de vos droits d'accès globaux récemment créés.

Procédure

- 1 Démarrez Horizon Client.
- 2 Connectez-vous à une instance du Serveur de connexion dans la fédération d'espaces en utilisant les informations d'identification d'un utilisateur dans l'un de vos nouveaux droits globaux.

Dès que vous êtes connecté à l'instance du Serveur de connexion, le nom du droit global figure dans la liste des postes de travail ou des applications disponibles.

- 3 Sélectionnez le droit global et connectez-vous à une application publiée ou un poste de travail distant.

Résultats

L'application publiée ou le poste de travail distant démarre correctement. Le poste de travail distant ou l'application publiée qui démarre dépend de la configuration individuelle du droit global, des espaces et des pools de postes de travail et d'applications. La fonctionnalité Architecture Cloud Pod tente d'allouer un poste de travail distant ou une application publiée à partir de l'espace auquel vous êtes connecté.

Étape suivante

Si le droit global ne s'affiche pas lorsque vous vous connectez à l'instance du Serveur de connexion, utilisez Horizon Console pour vérifier que le droit est correctement configuré. Si le droit global s'affiche mais que le poste de travail distant ou l'application publiée ne démarre pas, tous les pools de postes de travail ou d'applications sont peut-être attribués à d'autres utilisateurs.

Exemple : Paramétrage d'une configuration Architecture Cloud Pod de base

Cet exemple indique comment vous pouvez utiliser la fonctionnalité Architecture Cloud Pod pour réaliser une configuration Architecture Cloud Pod.

Dans cet exemple, une société d'assurance maladie dispose d'une force de vente mobile qui travaille sur deux régions, la région du centre et la région de l'est. Les agents commerciaux utilisent des appareils mobiles pour présenter des devis de polices d'assurance à des clients, et ces derniers affichent et signent des documents numériques.

Plutôt que stocker les données des clients sur leur appareils mobiles, les agents commerciaux utilisent des postes de travail flottants normalisés. L'accès aux données des clients est maintenu sécurisé dans les centres de données de la société d'assurance maladie.

La société d'assurance maladie dispose de deux centres de données, un dans chaque région. Lors de problèmes de capacité occasionnels, les agents commerciaux doivent rechercher des postes de travail disponibles dans un centre de données non local, ce qui peut parfois entraîner des problèmes de latence de réseau étendu. Si les agents commerciaux se déconnectent des postes de travail mais laissent leur session ouverte, ils doivent se souvenir du centre de données qui hébergeait leur session pour se reconnecter à leur poste de travail.

Pour résoudre ces problèmes, la société d'assurance maladie conçoit une topologie Architecture Cloud Pod, initialise la fonctionnalité Architecture Cloud Pod, joint ses espaces existants à la fédération d'espaces, crée des sites pour chacun de ses centres de données, octroie à ses agents commerciaux tous ses pools de postes de travail et implémente une URL unique.

Procédure

1 Conception de l'exemple de topologie

La société d'assurances conçoit une topologie Architecture Cloud Pod qui inclut un site pour chaque région.

2 Initialisation de l'exemple de configuration

Pour initialiser la fonctionnalité Architecture Cloud Pod, l'administrateur Horizon ouvre une session sur l'interface utilisateur d'Horizon Console pour une instance du Serveur de connexion d'East Pod 1, sélectionne **Paramètres > Architecture Cloud Pod** et clique sur **Initialiser la fonctionnalité Architecture Cloud Pod**.

3 Jonction d'espaces dans l'exemple de configuration

L'administrateur Horizon utilise Horizon Console pour joindre Central Pod 1 et Central Pod 2 à la fédération d'espaces.

4 Création de sites dans l'exemple de configuration

L'administrateur Horizon utilise Horizon Console pour créer un site pour les centres de données Central (Centre) et Eastern (Est), puis ajoute des espaces à ces sites.

5 Création de droits de poste de travail globaux dans l'exemple de configuration

L'administrateur Horizon utilise Horizon Console pour créer un droit de poste de travail global unique afin d'octroyer à tous les agents commerciaux un accès à tous les postes de travail des pools de postes de travail d'agents commerciaux dans tous les espaces de la fédération d'espaces.

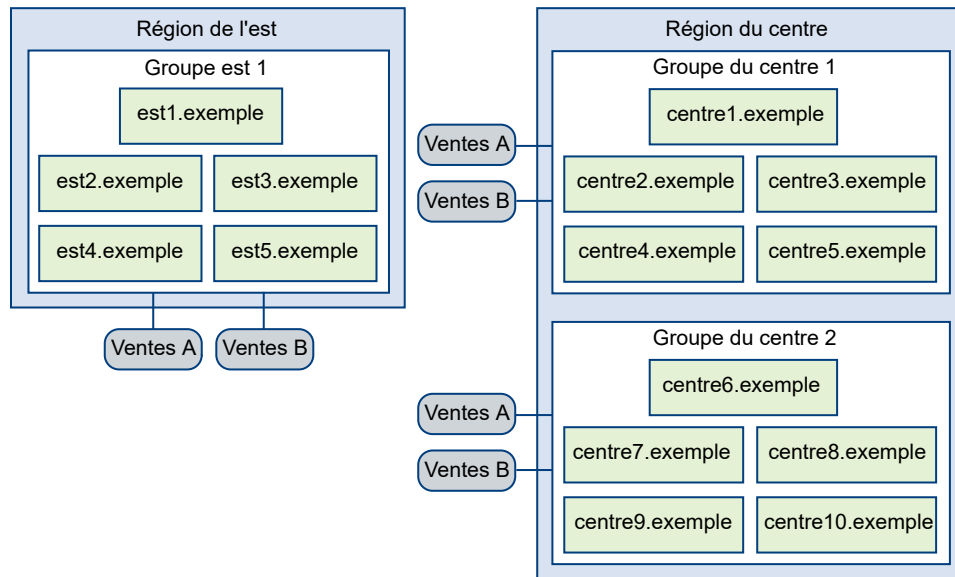
6 Création d'une URL pour l'exemple de configuration

La société d'assurances utilise une URL unique, ainsi qu'un service DNS afin de résoudre sales.example sur l'espace le plus proche du centre de données le plus proche. Ainsi, les agents commerciaux n'ont pas besoin de se souvenir des différentes URL de chaque espace et sont toujours dirigés vers le centre de données le plus proche, où qu'ils se trouvent.

Conception de l'exemple de topologie

La société d'assurances conçoit une topologie Architecture Cloud Pod qui inclut un site pour chaque région.

Figure 3-1. Exemple de topologie Architecture Cloud Pod



Dans cette topologie, le site Eastern Region contient un espace unique, East Pod 1, composé de cinq instances du Serveur de connexion nommées east1.example à east5.example.

Le site Central Region contient deux espaces, Central Pod 1 et Central Pod 2. Chaque espace contient cinq instances du Serveur de connexion. Les Serveurs de connexion dans le premier espace sont appelés central1.example à central5.example. Les instances du Serveur de connexion dans le second espace sont appelés central6.example à central10.example.

Chaque espace de la topologie contient deux pools de postes de travail d'agents commerciaux, appelés Sales A et Sales B.

Initialisation de l'exemple de configuration

Pour initialiser la fonctionnalité Architecture Cloud Pod, l'administrateur Horizon ouvre une session sur l'interface utilisateur d'Horizon Console pour une instance du Serveur de connexion d'East Pod 1, sélectionne **Paramètres > Architecture Cloud Pod** et clique sur **Initialiser la fonctionnalité Architecture Cloud Pod**.

Comme l'administrateur Horizon utilise l'interface utilisateur d'Horizon Console pour une instance du Serveur de connexion d'East Pod 1, la fédération d'espaces contient initialement East Pod 1. La fédération d'espaces contient également un seul site, appelé Default First Site, contenant East Pod 1.

Jonction d'espaces dans l'exemple de configuration

L'administrateur Horizon utilise Horizon Console pour joindre Central Pod 1 et Central Pod 2 à la fédération d'espaces.

- 1 Pour joindre Central Pod 1, l'administrateur Horizon ouvre une session sur l'interface utilisateur d'Horizon Console pour une instance du Serveur de connexion de Central Pod 1, sélectionne **Paramètres > Architecture Cloud Pod**, clique sur **Joindre la fédération d'espaces** et fournit le nom d'hôte ou l'adresse IP d'une instance du Serveur de connexion d'East Pod 1.

Central Pod 1 est à présent joint à la fédération d'espaces.

- 2 Pour joindre Central Pod 2, l'administrateur Horizon ouvre une session sur l'interface utilisateur d'Horizon Console pour une instance du Serveur de connexion de Central Pod 2, sélectionne **Paramètres > Architecture Cloud Pod**, clique sur **Joindre la fédération d'espaces** et fournit le nom d'hôte ou l'adresse IP d'une instance du Serveur de connexion d'East Pod 1 ou Central Pod 1.

Central Pod 2 est à présent joint à la fédération d'espaces.

Une fois Central Pod 1 et Central Pod 2 joints à la fédération d'espaces, les 10 instances du Serveur de connexion dans les deux espaces de Central Region font toutes partie de la fédération d'espaces.

Création de sites dans l'exemple de configuration

L'administrateur Horizon utilise Horizon Console pour créer un site pour les centres de données Central (Centre) et Eastern (Est), puis ajoute des espaces à ces sites.

- 1 L'administrateur Horizon ouvre une session sur l'interface utilisateur d'Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Pour créer un site pour le centre de données Eastern, l'administrateur Horizon sélectionne **Paramètres > Sites** et clique sur **Ajouter**.
- 3 Pour créer un site pour le centre de données Central, l'administrateur Horizon sélectionne **Paramètres > Sites** et clique sur **Ajouter**.
- 4 Pour déplacer East Pod 1 vers le site du centre de données Eastern, l'administrateur Horizon sélectionne **Paramètres > Sites**, sélectionne le site contenant actuellement East Pod 1, sélectionne East Pod 1, clique sur **Modifier**, puis sélectionne le site du centre de données Eastern dans le menu déroulant **Site**.

- 5 Pour déplacer Central Pod 1 vers le site du centre de données Central, l'administrateur Horizon sélectionne **Paramètres > Sites**, sélectionne le site contenant actuellement Central Pod 1, sélectionne Central Pod 1, clique sur **Modifier**, puis sélectionne le site du centre de données Central dans le menu déroulant **Site**.
- 6 Pour déplacer Central Pod 2 vers le site du centre de données Central, l'administrateur Horizon sélectionne **Paramètres > Sites**, sélectionne le site contenant actuellement Central Pod 2, sélectionne Central Pod 2, clique sur **Modifier**, puis sélectionne le site du centre de données Central dans le menu déroulant **Site**.

La topologie des sites de la fédération d'espaces reflète maintenant la répartition géographique des espaces dans le réseau de la société d'assurances.

Création de droits de poste de travail globaux dans l'exemple de configuration

L'administrateur Horizon utilise Horizon Console pour créer un droit de poste de travail global unique afin d'octroyer à tous les agents commerciaux un accès à tous les postes de travail des pools de postes de travail d'agents commerciaux dans tous les espaces de la fédération d'espaces.

- 1 Pour ajouter des utilisateurs au droit de poste de travail global, l'administrateur Horizon se connecte à l'interface utilisateur d'Horizon Console pour un Serveur de connexion de la fédération d'espaces, sélectionne **Inventaire > Droits globaux**, clique sur l'onglet **Utilisateurs et groupes**, puis sur **Ajouter des droits**.

L'administrateur Horizon ajoute le groupe Sales Agents (Agents commerciaux) au droit de poste de travail global. Le groupe Sales Agent (Agents commerciaux) est défini dans Active Directory et contient tous les utilisateurs agents commerciaux. L'ajout du groupe Sales Agent (Agents commerciaux) au droit de poste de travail global Agent Sales (Ventes d'agent) permet aux agents commerciaux d'accéder aux pools de postes de travail Sales A (Ventes A) et Sales B (Ventes B) sur les espaces Eastern region et Central region.

- 2 Pour ajouter les pools de postes de travail d'East Pod 1 au droit de poste de travail global, l'administrateur Horizon ouvre une session sur l'interface utilisateur d'Horizon Console pour une instance du Serveur de connexion d'East Pod 1, sélectionne **Inventaire > Droits globaux**, clique sur le nom du droit de poste de travail global, puis sur **Ajouter** dans l'onglet **Pools locaux**, sélectionne les pools de postes de travail à ajouter, puis clique sur **Ajouter**.
- 3 Pour ajouter les pools de postes de travail de Central Pod 1 au droit de poste de travail global, l'administrateur Horizon ouvre une session sur l'interface utilisateur d'Horizon Console pour une instance du Serveur de connexion de Central Pod 1, sélectionne **Inventaire > Droits globaux**, clique sur le nom du droit de poste de travail global, clique sur **Ajouter** dans l'onglet **Pools locaux**, sélectionne les pools de postes de travail à ajouter, puis clique sur **Ajouter**.

- 4 Pour ajouter les pools de postes de travail de Central Pod 2 au droit de poste de travail global, l'administrateur Horizon ouvre une session sur l'interface utilisateur d'Horizon Console pour une instance du Serveur de connexion de Central Pod 2, sélectionne **Inventaire > Droits globaux**, clique sur le nom du droit de poste de travail global, clique sur **Ajouter** dans l'onglet **Pools locaux**, sélectionne les pools de postes de travail à ajouter, puis clique sur **Ajouter**.

Création d'une URL pour l'exemple de configuration

La société d'assurances utilise une URL unique, ainsi qu'un service DNS afin de résoudre sales.example sur l'espace le plus proche du centre de données le plus proche. Ainsi, les agents commerciaux n'ont pas besoin de se souvenir des différentes URL de chaque espace et sont toujours dirigés vers le centre de données le plus proche, où qu'ils se trouvent.

Lorsqu'un agent commercial se connecte à l'URL dans Horizon Client, le droit global Agent commercial s'affiche dans la liste des pools de postes de travail disponibles. Quand un agent commercial sélectionne le droit de poste de travail global, la fonctionnalité Architecture Cloud Pod fournit le poste de travail disponible le plus proche dans la fédération d'espaces. Si tous les postes de travail du centre de données local sont utilisés, la fonctionnalité Architecture Cloud Pod sélectionne un poste de travail de l'autre centre de données. Si un agent commercial quitte une session de poste de travail ouverte, la fonctionnalité Architecture Cloud Pod renvoie l'agent commercial vers ce poste de travail, même s'il s'est, entre temps, déplacé dans une autre région.

Gestion d'un environnement Architecture Cloud Pod dans Horizon Console

4

Vous pouvez utiliser Horizon Console pour afficher, modifier et gérer votre environnement Architecture Cloud Pod.

Pour obtenir des informations générales sur l'utilisation d'Horizon Console, reportez-vous à la section « Utilisation de VMware Horizon Console » dans le document *Administration de VMware Horizon Console*. Pour plus d'informations sur l'utilisation de l'interface de ligne de commande `lmvutil`, reportez-vous à la section [Chapitre 5 Administration d'Architecture Cloud Pod avec lmvutil](#).

Ce chapitre contient les rubriques suivantes :

- [Afficher une configuration d'Architecture Cloud Pod dans Horizon Console](#)
- [Afficher l'intégrité d'une fédération d'espaces dans Horizon Console](#)
- [Afficher les sessions de postes de travail et d'applications dans Horizon Console](#)
- [Gestion des sites dans Horizon Console](#)
- [Gestion des droits globaux dans Horizon Console](#)
- [Gestion des sites de base dans Horizon Console](#)
- [Supprimer un espace de la fédération d'espaces dans Horizon Console](#)
- [Annuler l'initialisation de la fonctionnalité Architecture Cloud Pod dans Horizon Console](#)

Afficher une configuration d'Architecture Cloud Pod dans Horizon Console

Vous pouvez utiliser Horizon Console pour afficher des informations sur les droits globaux, les espaces, les sites et les sites de base.

Procédure

- ◆ Pour répertorier tous les droits globaux de votre configuration, sélectionnez **Inventaire > Droits globaux**.

Vous pouvez utiliser l'interface utilisateur d'Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.

- ◆ Pour répertorier les pools de postes de travail ou d'applications d'un droit global, sélectionnez **Inventaire > Droits globaux**, puis cliquez sur le nom de l'autorisation globale et sur l'onglet **Pools locaux**.

Seuls les pools de l'espace local s'affichent sur l'onglet **Pools locaux**. Si un droit global inclut des pools de postes de travail ou d'applications dans un espace distant, vous devez ouvrir une session sur l'interface utilisateur d'Horizon Console pour une instance du Serveur de connexion de l'espace distant afin d'afficher ces pools.

- ◆ Pour afficher le droit de poste de travail global qui contient un pool de postes de travail spécifique, sélectionnez **Inventaire > Postes de travail**.

Le nom du droit de poste de travail global qui contient le pool de postes de travail s'affiche dans la colonne Droit global pour ce pool de postes de travail sur la page Pools de postes de travail. Vous pouvez également cliquer sur un nom de pool de postes de travail sur la page Pools de postes de travail et afficher le nom du droit de poste de travail global dans l'onglet **Résumé**.

- ◆ Pour répertorier les utilisateurs et les groupes associés à un droit global, sélectionnez **Inventaire > Droits globaux**, puis cliquez sur le nom de l'autorisation globale et sur l'onglet **Utilisateurs et groupes**.

Vous pouvez utiliser l'interface utilisateur d'Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.

- ◆ Pour identifier rapidement l'espace auquel vous êtes connecté dans Horizon Console, recherchez le nom de l'espace dans l'en-tête en haut de la fenêtre Horizon Console.

Cette fonctionnalité est particulièrement utile lorsque vous êtes connecté à plusieurs espaces.

- ◆ Pour répertorier les espaces de la fédération d'espaces, sélectionnez **Paramètres > Architecture Cloud Pod**.

Vous pouvez utiliser l'interface utilisateur d'Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.

- ◆ Pour répertorier les sites de la fédération d'espaces, y compris les espaces d'un site, sélectionnez **Paramètres > Sites**.

Vous pouvez utiliser l'interface utilisateur d'Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.

- ◆ Pour répertorier les attributions de site de base pour des utilisateurs et des groupes, sélectionnez **Utilisateurs et groupes** et cliquez sur l'onglet **Attribution de site de base**.

- ◆ Pour répertorier les sites de base pour un utilisateur ou un groupe par droit global, procédez comme suit.
 - a Sélectionnez **Utilisateurs et groupes**, puis cliquez sur l'onglet **Résolution du site de base**.
 - b Cliquez sur **Rechercher un utilisateur**.
 - c Sélectionnez un ou plusieurs critères de recherche et cliquez sur **Rechercher** pour filtrer les utilisateurs Active Directory en fonction de vos critères de recherche.
 - d Sélectionnez l'utilisateur Active Directory et cliquez sur **OK**.

Le nom du droit global s'affiche dans la colonne Droits, tandis que le site de base effectif du droit global s'affiche dans la colonne Résolution du site de base. L'origine d'une attribution de site de base s'affiche entre parenthèses après le nom du site de base. Si un utilisateur dispose de plusieurs sites de base, une icône de dossier s'affiche à côté du nom du droit global. Vous pouvez développer ce dossier pour répertorier les attributions de site de base non effectives pour le droit global.

- ◆ Pour répertorier les balises associées à un droit global, sélectionnez **Inventaire > Droits globaux**, puis cliquez sur le nom du droit global et sur l'onglet **Résumé**.

Les balises qui sont associées au droit global s'affichent dans le champ Restrictions du Serveur de connexion.

Afficher l'intégrité d'une fédération d'espaces dans Horizon Console

Horizon surveille constamment l'intégrité de la fédération d'espaces en vérifiant l'intégrité de chaque espace et des instances du Serveur de connexion dans ces espaces. Vous pouvez afficher l'intégrité d'une fédération d'espaces dans Horizon Console.

Vous pouvez également afficher l'intégrité d'une fédération d'espaces à partir de la ligne de commande en utilisant la commande `vdadmin` avec l'option `-H`. Pour plus d'informations sur la syntaxe de `vdadmin`, reportez-vous au document *Administration d'Horizon 7*.

Important Les bases de données d'événements Horizon ne sont pas partagées entre les espaces d'une fédération d'espaces.

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Dans Horizon Console, sélectionnez **Surveiller > Tableau de bord**.
- 3 Dans le volet **Intégrité du système**, cliquez sur **Afficher**, puis sur **Espaces distants**.

Résultats

La page Espaces distants répertorie tous les espaces, leurs instances membres du Serveur de connexion et l'état de santé connu de chaque instance du Serveur de connexion.

Une icône de santé verte indique que l'instance du Serveur de connexion est en ligne et disponible pour la fonctionnalité Architecture Cloud Pod. Une icône de santé rouge indique que l'instance du Serveur de connexion est hors ligne ou que la fonctionnalité Architecture Cloud Pod ne peut pas s'y connecter pour confirmer sa disponibilité.

Afficher les sessions de postes de travail et d'applications dans Horizon Console

Vous pouvez utiliser Horizon Console pour afficher des sessions de postes de travail et d'applications dans une fédération d'espaces.

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.

2 Pour rechercher des sessions, procédez comme suit.

- a Dans Horizon Console, sélectionnez **Recherche de sessions**.
- b Sélectionnez les critères de recherche et commencez la recherche.

Vous pouvez rechercher des sessions de poste de travail et d'application par utilisateur, par espace ou par espace d'échange. L'utilisateur est l'utilisateur final qui est connecté au poste de travail ou à l'application. L'espace est celui sur lequel le poste de travail ou l'application est hébergé et l'espace d'échange est celui auquel l'utilisateur était connecté lorsque le poste de travail ou l'application a été alloué pour la première fois.

Option	Action
Rechercher par utilisateur	<ol style="list-style-type: none"> 1 Sélectionnez Utilisateur dans le menu déroulant et cliquez sur Rechercher des utilisateurs. 2 Sélectionnez les critères de recherche dans la boîte de dialogue Rechercher des utilisateurs et cliquez sur Rechercher.
Rechercher par espace	<ol style="list-style-type: none"> 1 Sélectionnez Espace dans le menu déroulant. 2 Sélectionnez un espace dans la liste des espaces et cliquez sur Rechercher.
Rechercher par espace d'échange	<ol style="list-style-type: none"> 1 Sélectionnez Groupe intermédiaire dans le menu déroulant. 2 Sélectionnez un espace dans la liste des espaces et cliquez sur Rechercher.

Les résultats de la recherche incluent l'utilisateur, le type de session (poste de travail ou application), la machine, le pool ou la batterie de serveurs, l'espace, l'ID de l'espace d'échange, le site et les droits d'accès globaux associés à chaque session. La date de début, ainsi que la durée et l'état de la session s'affichent également dans les résultats de la recherche. Sur la page des résultats de la recherche, vous pouvez vous déconnecter ou fermer une session, redémarrer un poste de travail, réinitialiser une machine virtuelle ou envoyer un message à un utilisateur de poste de travail.

Note L'ID de l'espace d'échange pour les nouvelles sessions n'est pas immédiatement renseigné dans les résultats de la recherche. Cet ID s'affiche généralement dans Horizon Console deux ou trois minutes après le début d'une session.

- 3 Pour afficher des informations sur toutes les sessions de Architecture Cloud Pod, procédez comme suit.

- a Sélectionnez **Surveiller > Tableau de bord**.
- b Dans le volet **Sessions Architecture Cloud Pod**, sélectionnez un espace dans le menu déroulant.

Le graphique en anneau affiche le nombre total de sessions hébergées et réparties pour l'espace que vous avez sélectionné.

- c Pour afficher d'autres informations sur la session, cliquez sur **Afficher**.

Un tableau affiche le nombre total de sessions réparties et hébergées pour chaque espace, ainsi que l'état de l'espace. Si l'état de l'espace est rouge, l'espace est inactif ou n'exécute pas Horizon 7 version 7.12 ou ultérieure. Les sessions sur les espaces qui exécutent des versions antérieures de Horizon 7 ne sont pas comptabilisées.

Gestion des sites dans Horizon Console

Vous pouvez utiliser Horizon Console pour créer, modifier et supprimer des sites Architecture Cloud Pod. Un site est un regroupement d'espaces.

Ajouter un espace à un site dans Horizon Console

Vous pouvez utiliser Horizon Console pour ajouter un espace à un site existant.

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Sélectionnez **Paramètres > Sites**.
- 3 Sélectionnez le site contenant actuellement l'espace à ajouter au site.
- 4 Sélectionnez l'espace à ajouter au site et cliquez sur **Modifier**.
- 5 Sélectionnez le site dans le menu déroulant **Site** et cliquez sur **OK**.

Supprimer un site dans Horizon Console

Vous pouvez utiliser Horizon Console pour supprimer un site de la fédération d'espaces.

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Sélectionnez **Paramètres > Sites**.
- 3 Sélectionnez le site à supprimer, cliquez sur **Supprimer**, puis sur **OK**.

Modifier un nom ou une description de site dans Horizon Console

Vous pouvez utiliser Horizon Console pour modifier un nom ou une description de site.

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Sélectionnez **Paramètres > Sites**.
- 3 Sélectionnez le site à modifier, cliquez sur **Modifier**, apportez vos modifications, puis cliquez sur **OK**.

Gestion des droits globaux dans Horizon Console

Vous pouvez utiliser Horizon Console pour ajouter des pools, des utilisateurs et des groupes à des droits globaux ou en supprimer. Vous pouvez également supprimer des droits globaux et modifier leurs attributs et leurs stratégies.

Supprimer un pool d'un droit global dans Horizon Console

Vous pouvez utiliser Horizon Console pour supprimer un pool d'un droit global.

Procédure

- 1 Ouvrez une session sur l'interface utilisateur de Horizon Console pour toutes les instances du Serveur de connexion de l'espace contenant le pool à supprimer.
- 2 Sélectionnez **Inventaire > Droits globaux**.
- 3 Cliquez sur le nom du droit global.
- 4 Sous l'onglet **Pools locaux**, cliquez sur la ligne contenant le pool, sur **Supprimer**, puis sur **OK**.

Ajouter un utilisateur ou un groupe à un droit global dans Horizon Console

Vous pouvez utiliser Horizon Console pour ajouter un utilisateur ou un groupe à un droit global existant.

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Sélectionnez **Inventaire > Droits globaux** et cliquez sur le nom du droit global.
- 3 Dans l'onglet **Utilisateurs et groupes**, cliquez sur **Ajouter des droits**.

- 4 Pour rechercher des utilisateurs ou des groupes Active Directory, cliquez sur **Ajouter**, sélectionnez un ou plusieurs critères de recherche, puis cliquez sur **Rechercher**.

Vous pouvez cocher la case **Utilisateurs non authentifiés** pour rechercher et ajouter des utilisateurs ne disposant pas d'un accès authentifié à des droits d'application globaux. Vous ne pouvez pas ajouter des utilisateurs ne disposant pas d'un accès authentifié à des droits de poste de travail globaux.

- 5 Sélectionnez l'utilisateur ou le groupe Active Directory à ajouter au droit d'accès global et cliquez sur **OK**.

Vous pouvez appuyer sur les touches Ctrl et Maj pour sélectionner plusieurs utilisateurs et groupes.

Pour restreindre le droit global à des ordinateurs clients spécifiques, sélectionnez le groupe de sécurité Active Directory contenant les noms des ordinateurs auxquels vous voulez octroyer ce droit.

- 6 Cliquez sur **OK** pour enregistrer les modifications.

Supprimer un utilisateur ou un groupe d'un droit global dans Horizon Console

Vous pouvez utiliser Horizon Console pour supprimer un utilisateur ou un groupe d'un droit global.

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Sélectionnez **Inventaire > Droits globaux** et cliquez sur le nom du droit global.
- 3 Sous l'onglet Utilisateurs et groupes, cochez la case en regard de l'utilisateur ou du groupe à supprimer, puis cliquez sur **Supprimer des droits**.
- 4 Cliquez sur **OK** dans la boîte de dialogue de confirmation.

Modifier les attributs ou les stratégies d'un droit global dans Horizon Console

Vous pouvez utiliser Horizon Console pour modifier les attributs et les stratégies de droit global.

Vous pouvez modifier le nom et la description du droit global, les balises du Serveur de connexion associées au droit d'accès global et le dossier de catégorie pour créer un raccourci du menu Démarrer de Windows. Vous pouvez modifier l'étendue, le site de base, la session redondante, le protocole d'affichage par défaut, HTML Access, le pré-lancement, la collaboration de session et les stratégies de restrictions du client. Vous pouvez également ajouter un droit global de sauvegarde.

Pour un droit applicatif, vous pouvez modifier le chemin, la version et l'éditeur de l'application après l'ajout du premier pool d'applications. Si vous ajoutez un pool d'applications à un droit applicatif qui contient déjà un pool d'applications, les valeurs précédentes de chemin, de version et d'éditeur de l'application sont conservées.

Vous ne pouvez pas modifier le type de pool de postes de travail qu'un droit de poste de travail global peut contenir.

Conditions préalables

Utilisez la feuille de calcul de configuration de droit d'accès global pour enregistrer les attributs et les stratégies à modifier. Reportez-vous à la section [Feuille de calcul pour la configuration d'un droit d'accès global](#).

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Sélectionnez **Inventaire > Droits globaux**.
- 3 Sélectionnez la ligne du droit global et cliquez sur **Modifier**.
- 4 Modifiez les attributs et les stratégies de droit d'accès global.

Utilisez les informations de configuration que vous avez collectées dans la feuille de calcul de configuration de droit global.

- 5 Cliquez sur **Envoyer** pour enregistrer les modifications.

Supprimer un droit global dans Horizon Console

Vous pouvez utiliser Horizon Console pour supprimer définitivement un droit global. Lorsque vous supprimez un droit global, tous les utilisateurs qui dépendent de ce droit global pour des postes de travail ne peuvent pas accéder à leurs postes de travail. Les sessions de poste de travail existantes restent connectées.

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Sélectionnez **Inventaire > Droits globaux**.
- 3 Cliquez sur la ligne du droit global à supprimer et cliquez sur **Supprimer**.
- 4 Cliquez sur **OK** dans la boîte de dialogue de confirmation.

Gestion des sites de base dans Horizon Console

Vous pouvez utiliser Horizon Console pour créer, modifier, supprimer et répertorier des sites de base.

Modifier une attribution de site de base dans Horizon Console

Vous pouvez modifier une attribution de site de base existante pour un utilisateur ou un groupe spécifique dans Horizon Console.

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Sélectionnez **Utilisateurs et groupes**, puis cliquez sur l'onglet **Attribution de site de base**.
- 3 Sélectionnez la ligne de l'utilisateur ou du groupe et cliquez sur **Modifier**.
- 4 Sélectionnez un site de base différent dans le menu déroulant **Site de base** et cliquez sur **OK**.

Supprimer une attribution de site de base dans Horizon Console

Vous pouvez supprimer l'association entre un utilisateur ou un groupe et un site de base dans Horizon Console.

Pour supprimer l'association entre un site de base et un droit global pour un utilisateur ou un groupe spécifique, reportez-vous à la section [Supprimer le remplacement du site de base dans Horizon Console](#).

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Sélectionnez **Utilisateurs et groupes**, puis cliquez sur l'onglet **Attribution de site de base**.
- 3 Sélectionnez la ligne de l'utilisateur ou du groupe et cliquez sur **Supprimer**.
- 4 Pour supprimer l'attribution de site de base, cliquez sur **OK**.

Déterminer le site de base effectif d'un utilisateur dans Horizon Console

Comme vous pouvez attribuer des sites de base aux utilisateurs et aux groupes, un seul utilisateur peut avoir plusieurs sites de base. De plus, les sites de base associés à des droits globaux peuvent remplacer le site de base d'un utilisateur. Vous pouvez utiliser Horizon Console pour déterminer le site de base effectif d'un utilisateur.

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Sélectionnez **Utilisateurs et groupes**, puis cliquez sur l'onglet **Résolution du site de base**.
- 3 Cliquez sur **Rechercher un utilisateur**.

- 4 Pour rechercher des utilisateurs Active Directory, sélectionnez un ou plusieurs critères de recherche et cliquez sur **Rechercher**.
- 5 Sélectionnez l'utilisateur Active Directory dont vous voulez afficher le site de base effectif et cliquez sur **OK**.

Résultats

Horizon Console affiche le site de base effectif de chaque droit global auquel l'utilisateur appartient. Seuls les droits globaux avec la stratégie **Utiliser le site de base** activée sont affichés.

Le site de base effectif s'affiche dans la colonne Résolution du site de base. Si un utilisateur dispose de plusieurs sites de base, une icône de dossier apparaît à côté du nom du droit global dans la colonne Droits. Vous pouvez développer ce dossier pour répertorier les attributions de site de base non effectives pour le droit global. Horizon Console utilise du texte barré pour indiquer un site de base non actif.

Horizon Console affiche l'origine d'une attribution de site de base entre parenthèses après le nom du site de base dans la colonne Résolution du site de base. Si le site de base provient d'un groupe auquel l'utilisateur appartient, Horizon Console affiche le nom du groupe, par exemple, **(via Utilisateurs de domaine)**. Si le site de base provient de l'attribution de site de base de l'utilisateur, Horizon Console affiche **(Par défaut)**. Si le site de base provient du droit global (un remplacement du site de base), Horizon Console affiche **(Direct)**.

Si l'utilisateur n'a pas de site de base, Horizon Console affiche **Aucun site de base défini** dans la colonne Résolution du site de base.

Modifier le remplacement du site de base dans Horizon Console

Vous pouvez modifier l'association entre un droit global et un site de base pour un utilisateur ou un groupe spécifique dans Horizon Console.

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Sélectionnez **Inventaire > Droits globaux**.
- 3 Sélectionnez le nom du droit global, puis cliquez sur l'onglet **Remplacement du site de base**.
- 4 Sélectionnez le remplacement du site de base à modifier et cliquez sur **Modifier**.
- 5 Sélectionnez un site de base différent dans le menu déroulant **Remplacement du site de base** et cliquez sur **OK**.

Supprimer le remplacement du site de base dans Horizon Console

Vous pouvez supprimer l'association entre un droit global et un site de base pour un utilisateur ou un groupe spécifique.

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Sélectionnez **Inventaire > Droits globaux**.
- 3 Sélectionnez le nom du droit global, puis cliquez sur l'onglet **Remplacement du site de base**.
- 4 Sélectionnez le remplacement du site de base et cliquez sur **Supprimer**.
- 5 Pour supprimer le remplacement du site de base, cliquez sur **OK**.

Supprimer un espace de la fédération d'espaces dans Horizon Console

Vous pouvez utiliser Horizon Console pour supprimer un espace préalablement joint à la fédération d'espaces. Vous pouvez choisir de supprimer un espace d'une fédération d'espaces s'il est remis en service à d'autres fins ou s'il n'a pas été correctement configuré.

Pour supprimer le dernier espace de la fédération d'espaces, vous devez annuler l'initialisation de la fonctionnalité Architecture Cloud Pod. Reportez-vous à la section [Annuler l'initialisation de la fonctionnalité Architecture Cloud Pod dans Horizon Console](#).

Important Vous ne devez ni arrêter ni démarrer une instance du Serveur de connexion lorsque sa suppression d'une fédération d'espaces est en cours. Le service Serveur de connexion risque de ne pas redémarrer correctement.

Procédure

- 1 Ouvrez une session sur l'interface utilisateur de Horizon Console pour toutes les instances du Serveur de connexion de l'espace que vous souhaitez supprimer de la fédération d'espaces.
- 2 Sélectionnez **Paramètres > Architecture Cloud Pod**, sélectionnez ensuite l'espace dont vous souhaitez annuler la jonction, puis cliquez sur **Annuler la jonction**.
- 3 Pour commencer l'opération d'annulation de la jonction, cliquez sur **OK**.

Horizon Console affiche l'avancement du processus d'annulation de la jonction.

Annuler l'initialisation de la fonctionnalité Architecture Cloud Pod dans Horizon Console

Vous pouvez utiliser Horizon Console pour annuler l'initialisation de la fonctionnalité Architecture Cloud Pod.

Conditions préalables

Vous devez annuler l'initialisation de la fonctionnalité Architecture Cloud Pod sur un seul espace de la fédération d'espaces. Si la fédération d'espaces contient plusieurs espaces, vous devez annuler la jonction des autres espaces avant de commencer le processus d'annulation de l'initialisation. Reportez-vous à la section [Supprimer un espace de la fédération d'espaces dans Horizon Console](#).

Procédure

- 1 Ouvrez une session sur l'interface utilisateur Horizon Console pour toutes les instances du Serveur de connexion de la fédération d'espaces.
- 2 Sélectionnez **Paramètres > Architecture Cloud Pod**, puis cliquez sur **Annuler l'initialisation**.
- 3 Pour commencer le processus d'annulation de l'initialisation, cliquez sur **OK**.

Horizon Console affiche l'avancement du processus d'annulation de l'initialisation. Une fois ce processus terminé, l'intégralité de votre configuration Architecture Cloud Pod, notamment les sites, les sites de base et les droits globaux, est supprimée.

Administration d'Architecture Cloud Pod avec Imvutil

5

Vous utilisez l'interface de ligne de commande `lmvutil` pour configurer et gérer une implémentation Architecture Cloud Pod.

Note Vous pouvez utiliser l'interface de ligne de commande `vdmutl` pour effectuer les mêmes opérations que `lmvutil`.

Ce chapitre contient les rubriques suivantes :

- [Utilisation de la commande Imvutil](#)
- [Initialisation de la fonctionnalité Architecture Cloud Pod.](#)
- [Désactivation de la fonctionnalité Architecture Cloud Pod](#)
- [Gestion d'une fédération d'espaces](#)
- [Gestion des sites](#)
- [Gestion des droits d'accès globaux](#)
- [Gestion des sites de base](#)
- [Affichage d'une configuration Architecture Cloud Pod](#)
- [Gestion des certificats SSL](#)

Utilisation de la commande Imvutil

La syntaxe de la commande `lmvutil` contrôle son fonctionnement.

Utilisez la forme suivante de la commande `lmvutil` dans une invite de commande Windows.

```
lmvutil command_option [additional_option argument] ...
```

Sinon, vous pouvez utiliser la commande `vdmutl` pour effectuer les mêmes opérations que la commande `lmvutil`. Utilisez la forme suivante de la commande `vdmutl` dans une invite de commande Windows.

```
vdmutl command_option [additional_option argument] ...
```

Les options supplémentaires que vous pouvez utiliser dépendent de l'option de commande.

Par défaut, le chemin d'accès vers les fichiers exécutables de la commande `lmvutil` et `vdmutil` est `C:\Program Files\VMware\VMware View\Server\tools\bin`. Pour éviter d'entrer le chemin d'accès sur la ligne de commande, ajoutez-le à la variable d'environnement `PATH`.

Authentification de la commande `lmvutil`

Lorsque vous utilisez la commande `lmvutil` pour configurer et gérer un environnement Architecture Cloud Pod, vous devez l'exécuter en tant qu'utilisateur disposant du rôle Administrateurs.

Vous pouvez utiliser Horizon Console pour affecter le rôle Administrateurs à un utilisateur. Reportez-vous au document *Administration d'Horizon 7*.

La commande `lmvutil` inclut des options pour spécifier le nom d'utilisateur, le domaine et le mot de passe à utiliser pour l'authentification.

Tableau 5-1. Options d'authentification de la commande `lmvutil`

Option	Description
<code>--authAs</code>	Nom d'un utilisateur administrateur Horizon. N'utilisez ni le format <i>domain\username</i> ni le format de nom principal d'utilisateur (UPN).
<code>--authDomain</code>	Nom de domaine complet de l'utilisateur administrateur Horizon spécifié dans l'option <code>--authAs</code> .
<code>--authPassword</code>	Mot de passe de l'utilisateur administrateur Horizon spécifié dans l'option <code>--authAs</code> . Si vous entrez « * » plutôt qu'un mot de passe, la commande <code>lmvutil</code> affiche une invite de mot de passe et ne conserve pas les mots de passe sensibles dans l'historique des commandes sur la ligne de commande.

Par exemple, la commande `lmvutil` suivante connecte l'utilisateur `domainEast\adminEast` et initialise la fonctionnalité Architecture Cloud Pod.

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --initialize
```

Vous devez utiliser les options d'authentification avec toutes les options de la commande `lmvutil`, à l'exception de `--help` et de `--verbose`.

Sortie de la commande `lmvutil`

La commande `lmvutil` renvoie 0 lorsqu'une opération réussit et un code différent de zéro spécifique d'un échec lorsqu'une opération échoue.

La commande `lmvutil` écrit des messages d'erreur en format d'erreur standard. Lorsqu'une opération produit une sortie ou lorsque la journalisation détaillée est activée à l'aide de l'option `--verbose`, la commande `lmvutil` écrit la sortie au format de sortie standard.

La commande `lmvutil` produit uniquement une sortie en anglais américain.

Options de la commande `lmvutil`

Vous utilisez les options de la commande `lmvutil` pour spécifier l'opération à effectuer. Toutes les options sont précédées de deux traits d'union (--).

Pour connaître les options d'authentification de la commande `lmvutil`, reportez-vous à [Authentification de la commande `lmvutil`](#).

Tableau 5-2. Options de la commande `lmvutil`

Option	Description
<code>--activatePendingCertificate</code>	Active un certificat SSL en attente. Reportez-vous à la section Activation d'un certificat en attente .
<code>--addGroupEntitlement</code>	Associe un groupe d'utilisateurs à un droit d'accès global. Reportez-vous à la section Ajout d'un utilisateur ou d'un groupe à un droit d'accès global .
<code>--addPoolAssociation</code>	Associe un pool de postes de travail à un droit de poste de travail global ou un pool d'applications avec un droit d'application global. Reportez-vous à la section Ajout d'un pool à un droit d'accès global .
<code>--addUserEntitlement</code>	Associe un utilisateur à un droit d'accès global. Reportez-vous à la section Ajout d'un utilisateur ou d'un groupe à un droit d'accès global .
<code>--assignPodToSite</code>	Affecte un espace à un site. Reportez-vous à la section Affectation d'un espace à un site .
<code>--createGlobalApplicationEntitlement</code>	Crée un droit d'application global. Reportez-vous à la section Création d'un droit d'accès global .
<code>--createGlobalEntitlement</code>	Crée un droit de poste de travail global. Reportez-vous à la section Création d'un droit d'accès global .
<code>--createSite</code>	Crée un site. Reportez-vous à la section Création d'un site .
<code>--createGroupHomeSite</code>	Associe un groupe d'utilisateurs à un site de base. Reportez-vous à la section Configuration d'un site de base .
<code>--createPendingCertificate</code>	Crée un certificat SSL en attente. Reportez-vous à la section Création d'un certificat en attente .
<code>--createUserHomeSite</code>	Associe un utilisateur à un site de base. Reportez-vous à la section Configuration d'un site de base .
<code>--deleteGlobalApplicationEntitlement</code>	Supprime un droit d'application global. Reportez-vous à la section Suppression d'un droit d'accès global .
<code>--deleteGlobalEntitlement</code>	Supprime un droit de poste de travail global. Reportez-vous à la section Suppression d'un droit d'accès global .
<code>--deleteSite</code>	Supprime un site. Reportez-vous à la section Suppression d'un site .
<code>--deleteGroupHomeSite</code>	Supprime l'association entre un groupe d'utilisateurs et un site de base. Reportez-vous à la section Suppression d'un site de base .

Tableau 5-2. Options de la commande `lmvutil` (suite)

Option	Description
<code>--deleteUserHomeSite</code>	Supprime l'association entre un utilisateur et un site de base. Reportez-vous à la section Suppression d'un site de base .
<code>--editSite</code>	Modifie le nom ou la description d'un site. Reportez-vous à la section Modification du nom ou de la description d'un site .
<code>--ejectPod</code>	Supprime un espace indisponible d'une fédération d'espaces. Reportez-vous à la section Suppression d'un espace d'une fédération d'espaces .
<code>--help</code>	Répertorie les options de la commande <code>lmvutil</code> .
<code>--initialize</code>	Initialise la fonctionnalité Architecture Cloud Pod. Reportez-vous à la section Initialisation de la fonctionnalité Architecture Cloud Pod .
<code>--join</code>	Joint un espace à une fédération d'espaces. Reportez-vous à la section Jonction d'un espace à la fédération d'espaces .
<code>--listAssociatedPools</code>	Répertorie les pools de postes de travail associés à un droit de poste de travail global ou les pools d'applications associés à un droit d'application global. Reportez-vous à la section Affichage de la liste des pools d'un droit d'accès global .
<code>--listEntitlements</code>	Répertorie les associations entre les utilisateurs ou les groupes d'utilisateurs et les droits d'accès globaux. Affichage de la liste des utilisateurs ou des groupes d'un droit d'accès global .
<code>--listGlobalApplicationEntitlements</code>	Répertorie tous les droits d'application globaux. Reportez-vous à la section Affichage de la liste des droits d'accès globaux .
<code>--listGlobalEntitlements</code>	Répertorie tous les droits de poste de travail globaux. Reportez-vous à la section Affichage de la liste des droits d'accès globaux .
<code>--listPods</code>	Répertorie les espaces d'une topologie Architecture Cloud Pod. Reportez-vous à la section Affichage de la liste des espaces ou des sites dans une topologie Architecture Cloud Pod .
<code>--listSites</code>	Répertorie les sites d'une topologie Architecture Cloud Pod. Reportez-vous à la section Affichage de la liste des espaces ou des sites dans une topologie Architecture Cloud Pod .
<code>--listUserAssignments</code>	Répertorie les attributions d'espaces de postes de travail dédiés pour une combinaison d'utilisateur et de droit d'accès global. Reportez-vous à la section Affichage de la liste des attributions de pool de postes de travail dédiés .
<code>--removePoolAssociation</code>	Supprime l'association entre un pool de postes de travail et un droit d'accès global. Reportez-vous à la section Suppression d'un pool d'un droit d'accès global .

Tableau 5-2. Options de la commande `lmvutil` (suite)

Option	Description
<code>--resolveUserHomeSite</code>	Affiche le site de base effectif d'un utilisateur. Reportez-vous à la section Affichage du site de base effectif d'un utilisateur .
<code>--removeGroupEntitlement</code>	Supprime un groupe d'utilisateurs d'un droit d'accès global. Reportez-vous à la section Suppression d'un utilisateur ou d'un groupe d'un droit global .
<code>--removeUserEntitlement</code>	Supprime un utilisateur d'un droit d'accès global. Reportez-vous à la section Suppression d'un utilisateur ou d'un groupe d'un droit global .
<code>--showGroupHomeSites</code>	Affiche tous les sites de base d'un groupe. Reportez-vous à la section Affichage de la liste des sites de base d'un utilisateur ou d'un groupe .
<code>--showUserHomeSites</code>	Affiche tous les sites de base d'un utilisateur. Reportez-vous à la section Affichage de la liste des sites de base d'un utilisateur ou d'un groupe .
<code>--uninitialize</code>	Désactive la fonctionnalité Architecture Cloud Pod. Reportez-vous à la section Désactivation de la fonctionnalité Architecture Cloud Pod .
<code>--unjoin</code>	Supprime un espace disponible d'une fédération d'espaces. Reportez-vous à la section Suppression d'un espace d'une fédération d'espaces .
<code>--updateGlobalApplicationEntitlement</code>	Modifie un droit d'application global. Reportez-vous à la section Modification d'un droit d'accès global .
<code>--updateGlobalEntitlement</code>	Modifie un droit de poste de travail global. Reportez-vous à la section Modification d'un droit d'accès global .
<code>--updatePod</code>	Modifie le nom ou la description d'un espace. Reportez-vous à la section Modification du nom ou de la description d'un espace .
<code>--verbose</code>	Active la journalisation détaillée. Vous pouvez ajouter cette option à n'importe quelle autre option pour obtenir une sortie de commande détaillée. La commande <code>lmvutil</code> écrit dans la sortie standard.

Initialisation de la fonctionnalité Architecture Cloud Pod.

Utilisez la commande `lmvutil` avec l'option `--initialize` pour initialiser la fonctionnalité Architecture Cloud Pod. Lorsque vous initialisez la fonctionnalité Architecture Cloud Pod, Horizon configure la couche de données globale sur chaque instance du Serveur de connexion de l'espace et configure le canal de communication VIPA.

Syntaxe

```
lmvutil --initialize
```

Notes d'utilisation

Exécutez cette commande une seule fois, sur une seule instance du Serveur de connexion de l'espace. Vous pouvez exécuter cette commande sur n'importe quelle instance du Serveur de connexion de l'espace. Vous n'avez pas besoin d'exécuter cette commande pour des espaces supplémentaires. Les autres espaces sont joints à l'espace initialisé.

Cette commande renvoie un message d'erreur si la fonctionnalité Architecture Cloud Pod est déjà initialisée ou si la commande ne parvient pas à terminer l'opération.

Exemple

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --initialize
```

Désactivation de la fonctionnalité Architecture Cloud Pod

Utilisez la commande `lmvutil` avec l'option `--uninitialize` pour désactiver la fonctionnalité Architecture Cloud Pod.

Syntaxe

```
lmvutil --uninitialize
```

Notes d'utilisation

Avant d'exécuter cette commande, utilisez la commande `lmvutil` avec l'option `--unjoin` pour supprimer les autres espaces dans la fédération d'espaces.

Exécutez cette commande sur une seule instance du Serveur de connexion dans un espace. Vous pouvez exécuter cette commande sur n'importe quelle instance du Serveur de connexion de l'espace. Si votre fédération d'espaces contient plusieurs espaces, vous devez exécuter cette commande pour un seul espace.

Cette commande renvoie un message d'erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée, si la commande ne trouve pas l'espace ou si d'autres espaces sont présents dans la fédération d'espaces.

Exemple

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --uninitialize
```

Gestion d'une fédération d'espaces

La commande `lmvutil` fournit des options pour configurer et modifier une fédération d'espaces.

- **Jonction d'un espace à la fédération d'espaces**

Utilisez la commande `lmvutil` avec l'option `--join` pour joindre un espace à la fédération d'espaces.

- **Suppression d'un espace d'une fédération d'espaces**

Utilisez la commande `lmvutil` avec l'option `--unjoin` ou `--ejectPod` pour supprimer un espace d'une fédération d'espaces.

- **Modification du nom ou de la description d'un espace**

Utilisez la commande `lmvutil` avec l'option `--updatePod` pour mettre à jour ou modifier le nom ou la description d'un espace.

Jonction d'un espace à la fédération d'espaces

Utilisez la commande `lmvutil` avec l'option `--join` pour joindre un espace à la fédération d'espaces.

Syntaxe

```
lmvutil --join joinServer serveraddress --userName domain\username --password password
```

Notes d'utilisation

Vous devez exécuter cette commande sur chaque espace que vous souhaitez joindre à la fédération d'espaces. Vous pouvez exécuter cette commande sur n'importe quelle instance du Serveur de connexion dans un espace.

Cette commande renvoie un message d'erreur si vous fournissez des informations d'identification non valides, si l'instance du Serveur de connexion spécifiée n'existe pas, si une fédération d'espaces n'existe pas sur le serveur spécifié ou si la commande ne peut pas terminer l'opération.

Options

Vous devez spécifier plusieurs options lorsque vous joignez un espace à une fédération d'espaces.

Tableau 5-3. Options de jonction d'un espace à une fédération d'espaces

Option	Description
<code>--joinServer</code>	Nom DNS ou adresse IP d'une instance du Serveur de connexion dans un espace qui a été initialisé ou qui fait déjà partie de la fédération d'espaces.
<code>--userName</code>	Nom d'un utilisateur administrateur Horizon sur l'espace déjà initialisé. Utilisez le format <code>domain\username</code> .
<code>--password</code>	Mot de passe de l'utilisateur indiqué dans l'option <code>--userName</code> .

Exemple

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --join
--joinServer 123.456.789.1 --userName domainCentral\adminCentral --password secret123
```

Suppression d'un espace d'une fédération d'espaces

Utilisez la commande `lmvutil` avec l'option `--unjoin` ou `--ejectPod` pour supprimer un espace d'une fédération d'espaces.

Syntaxe

```
lmvutil --unjoin
```

```
lmvutil --ejectPod --pod pod
```

Notes d'utilisation

Pour supprimer un espace d'une fédération d'espaces, utilisez l'option `--unjoin`. Vous pouvez exécuter cette commande sur n'importe quelle instance du Serveur de connexion de l'espace.

Pour supprimer un espace qui n'est pas disponible d'une fédération d'espaces, utilisez l'option `--ejectPod`. Par exemple, un espace peut devenir indisponible en cas de panne matérielle. Vous pouvez effectuer cette opération sur n'importe quel espace de la fédération d'espaces.

Important Dans la plupart des cas, vous devez utiliser l'option `--unjoin` pour supprimer un espace d'une fédération d'espaces.

Ces commandes renvoient un message d'erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée, si l'espace n'est pas joint à une fédération d'espaces ou si les commandes ne peuvent pas effectuer les opérations spécifiées.

Options

Lorsque vous utilisez l'option `--ejectPod`, vous utilisez l'option `--pod` pour identifier l'espace à supprimer de la fédération d'espaces.

Exemple

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --unjoin
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --ejectPod
--pod "East Pod 1"
```

Modification du nom ou de la description d'un espace

Utilisez la commande `lmvutil` avec l'option `--updatePod` pour mettre à jour ou modifier le nom ou la description d'un espace.

Syntaxe

```
lmvutil --updatePod --podName podname [--newPodName podname] [--description text]
```

Notes d'utilisation

Cette commande renvoie un message d'erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée ou si la commande est incapable de trouver ou de mettre à jour l'espace.

Options

Vous pouvez spécifier les options suivantes lorsque vous mettez à niveau le nom ou la description d'un espace.

Tableau 5-4. Options permettant de modifier le nom ou la description d'un espace

Option	Description
--podName	Nom de l'espace à mettre à jour.
--newPodName	(Facultatif) Nouveau nom de l'espace. Un nom d'espace peut contenir entre 1 et 64 caractères.
--description	(Facultatif) Description du site. La description peut contenir entre 1 et 1 024 caractères.

Exemple

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--updatePod --podName "East Pod 1" --newPodName "East Pod 2"
```

Gestion des sites

Vous pouvez utiliser les options de la commande `lmvutil` pour créer, modifier et supprimer des sites Architecture Cloud Pod. Un site est un regroupement d'espaces.

■ Création d'un site

Utilisez la commande `lmvutil` avec l'option `--createSite` pour créer un site dans une topologie Architecture Cloud Pod

■ Affectation d'un espace à un site

Utilisez la commande `lmvutil` avec l'option `--assignPodToSite` pour attribuer un espace à un site.

■ Modification du nom ou de la description d'un site

Utilisez la commande `lmvutil` avec l'option `--editSite` pour modifier le nom ou la description d'un site.

■ Suppression d'un site

Utilisez la commande `lmvutil` avec l'option `--deleteSite` pour supprimer un site.

Création d'un site

Utilisez la commande `lmvutil` avec l'option `--createSite` pour créer un site dans une topologie Architecture Cloud Pod.

Syntaxe

```
lmvutil --createSite --siteName sitename [--description text]
```

Notes d'utilisation

Cette commande renvoie un message d'erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée, si le site spécifié existe déjà ou si la commande ne peut pas créer le site.

Options

Vous pouvez spécifier les options suivantes lorsque vous créez un site.

Tableau 5-5. Options permettant de créer un site

Option	Description
<code>--siteName</code>	Nom du nouveau site. Le nom du site peut contenir entre 1 et 64 caractères.
<code>--description</code>	(Facultatif) Description du site. La description peut contenir entre 1 et 1 024 caractères.

Exemple

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --createSite
--siteName "Eastern Region"
```

Affectation d'un espace à un site

Utilisez la commande `lmvutil` avec l'option `--assignPodToSite` pour attribuer un espace à un site.

Syntaxe

```
lmvutil --assignPodToSite --podName podname --siteName sitename
```

Notes d'utilisation

Avant de pouvoir attribuer un espace à un site, vous devez créer le site. Reportez-vous à la section [Création d'un site](#).

Cette commande renvoie un message d'erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée, si la commande ne parvient pas à trouver l'espace ou le site spécifié ou si la commande ne peut pas attribuer l'espace au site.

Options

Vous devez spécifier les options suivantes lorsque vous attribuez un espace à un site.

Tableau 5-6. Options permettant d'attribuer un espace à un site

Option	Description
<code>--podName</code>	Nom de l'espace à attribuer au site.
<code>--siteName</code>	Nom du site.

Vous pouvez utiliser la commande `lmvutil` avec l'option `--listPods` pour répertorier les noms des espaces d'une topologie Architecture Cloud Pod. Reportez-vous à la section [Affichage de la liste des espaces ou des sites dans une topologie Architecture Cloud Pod](#).

Exemple

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--assignPodToSite --podName "East Pod 1" --siteName "Eastern Region"
```

Modification du nom ou de la description d'un site

Utilisez la commande `lmvutil` avec l'option `--editSite` pour modifier le nom ou la description d'un site.

Syntaxe

```
lmvutil --editSite --siteName sitename [--newSiteName sitename] [--description text]
```

Notes d'utilisation

La commande renvoie un message d'erreur si le site spécifié n'existe pas ou si la commande ne peut pas trouver ou mettre à jour le site.

Options

Vous pouvez spécifier ces options lorsque vous modifiez le nom ou la description d'un site.

Tableau 5-7. Options de modification du nom ou de la description d'un site

Option	Description
<code>--siteName</code>	Nom du site à modifier.
<code>--newSiteName</code>	(Facultatif) Nouveau nom du site. Le nom du site peut contenir entre 1 et 64 caractères.
<code>--description</code>	(Facultatif) Description du site. La description peut contenir entre 1 et 1 024 caractères.

Exemple

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --editSite
--siteName "Eastern Region" --newSiteName "Western Region"
```

Suppression d'un site

Utilisez la commande `lmvutil` avec l'option `--deleteSite` pour supprimer un site.

Syntaxe

```
lmvutil --deleteSite --sitename sitename
```

Notes d'utilisation

Cette commande renvoie un message d'erreur si le site spécifié n'existe pas ou si la commande ne peut pas trouver ou supprimer le site.

Options

Vous utilisez l'option `--sitename` pour spécifier le nom du site à supprimer.

Exemple

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--deleteSite --sitename "Eastern Region"
```

Gestion des droits d'accès globaux

Vous pouvez utiliser les options de la commande `lmvutil` pour créer, modifier et répertorier les droits de poste de travail globaux et les droits d'application globaux dans un environnement Architecture Cloud Pod.

■ Création d'un droit d'accès global

Pour créer un droit de poste de travail global, utilisez la commande `lmvutil` avec l'option `--createGlobalEntitlement`. Pour créer un droit d'application global, utilisez la commande `lmvutil` avec l'option `--createGlobalApplicationEntitlement`.

■ Modification d'un droit d'accès global

Pour modifier un droit de poste de travail global, utilisez la commande `lmvutil` avec l'option `--updateGlobalEntitlement`. Pour modifier un droit d'application global, utilisez la commande `lmvutil` avec l'option `--updateGlobalApplicationEntitlement`.

■ Suppression d'un droit d'accès global

Pour supprimer un droit de poste de travail global, utilisez la commande `lmvutil` avec l'option `--deleteGlobalEntitlement`. Pour supprimer un droit d'application global, utilisez la commande `lmvutil` avec l'option `--deleteGlobalApplicationEntitlement`.

■ Ajout d'un pool à un droit d'accès global

Utilisez la commande `lmvutil` avec l'option `--addPoolAssociation` pour ajouter un pool de postes de travail à un droit de poste de travail global ou un pool d'applications à un droit d'application global.

■ Suppression d'un pool d'un droit d'accès global

Utilisez la commande `lmvutil` avec l'option `--removePoolAssociation` pour supprimer un pool de postes de travail d'un droit de poste de travail global ou un pool d'applications d'un droit d'application global.

■ Ajout d'un utilisateur ou d'un groupe à un droit d'accès global

Pour ajouter un utilisateur à un droit d'accès global, utilisez la commande `lmvutil` avec l'option `--addUserEntitlement`. Pour ajouter un groupe à un droit d'accès global, utilisez la commande `lmvutil` avec l'option `--addGroupEntitlement`.

■ Suppression d'un utilisateur ou d'un groupe d'un droit global

Pour supprimer un utilisateur d'un droit d'accès global, utilisez la commande `lmvutil` avec l'option `--removeUserEntitlement`. Pour supprimer un groupe d'un droit d'accès global, utilisez la commande `lmvutil` avec l'option `--removeGroupEntitlement`.

Création d'un droit d'accès global

Pour créer un droit de poste de travail global, utilisez la commande `lmvutil` avec l'option `--createGlobalEntitlement`. Pour créer un droit d'application global, utilisez la commande `lmvutil` avec l'option `--createGlobalApplicationEntitlement`.

Les droits d'accès globaux font le lien entre les utilisateurs et leurs postes de travail et applications, quel que soit l'emplacement de ces postes de travail et applications dans la fédération d'espaces. Les droits d'accès globaux incluent également des stratégies qui déterminent comment la fonctionnalité Architecture Cloud Pod alloue des postes de travail et des applications à des utilisateurs autorisés.

Syntaxe

```
lmvutil --createGlobalEntitlement --entitlementName name --scope scope
[--isDedicated | --isFloating] [--description text] [--disabled]
[--fromHome] [--multipleSessionAutoClean] [--requireHomeSite] [--defaultProtocol value]
[--preventProtocolOverride] [--allowReset] [--htmlAccess] [--multipleSessionsPerUser]
[--tags tags] [--categoryFolder foldername] [--clientRestrictions] [--collaboration]
[--shortcutLocations {desktop | launcher | desktop,launcher}] [--displayAssignedHostName]
```

```
lmvutil --createGlobalApplicationEntitlement --entitlementName name --scope scope
[--description text] [--disabled] [--fromHome] [--multipleSessionAutoClean]
[--requireHomeSite] [--defaultProtocol value] [--preventProtocolOverride] [--htmlAccess]
[--preLaunch] [--tags tags] [--categoryFolder foldername] [--clientRestrictions]
[--shortcutLocations {desktop | launcher | desktop,launcher}] [--multiSessionMode value]
```

Notes d'utilisation

Vous pouvez utiliser ces commandes sur n'importe quelle instance du Serveur de connexion dans une fédération d'espaces. La fonctionnalité Architecture Cloud Pod stocke les nouvelles données dans la couche de données globale et les réplique dans tous les espaces de la fédération d'espaces.

Ces commandes renvoient un message d'erreur si le droit d'accès global existe déjà, si l'étendue n'est pas valide, si la fonctionnalité Architecture Cloud Pod n'est pas initialisée ou si les commandes ne peuvent pas créer le droit d'accès global.

Options

Vous pouvez spécifier les options suivantes lorsque vous créez un droit d'accès global. Certaines options s'appliquent uniquement à des droits de poste de travail globaux.

Tableau 5-8. Options permettant de créer des droits d'accès globaux

Option	Description
<code>--entitlementName</code>	Nom du droit d'accès global. Le nom peut contenir entre 1 et 64 caractères. Le nom du droit d'accès global apparaît dans la liste de postes de travail et d'applications dans Horizon Client pour les utilisateurs autorisés.
<code>--scope</code>	Portée du droit d'accès global. Les valeurs valides sont les suivantes : <ul style="list-style-type: none"> ■ ANY. Horizon recherche des ressources dans n'importe quel espace de la fédération d'espaces. ■ SITE. Horizon recherche des ressources uniquement dans les espaces se trouvant dans le même site que l'espace auquel l'utilisateur est connecté. ■ LOCAL. Horizon recherche des ressources uniquement dans l'espace auquel l'utilisateur est connecté.
<code>--isDedicated</code>	Crée un droit de poste de travail dédié. Un droit de poste de travail dédié peut uniquement contenir des pools de postes de travail dédiés. Pour créer un droit de poste de travail flottant, utilisez l'option <code>--isFloating</code> . Un droit de poste de travail global peut être dédié ou flottant. Vous ne pouvez pas spécifier l'option <code>--isDedicated</code> avec l'option <code>--multipleSessionAutoClean</code> . S'applique uniquement à des droits de poste de travail globaux.
<code>--isFloating</code>	Crée un droit de poste de travail flottant. Un droit de poste de travail flottant peut uniquement contenir des pools de postes de travail flottants. Pour créer un droit de poste de travail dédié, utilisez l'option <code>--isDedicated</code> . Un droit de poste de travail global peut être flottant ou dédié. S'applique uniquement à des droits de poste de travail globaux.
<code>--disabled</code>	(Facultatif) Crée le droit d'accès global à l'état désactivé.
<code>--description</code>	(Facultatif) Description du droit d'accès global. La description peut contenir entre 1 et 1 024 caractères.
<code>--fromHome</code>	(Facultatif) Si l'utilisateur dispose d'un site de base, Horizon commence à rechercher des ressources sur le site de base de l'utilisateur. Si l'utilisateur ne dispose pas d'un site de base, Horizon effectue une recherche des ressources sur le site auquel l'utilisateur est actuellement connecté.

Tableau 5-8. Options permettant de créer des droits d'accès globaux (suite)

Option	Description
<code>--multipleSessionAutoClean</code>	<p>(Facultatif) Ferme les sessions supplémentaires de l'utilisateur pour le même droit d'accès. Plusieurs sessions peuvent être établies lorsqu'un espace contenant une session se déconnecte, lorsque l'utilisateur se reconnecte et démarre une autre session, et lorsque l'espace problématique revient en ligne avec la session d'origine.</p> <p>Lorsque plusieurs sessions sont établies, Horizon Client demande à l'utilisateur de sélectionner une session. Cette option détermine ce qu'il advient des sessions que l'utilisateur ne sélectionne pas.</p> <p>Si vous ne spécifiez pas cette option, les utilisateurs doivent manuellement terminer leurs propres sessions supplémentaires, en fermant la session dans Horizon Client ou en ouvrant les sessions, puis en les fermant.</p>
<code>--requireHomeSite</code>	<p>(Facultatif) Rend le droit d'accès global disponible uniquement si l'utilisateur dispose d'un site de base. Cette option est applicable uniquement lorsque l'option <code>--fromHome</code> est également spécifiée.</p>
<code>--defaultProtocol</code>	<p>(Facultatif) Spécifie le protocole d'affichage par défaut pour les postes de travail ou les applications dans le droit global. Les valeurs valides sont RDP, PCOIP et BLAST pour les droits de poste de travail globaux et PCOIP et BLAST pour les droits d'application globaux.</p>
<code>--preventProtocolOverride</code>	<p>(Facultatif) Empêche les utilisateurs de remplacer le protocole d'affichage par défaut.</p>
<code>--allowReset</code>	<p>(Facultatif) Autorise les utilisateurs à réinitialiser des postes de travail. S'applique uniquement à des droits de poste de travail globaux.</p>
<code>--htmlAccess</code>	<p>(Facultatif) Active la stratégie HTML Access qui permet aux utilisateurs d'employer la fonctionnalité HTML Access pour accéder aux ressources dans le droit global. Avec HTML Access, les utilisateurs finaux peuvent utiliser un navigateur Web pour accéder à des ressources distantes et n'ont pas besoin d'installer un logiciel client sur leurs systèmes locaux.</p>
<code>--multipleSessionsPerUser</code>	<p>(Facultatif) Active la stratégie de sessions multiples par utilisateur, ce qui permet aux utilisateurs d'ouvrir des sessions de poste de travail séparées depuis des périphériques clients différents. Les utilisateurs qui se connectent au droit de poste de travail global depuis des périphériques clients différents reçoivent des sessions de poste de travail différentes. Pour se reconnecter à une session de poste de travail existante, les utilisateurs doivent utiliser le périphérique sur lequel cette session a été initiée. Si vous n'activez pas cette stratégie, les utilisateurs sont toujours reconnectés à leurs sessions de poste de travail existantes, quel que soit le périphérique client qu'ils utilisent. S'applique uniquement à des droits de poste de travail flottants.</p>
<code>--preLaunch</code>	<p>(Facultatif) Active la stratégie de pré-lancement, qui lance la session d'application avant qu'un utilisateur ouvre le droit d'application global dans Horizon Client. Lorsque vous activez la stratégie de pré-lancement, les utilisateurs peuvent lancer plus rapidement le droit d'application global. Tous les pools d'applications dans le droit d'application global doivent prendre en charge la fonctionnalité de pré-lancement de session, et le délai d'expiration de session de pré-lancement doit être le même pour toutes les batteries de serveurs.</p>

Tableau 5-8. Options permettant de créer des droits d'accès globaux (suite)

Option	Description
--tags	(Facultatif) Spécifie une ou plusieurs balises qui limitent l'accès au droit global des instances du Serveur de connexion. Pour spécifier plusieurs balises, saisissez une liste de noms de balises entre guillemets séparés par une virgule ou un point-virgule. Pour plus d'informations, reportez-vous à la section Mise en œuvre des restrictions du Serveur de connexion pour les droits d'accès globaux .
--categoryFolder	(Facultatif) Spécifie le nom du dossier de catégorie qui contient un raccourci pour le droit global sur les périphériques clients. Vous pouvez configurer jusqu'à quatre niveaux de dossier. Un nom de dossier peut comprendre jusqu'à 64 caractères. Pour spécifier un sous-dossier, entrez une barre oblique inversée (\), par exemple, dir1\dir2\dir3\dir4. Vous pouvez entrer jusqu'à quatre niveaux de dossier. Vous ne pouvez pas commencer ni terminer un nom de dossier avec une barre oblique inversée, et vous ne pouvez pas combiner plusieurs barres obliques inversées. Par exemple, \dir1, dir1\dir2\, dir1\\dir2 et dir1\\dir2 ne sont pas valides. Vous ne pouvez pas entrer de mots clés réservés Windows. Vous devez également spécifier l'option --shortcutLocations pour indiquer l'emplacement du raccourci sur un périphérique client Windows. Pour plus d'informations, reportez-vous à la section Configuration des raccourcis pour les droits d'accès globaux .
--clientRestrictions	(Facultatif) Active la stratégie de restrictions du client, qui restreint le droit global à des ordinateurs clients spécifiques. Pour plus d'informations, reportez-vous à la section Mise en œuvre des restrictions du client pour les droits d'accès globaux .
--collaboration	(Facultatif) Active la stratégie de collaboration de session, ce qui permet aux utilisateurs de sessions de poste de travail distantes d'inviter d'autres utilisateurs à rejoindre leurs sessions. Tous les pools de postes de travail dans le droit de poste de travail global doivent prendre en charge la fonctionnalité de collaboration de session. S'applique uniquement à des droits de poste de travail globaux.
--shortcutLocations	(Facultatif) Utilisez cette option avec l'option --categoryFolder pour spécifier l'emplacement du raccourci sur le périphérique client. Les valeurs valides sont desktop, ce qui crée le raccourci sur le poste de travail Windows, et launcher, ce qui crée le raccourci dans le menu Démarrer de Windows. Vous pouvez également spécifier desktop et launcher, séparés par une virgule, pour créer les raccourcis du poste de travail Windows et du menu Démarrer de Windows.
--multiSessionMode	(Facultatif) Configure la fonctionnalité de mode de sessions multiples pour le droit applicatif global. Spécifiez l'une des valeurs suivantes : DISABLED, ENABLED_DEFAULT_OFF, ENABLED_DEFAULT_ON ou ENABLED_ENFORCED. Pour plus d'informations, reportez-vous à la section Activation du mode de sessions multiples pour les droits applicatifs globaux .
--displayAssignedHostName	(Facultatif) Dans Horizon Client, affiche le nom d'hôte de la machine attribuée à l'utilisateur plutôt que le nom du droit global. S'applique uniquement à des droits de poste de travail dédié.

Exemples

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --createGlobalEntitlement --entitlementName "Windows 8 Desktop" --scope LOCAL --isDedicated
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --createGlobalApplicationEntitlement --entitlementName "Microsoft Office PowerPoint" --scope LOCAL
```

Modification d'un droit d'accès global

Pour modifier un droit de poste de travail global, utilisez la commande `lmvutil` avec l'option `--updateGlobalEntitlement`. Pour modifier un droit d'application global, utilisez la commande `lmvutil` avec l'option `--updateGlobalApplicationEntitlement`.

Syntaxe

```
lmvutil --updateGlobalEntitlement --entitlementName name [--description text]
[--disabled] [--enabled] [--fromHome] [--disableFromHome] [--multipleSessionAutoClean]
[--disableMultipleSessionAutoClean] [--multipleSessionsPerUser]
[--disableMultipleSessionsPerUser] [--requireHomeSite] [--disableRequireHomeSite]
[--defaultProtocol value] [--scope scope] [--htmlAccess] [--disableHtmlAccess]
[--tags tags] [--notags] [--categoryFolder foldername] [--disableCategoryFolder]
[--clientRestrictions] [--disableClientRestrictions] [--collaboration]
[--disableCollaboration] [--shortcutLocations {desktop | launcher | desktop,launcher}]
[--backupEntitlementName name] [--disableBackupEntitlement] [--displayAssignedHostName]
[--disableDisplayAssignedHostName]
```

```
lmvutil --updateGlobalApplicationEntitlement --entitlementName name [--description text]
[--disabled] [--enabled] [--fromHome] [--disableFromHome] [--multipleSessionAutoClean]
[--disableMultipleSessionAutoClean] [--requireHomeSite] [--disableRequireHomeSite]
[--defaultProtocol value] [--scope scope] [--htmlAccess] [--disableHtmlAccess]
[--appVersion value] [--appPublisher value] [--appPath value] [--tags tags] [--notags]
[--preLaunch] [--disablePreLaunch] [--categoryFolder foldername] [--disableCategoryFolder]
[--clientRestrictions] [--disableClientRestrictions] [--shortcutLocations {desktop | launcher |
desktop,launcher}]
[--multiSessionMode value] [--backupEntitlementName name] [--disableBackupEntitlement]
```

Notes d'utilisation

Vous pouvez utiliser ces commandes sur n'importe quelle instance du Serveur de connexion dans une fédération d'espaces. La fonctionnalité Architecture Cloud Pod stocke les nouvelles données dans la couche de données globale et les réplique dans tous les espaces de la fédération d'espaces.

Ces commandes renvoient un message d'erreur si le droit d'accès global n'existe pas, si l'étendue n'est pas valide, si la fonctionnalité Architecture Cloud Pod n'est pas initialisée ou si les commandes ne peuvent pas mettre à jour le droit d'accès global.

Options

Vous pouvez spécifier les options suivantes lorsque vous modifiez un droit d'accès global. Certaines options s'appliquent uniquement aux droits de poste de travail global ou uniquement aux droits d'application global.

Tableau 5-9. Options permettant de modifier les droits d'accès globaux

Option	Description
<code>--entitlementName</code>	Nom du droit d'accès global à modifier.
<code>--scope</code>	Portée du droit d'accès global. Les valeurs valides sont les suivantes : <ul style="list-style-type: none"> ■ ANY. Horizon recherche des ressources dans n'importe quel espace de la fédération d'espaces. ■ SITE. Horizon recherche des ressources uniquement dans les espaces se trouvant dans le même site que l'espace auquel l'utilisateur est connecté. ■ LOCAL. Horizon recherche des ressources uniquement dans l'espace auquel l'utilisateur est connecté.
<code>--description</code>	(Facultatif) Description du droit d'accès global. La description peut contenir entre 1 et 1 024 caractères.
<code>--disabled</code>	(Facultatif) Désactive un droit d'accès global précédemment activé.
<code>--enabled</code>	(Facultatif) Active un droit d'accès global précédemment désactivé.
<code>--fromHome</code>	(Facultatif) Si l'utilisateur dispose d'un site de base, Horizon commence à rechercher des ressources sur le site de base de l'utilisateur. Si l'utilisateur ne dispose pas d'un site de base, Horizon effectue une recherche des ressources sur le site auquel l'utilisateur est actuellement connecté.
<code>--disableFromHome</code>	(Facultatif) Désactive la fonction <code>--fromHome</code> pour le droit global.
<code>--multipleSessionAutoClean</code>	(Facultatif) Ferme les sessions supplémentaires de l'utilisateur pour le même droit d'accès. Plusieurs sessions peuvent être établies lorsqu'un espace contenant une session se déconnecte, lorsque l'utilisateur se reconnecte et démarre une autre session, et lorsque l'espace problématique revient en ligne avec la session d'origine. Lorsque plusieurs sessions sont établies, Horizon Client demande à l'utilisateur de sélectionner une session. Cette option détermine ce qu'il advient des sessions que l'utilisateur ne sélectionne pas. Si vous ne spécifiez pas cette option, les utilisateurs doivent manuellement terminer leurs propres sessions supplémentaires, en fermant la session dans Horizon Client ou en ouvrant les sessions, puis en les fermant.
<code>--disableMultipleSessionAutoClean</code>	(Facultatif) Désactive la fonction <code>--multipleSessionAutoClean</code> pour le droit global.

Tableau 5-9. Options permettant de modifier les droits d'accès globaux (suite)

Option	Description
--multipleSessionsPerUser	(Facultatif) Active la stratégie de sessions multiples par utilisateur, ce qui permet aux utilisateurs d'ouvrir des sessions de poste de travail séparées depuis des périphériques clients différents. Les utilisateurs qui se connectent au droit de poste de travail global depuis des périphériques clients différents reçoivent des sessions de poste de travail différentes. Pour se reconnecter à une session de poste de travail existante, les utilisateurs doivent utiliser le périphérique sur lequel cette session a été initiée. Si vous n'activez pas cette stratégie, les utilisateurs sont toujours reconnectés à leurs sessions de poste de travail existantes, quel que soit le périphérique client qu'ils utilisent. S'applique uniquement à des droits de poste de travail flottants.
--disableMultipleSessionsPerUser	(Facultatif) Désactive la stratégie de sessions multiples par utilisateur pour le droit de poste de travail global.
--requireHomeSite	(Facultatif) Rend le droit d'accès global disponible uniquement si l'utilisateur dispose d'un site de base. Cette option est applicable uniquement lorsque l'option --fromHome est également spécifiée.
--disableRequireHomeSite	(Facultatif) Désactive la fonction --requireHomeSite pour le droit global.
--defaultProtocol	(Facultatif) Spécifie le protocole d'affichage par défaut pour les postes de travail ou les applications dans le droit global. Les valeurs valides sont RDP, PCOIP et BLAST pour les droits de poste de travail globaux et PCOIP et BLAST pour les droits d'application globaux.
--htmlAccess	(Facultatif) Active la stratégie HTML Access qui permet aux utilisateurs d'employer la fonctionnalité HTML Access pour accéder aux ressources dans le droit global. Avec HTML Access, les utilisateurs finaux peuvent utiliser un navigateur Web pour accéder à des ressources distantes et n'ont pas besoin d'installer un logiciel client sur leurs systèmes locaux.
--disableHtmlAccess	(Facultatif) Désactive la stratégie HTML Access pour le droit global.
--appVersion	(Facultatif) Version de l'application. S'applique uniquement à des droits d'application globaux.
--appPublisher	(Facultatif) Éditeur de l'application. S'applique uniquement à des droits d'application globaux.
--appPath	(Facultatif) Nom du chemin d'accès complet de l'application, par exemple, C:\Program Files\app1.exe. S'applique uniquement à des droits d'application globaux.
--tags	(Facultatif) Spécifie une ou plusieurs balises qui limitent l'accès au droit global des instances du Serveur de connexion. Pour spécifier plusieurs balises, saisissez une liste de noms de balises entre guillemets séparés par une virgule ou un point-virgule. Pour plus d'informations, reportez-vous à la section Mise en œuvre des restrictions du Serveur de connexion pour les droits d'accès globaux .
--notags	(Facultatif) Supprime les balises du droit global.

Tableau 5-9. Options permettant de modifier les droits d'accès globaux (suite)

Option	Description
<code>--preLaunch</code>	(Facultatif) Active la stratégie de pré-lancement, qui lance la session d'application avant qu'un utilisateur ouvre le droit d'application global dans Horizon Client. Lorsque vous activez la stratégie de pré-lancement, les utilisateurs peuvent lancer plus rapidement le droit d'application global. Tous les pools d'applications dans le droit d'application global doivent prendre en charge la fonctionnalité de pré-lancement de session, et le délai d'expiration de session de pré-lancement doit être le même pour toutes les batteries de serveurs.
<code>--disablePreLaunch</code>	(Facultatif) Désactive la stratégie de pré-lancement pour le droit d'application global.
<code>--categoryFolder</code>	(Facultatif) Spécifie le nom du dossier de catégorie qui contient un raccourci pour le droit global sur les périphériques clients. Vous pouvez configurer jusqu'à quatre niveaux de dossier. Un nom de dossier peut comprendre jusqu'à 64 caractères. Pour spécifier un sous-dossier, entrez une barre oblique inversée (\), par exemple, <code>dir1\dir2\dir3\dir4</code> . Vous pouvez entrer jusqu'à quatre niveaux de dossier. Vous ne pouvez pas commencer ni terminer un nom de dossier avec une barre oblique inversée, et vous ne pouvez pas combiner plusieurs barres obliques inversées. Par exemple, <code>\dir1</code> , <code>dir1\dir2\</code> , <code>dir1\dir2</code> et <code>dir1\\dir2</code> ne sont pas valides. Vous ne pouvez pas entrer de mots clés réservés Windows. Vous devez également spécifier l'option <code>--shortcutLocations</code> pour indiquer l'emplacement du raccourci sur un périphérique client Windows. Pour plus d'informations, reportez-vous à la section Configuration des raccourcis pour les droits d'accès globaux .
<code>--disableCategoryFolder</code>	(Facultatif) Supprime le dossier de catégorie pour le droit global.
<code>--clientRestrictions</code>	(Facultatif) Active la stratégie de restrictions du client, qui restreint le droit global à des ordinateurs clients spécifiques. Pour plus d'informations, reportez-vous à la section Mise en œuvre des restrictions du client pour les droits d'accès globaux .
<code>--disableClientRestrictions</code>	(Facultatif) Désactive la stratégie de restrictions du client pour les droits globaux.
<code>--collaboration</code>	(Facultatif) Active la stratégie de collaboration de session, ce qui permet aux utilisateurs de sessions de poste de travail distantes d'inviter d'autres utilisateurs à rejoindre leurs sessions. Tous les pools de postes de travail dans le droit de poste de travail global doivent prendre en charge la fonctionnalité de collaboration de session. S'applique uniquement à des droits de poste de travail globaux.
<code>--disableCollaboration</code>	(Facultatif) Désactive la stratégie de collaboration de session pour le droit de poste de travail global.

Tableau 5-9. Options permettant de modifier les droits d'accès globaux (suite)

Option	Description
<code>--shortcutLocations</code>	<p>(Facultatif) Utilisez cette option pour modifier ou créer un raccourci sur le périphérique client. Les valeurs valides sont <code>desktop</code>, ce qui crée le raccourci sur le poste de travail, et <code>launcher</code>, ce qui crée le raccourci dans le menu Démarrer de Windows. Vous pouvez également spécifier <code>desktop</code> et <code>launcher</code>, séparés par une virgule, pour créer les raccourcis du poste de travail et du menu Démarrer de Windows.</p> <p>Si vous modifiez un raccourci (autrement dit, le dossier de catégorie a déjà été créé), vous n'avez pas besoin de spécifier l'option <code>--categoryFolder</code>, sauf si vous souhaitez également modifier le nom du dossier de catégorie.</p> <p>Si le dossier de catégorie n'a pas été créé, vous devez spécifier l'option <code>--categoryFolder</code> en même temps que l'option <code>--shortcutLocations</code>.</p> <p>Note N'utilisez pas cette option avec l'option <code>--disableCategoryFolder</code>.</p>
<code>--multiSessionMode</code>	<p>(Facultatif) Configure la fonctionnalité de mode de sessions multiples pour le droit applicatif global. Spécifiez l'une des valeurs suivantes : <code>DISABLED</code>, <code>ENABLED_DEFAULT_OFF</code>, <code>ENABLED_DEFAULT_ON</code> ou <code>ENABLED_ENFORCED</code>. Pour plus d'informations, reportez-vous à la section Activation du mode de sessions multiples pour les droits applicatifs globaux.</p>
<code>--backupEntitlementName</code>	<p>(Facultatif) Spécifie le nom d'un droit global de sauvegarde. Un droit global de sauvegarde fournit des applications publiées ou des postes de travail distants lorsque le droit global principal ne peut pas démarrer une session. Pour les droits de poste de travail globaux, le type d'attribution d'utilisateur doit être Flottant. Pour plus d'informations, reportez-vous à la section Implémentation des droits globaux de sauvegarde.</p>
<code>--disableBackupEntitlement</code>	<p>(Facultatif) Désactive le droit global de sauvegarde.</p>
<code>--displayAssignedHostName</code>	<p>(Facultatif) Dans Horizon Client, affiche le nom d'hôte de la machine attribuée à l'utilisateur plutôt que le nom du droit global. S'applique uniquement à des droits de poste de travail dédié.</p>
<code>--disableDisplayAssignedHostName</code>	<p>(Facultatif) Spécifie que le nom d'hôte de la machine attribuée ne s'affiche pas dans Horizon Client. S'applique uniquement à des droits de poste de travail dédié.</p>

Exemples

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --updateGlobalEntitlement --entitlementName "Windows 8 Desktop" --scope ANY --isDedicated
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --updateGlobalApplicationEntitlement --entitlementName "Microsoft Office PowerPoint" --scope ANY
```

Suppression d'un droit d'accès global

Pour supprimer un droit de poste de travail global, utilisez la commande `lmvutil` avec l'option `--deleteGlobalEntitlement`. Pour supprimer un droit d'application global, utilisez la commande `lmvutil` avec l'option `--deleteGlobalApplicationEntitlement`.

Syntaxe

```
lmvutil --deleteGlobalEntitlement --entitlementName name
```

```
lmvutil --deleteGlobalApplicationEntitlement --entitlementName name
```

Utilisation de la commande

Ces commandes renvoient un message d'erreur si le droit d'accès global spécifié n'existe pas, si la fonctionnalité Architecture Cloud Pod n'est pas initialisée ou si les commandes ne peuvent pas supprimer le droit d'accès global.

Options

Vous utilisez l'option `--entitlementName` pour spécifier le nom du droit d'accès global à supprimer.

Exemples

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--deleteGlobalEntitlement --entitlementName "Windows 8 Desktop"
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--deleteGlobalApplicationEntitlement --entitlementName "Microsoft Office PowerPoint"
```

Ajout d'un pool à un droit d'accès global

Utilisez la commande `lmvutil` avec l'option `--addPoolAssociation` pour ajouter un pool de postes de travail à un droit de poste de travail global ou un pool d'applications à un droit d'application global.

Syntaxe

```
lmvutil --addPoolAssociation --entitlementName name --poolId poolid
```

Notes d'utilisation

Vous devez utiliser cette commande sur une instance du Serveur de connexion de l'espace contenant le pool. Par exemple, si `pod1` contient un pool de postes de travail à associer à un droit de poste de travail global, vous devez exécuter la commande sur une instance du Serveur de connexion résidant dans `pod1`.

Répétez cette commande pour chaque pool à ajouter au droit d'accès global. Vous pouvez ajouter un pool particulier à un seul droit d'accès global.

Important Si vous ajoutez plusieurs pools d'applications à un droit d'application global, vous devez ajouter la même application. Par exemple, n'ajoutez pas la Calculatrice et Microsoft Office PowerPoint au même droit d'application global. Si vous ajoutez différentes applications, les résultats seront imprévisibles et les utilisateurs autorisés recevront différentes applications à des moments différents.

Cette commande renvoie un message d'erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée, si le droit d'accès spécifié n'existe pas, si le pool est déjà associé au droit d'accès spécifié, si le pool n'existe pas ou si la commande ne peut pas ajouter le pool au droit d'accès global.

Options

Vous pouvez spécifier les options suivantes lorsque vous ajoutez un pool à un droit d'accès global.

Tableau 5-10. Options permettant d'ajouter un pool à un droit d'accès global

Option	Description
<code>--entitlementName</code>	Nom du droit d'accès global.
<code>--poolId</code>	ID du pool à ajouter au droit d'accès global. L'ID du pool doit correspondre au nom du pool tel qu'il est affiché sur l'espace.

Exemple

```
lsmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --addPoolAssociation
--entitlementName "Windows 8 Desktop" --poolId "Windows 8 Desktop Pool A"
```

Suppression d'un pool d'un droit d'accès global

Utilisez la commande `lsmvutil` avec l'option `--removePoolAssociation` pour supprimer un pool de postes de travail d'un droit de poste de travail global ou un pool d'applications d'un droit d'application global.

Syntaxe

```
lsmvutil --removePoolAssociation --entitlementName name --poolId poolid
```

Notes d'utilisation

Cette commande renvoie un message d'erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée, si le droit d'accès global ou le pool spécifié n'existe pas ou si la commande ne peut pas supprimer le pool du droit d'accès global.

Options

Vous pouvez spécifier les options suivantes lorsque vous supprimez un pool d'un droit d'accès global.

Tableau 5-11. Options de suppression d'un pool d'un droit d'accès global

Option	Description
<code>--entitlementName</code>	Nom du droit d'accès global.
<code>--poolId</code>	ID du pool à supprimer du droit d'accès global. L'ID du pool doit correspondre au nom du pool tel qu'il est affiché sur l'espace.

Exemple

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--removePoolAssociation --entitlementName "Windows 8 Desktop" --poolId "Windows 8 Desktop Pool A"
```

Ajout d'un utilisateur ou d'un groupe à un droit d'accès global

Pour ajouter un utilisateur à un droit d'accès global, utilisez la commande `lmvutil` avec l'option `--addUserEntitlement`. Pour ajouter un groupe à un droit d'accès global, utilisez la commande `lmvutil` avec l'option `--addGroupEntitlement`.

Syntaxe

```
lmvutil --addUserEntitlement --userName domain\username --entitlementName name
```

```
lmvutil --addGroupEntitlement --groupName domain\groupname --entitlementName name
```

Notes d'utilisation

Répétez ces commandes pour chaque utilisateur ou groupe à ajouter au droit d'accès global.

Ces commandes renvoient un message d'erreur si le droit d'accès, l'utilisateur ou le groupe spécifié n'existe pas ou si la commande ne peut pas ajouter l'utilisateur ou le groupe au droit d'accès.

Options

Vous pouvez spécifier les options suivantes lorsque vous ajoutez un utilisateur ou un groupe à un droit d'accès global.

Tableau 5-12. Options permettant d'ajouter un utilisateur ou un groupe à un droit d'accès global

Option	Description
<code>--userName</code>	Nom d'un utilisateur à ajouter au droit d'accès global. Utilisez le format <i>domain\username</i> .
<code>--groupName</code>	Nom d'un groupe à ajouter au droit d'accès global. Utilisez le format <i>domain\groupname</i> .
<code>--entitlementName</code>	Nom du droit d'accès global auquel ajouter l'utilisateur ou le groupe.

Exemples

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --addUserEntitlement
--userName domainCentral\adminCentral --entitlementName "Agent Sales"
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--addGroupEntitlement --groupName domainCentral\adminCentralGroup --entitlementName "Agent Sales"
```

Suppression d'un utilisateur ou d'un groupe d'un droit global

Pour supprimer un utilisateur d'un droit d'accès global, utilisez la commande `lmvutil` avec l'option `--removeUserEntitlement`. Pour supprimer un groupe d'un droit d'accès global, utilisez la commande `lmvutil` avec l'option `--removeGroupEntitlement`.

Syntaxe

```
lmvutil --removeUserEntitlement --userName domain\username --entitlementName name
```

```
lmvutil --removeGroupEntitlement --groupName domain\groupname --entitlementName name
```

Notes d'utilisation

Ces commandes renvoient un message d'erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée, si le nom d'utilisateur, le nom de groupe ou le droit d'accès spécifié n'existe pas, ou si la commande ne peut pas supprimer l'utilisateur ou le groupe du droit d'accès.

Options

Vous devez spécifier les options suivantes lorsque vous supprimez un utilisateur ou un groupe d'un droit d'accès global.

Tableau 5-13. Options de suppression d'un utilisateur ou d'un groupe d'un droit global

Option	Description
<code>--userName</code>	Nom d'un utilisateur à supprimer du droit d'accès global. Utilisez le format <i>domain\username</i> .
<code>--groupName</code>	Nom d'un groupe à supprimer du droit d'accès global. Utilisez le format <i>domain\groupname</i> .
<code>--entitlementName</code>	Nom du droit d'accès global duquel supprimer l'utilisateur ou le groupe.

Exemples

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--removeUserEntitlement --userName domainCentral\adminCentral --entitlementName "Agent Sales"
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--removeGroupEntitlement --groupName domainCentral\adminCentralGroup --entitlementName "Agent Sales"
```

Gestion des sites de base

Vous pouvez utiliser les options de la commande `lmvutil` pour créer, modifier, supprimer et répertorier des sites de base.

■ Configuration d'un site de base

Pour créer un site de base pour un utilisateur, utilisez la commande `lmvutil` avec l'option `--createUserHomeSite`. Pour créer un site de base pour un groupe, utilisez la commande `lmvutil` avec l'option `--createGroupHomeSite`. Vous pouvez également utiliser ces options pour associer un site de base à un droit de poste de travail ou d'application global.

■ Suppression d'un site de base

Pour supprimer l'association entre un utilisateur et un site de base, utilisez la commande `lmvutil` avec l'option `--deleteUserHomeSite`. Pour supprimer l'association entre un groupe et un site de base, utilisez la commande `lmvutil` avec l'option `--deleteGroupHomeSite`.

Configuration d'un site de base

Pour créer un site de base pour un utilisateur, utilisez la commande `lmvutil` avec l'option `--createUserHomeSite`. Pour créer un site de base pour un groupe, utilisez la commande `lmvutil` avec l'option `--createGroupHomeSite`. Vous pouvez également utiliser ces options pour associer un site de base à un droit de poste de travail ou d'application global.

Syntaxe

```
lmvutil --createUserHomeSite --userName domain\username --siteName name [--entitlementName name]
```

```
lmvutil --createGroupHomeSite --groupName domain\groupname --siteName name [--entitlementName name]
```

Notes d'utilisation

Vous devez créer un site avant de pouvoir le configurer comme site de base. Reportez-vous à la section [Création d'un site](#).

Ces commandes renvoient un message d'erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée, si l'utilisateur, le groupe, le site ou le droit spécifié n'existe pas ou si les commandes ne peuvent pas créer de site de base.

Options

Vous pouvez spécifier les options suivantes lorsque vous créez un site de base pour un utilisateur ou un groupe.

Tableau 5-14. Options permettant de créer un site de base pour un utilisateur ou un groupe

Option	Description
<code>--userName</code>	Nom d'un utilisateur à associer au site de base. Utilisez le format <i>domain\username</i> .
<code>--groupName</code>	Nom d'un groupe à associer au site de base. Utilisez le format <i>domain\groupname</i> .
<code>--siteName</code>	Nom du site à associer à l'utilisateur ou au groupe comme site de base.
<code>--entitlementName</code>	(Facultatif) Nom d'un droit de poste de travail ou d'application global à associer au site de base. Lorsqu'un utilisateur sélectionne le droit d'accès global spécifié, le site de base remplace le site de base de l'utilisateur. Si vous ne spécifiez pas cette option, la commande crée un site de base d'utilisateur ou de groupe global.

Exemples

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --createUserHomeSite --userName domainEast\adminEast --siteName "Eastern Region" --entitlementName "Agent Sales"
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--createGroupHomeSite --groupName domainEast\adminEastGroup --siteName "Eastern Region"
--entitlementName "Agent Sales"
```

Suppression d'un site de base

Pour supprimer l'association entre un utilisateur et un site de base, utilisez la commande `lmvutil` avec l'option `--deleteUserHomeSite`. Pour supprimer l'association entre un groupe et un site de base, utilisez la commande `lmvutil` avec l'option `--deleteGroupHomeSite`.

Syntaxe

```
lmvutil --deleteUserHomeSite --userName domain\username [--entitlementName name]
```

```
lmvutil --deleteGroupHomeSite --groupName domain\groupname [--entitlementName name]
```

Notes d'utilisation

Ces commandes renvoient un message d'erreur si le droit d'accès global, l'utilisateur ou le groupe spécifié n'existe pas, ou si les commandes ne peuvent pas supprimer le paramètre du site de base.

Options

Vous pouvez spécifier ces options lorsque vous supprimez l'association entre un utilisateur ou un groupe et un site de base.

Tableau 5-15. Options de suppression d'un site de base

Option	Description
<code>--userName</code>	Nom d'un utilisateur. Utilisez le format <i>domain\username</i> .
<code>--groupName</code>	Nom d'un groupe. Utilisez le format <i>domain\groupname</i> .
<code>--entitlementName</code>	(Facultatif) Nom d'un droit de poste de travail global ou d'un droit d'application global. Vous pouvez utiliser cette option pour supprimer l'association entre le site de base et un droit d'accès global pour l'utilisateur ou le groupe spécifié.

Exemples

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --deleteUserHomeSite
--userName domainEast\adminEast
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--deleteGroupHomeSite --groupName domainEast\adminEastGroup
```

Affichage d'une configuration Architecture Cloud Pod

Vous pouvez utiliser les options de la commande `lmvutil` pour répertorier les informations sur une configuration Architecture Cloud Pod.

- [Affichage de la liste des droits d'accès globaux](#)

Pour répertorier les informations sur tous les droits de poste de travail globaux, notamment leurs stratégies et leurs attributs, utilisez la commande `lmvutil` avec l'option `--listGlobalEntitlements`. Pour répertorier les informations sur tous les droits d'application globaux, notamment leurs stratégies et leurs attributs, utilisez la commande `lmvutil` avec l'option `--listGlobalApplicationEntitlements`.

- [Affichage de la liste des pools d'un droit d'accès global](#)

Utilisez la commande `lmvutil` avec l'option `--listAssociatedPools` pour répertorier les pools de postes de travail ou d'applications associés à un droit d'accès global spécifique.

- [Affichage de la liste des utilisateurs ou des groupes d'un droit d'accès global](#)

Utilisez la commande `lmvutil` avec l'option `--listEntitlements` pour répertorier tous les utilisateurs ou les groupes associés à un droit d'accès global spécifique.

- [Affichage de la liste des sites de base d'un utilisateur ou d'un groupe](#)

Pour répertorier tous les sites de base configurés d'un utilisateur spécifique, utilisez la commande `lmvutil` avec l'option `--showUserHomeSites`. Pour répertorier tous les sites de base configurés d'un groupe spécifique, utilisez la commande `lmvutil` avec l'option `--showGroupHomeSites`.

- **Affichage du site de base effectif d'un utilisateur**

Utilisez la commande `lmvutil` avec l'option `--resolveUserHomeSite` pour déterminer le site de base effectif d'un utilisateur spécifique. Comme les sites de base peuvent être attribués à des utilisateurs, à des groupes et à des droits d'accès globaux, il est possible de configurer plusieurs sites de base pour un utilisateur.

- **Affichage de la liste des attributions de pool de postes de travail dédiés**

Utilisez la commande `lmvutil` avec l'option `--listUserAssignments` pour répertorier les attributions de pools de postes de travail dédiés pour une combinaison d'utilisateur et de droit d'accès global.

- **Affichage de la liste des espaces ou des sites dans une topologie Architecture Cloud Pod**

Pour afficher les espaces dans la fédération d'espaces, utilisez la commande `lmvutil` avec l'option `--listPods`. Pour afficher les sites dans la fédération d'espaces, utilisez la commande `lmvutil` avec l'option `--listSites`.

Affichage de la liste des droits d'accès globaux

Pour répertorier les informations sur tous les droits de poste de travail globaux, notamment leurs stratégies et leurs attributs, utilisez la commande `lmvutil` avec l'option `--listGlobalEntitlements`. Pour répertorier les informations sur tous les droits d'application globaux, notamment leurs stratégies et leurs attributs, utilisez la commande `lmvutil` avec l'option `--listGlobalApplicationEntitlements`.

Syntaxe

```
lmvutil --listGlobalEntitlements
```

```
lmvutil --listGlobalApplicationEntitlements
```

Notes d'utilisation

Ces commandes renvoient un message d'erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée ou si les commandes ne peuvent pas répertorier les droits d'accès globaux.

Exemples

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --listGlobalEntitlements
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--listGlobalApplicationEntitlements
```

Affichage de la liste des pools d'un droit d'accès global

Utilisez la commande `lmvutil` avec l'option `--listAssociatedPools` pour répertorier les pools de postes de travail ou d'applications associés à un droit d'accès global spécifique.

Syntaxe

```
lmvutil --listAssociatedPools --entitlementName name
```

Notes d'utilisation

Cette commande renvoie un message d'erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée ou si le droit d'accès global spécifié n'existe pas.

Options

Vous utilisez l'option `--entitlementName` pour spécifier le nom du droit d'accès global pour lequel répertorier les pools de postes de travail ou d'applications associés.

Exemple

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --listAssociatedPools
--entitlementName "Agent Sales"
```

Affichage de la liste des utilisateurs ou des groupes d'un droit d'accès global

Utilisez la commande `lmvutil` avec l'option `--listEntitlements` pour répertorier tous les utilisateurs ou les groupes associés à un droit d'accès global spécifique.

Syntaxe

```
lmvutil --listEntitlements {--userName domain\username | --groupName domain\groupname | --
entitlementName name}
```

Notes d'utilisation

Cette commande renvoie un message d'erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée ou si l'utilisateur, le groupe ou le droit d'accès spécifié n'existe pas.

Options

Vous pouvez spécifier ces options lorsque vous répertoriez des associations de droits d'accès globaux.

Tableau 5-16. Options permettant de répertorier les associations de droits d'accès globaux

Option	Description
<code>--userName</code>	Nom de l'utilisateur pour lequel vous souhaitez répertorier les droits d'accès globaux. Utilisez le format <i>domain\username</i> . Cette option répertorie tous les droits d'accès globaux associés à l'utilisateur spécifié.
<code>--groupName</code>	Nom du groupe pour lequel vous souhaitez répertorier les droits d'accès globaux. Utilisez le format <i>domain\groupname</i> . Cette option répertorie tous les droits d'accès globaux associés au groupe spécifié.
<code>--entitlementName</code>	Nom d'un droit d'accès global. Cette option répertorie tous les utilisateurs et groupes du droit d'accès global spécifié.

Exemple

```
lsmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --listEntitlements
--userName example\adminEast
```

Affichage de la liste des sites de base d'un utilisateur ou d'un groupe

Pour répertorier tous les sites de base configurés d'un utilisateur spécifique, utilisez la commande `lsmvutil` avec l'option `--showUserHomeSites`. Pour répertorier tous les sites de base configurés d'un groupe spécifique, utilisez la commande `lsmvutil` avec l'option `--showGroupHomeSites`.

Syntaxe

```
lsmvutil --showUserHomeSites --userName domain\username [--entitlementName name]
```

```
lsmvutil --showGroupHomeSites --groupName domain\groupname [--entitlementName name]
```

Notes d'utilisation

Ces commandes renvoient un message d'erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée ou si l'utilisateur, le groupe ou le droit d'accès global spécifié n'existe pas.

Options

Vous pouvez spécifier les options suivantes lorsque vous affichez les sites de base d'un utilisateur ou d'un groupe.

Tableau 5-17. Options permettant d'afficher les sites de base d'un utilisateur ou d'un groupe

Option	Description
<code>--userName</code>	Nom d'un utilisateur. Utilisez le format <i>domain\username</i> .
<code>--groupName</code>	Nom d'un groupe. Utilisez le format <i>domain\groupname</i> .
<code>--entitlementName</code>	(Facultatif) nom d'un droit d'accès global. Utilisez cette option si vous voulez afficher tous les sites de base pour une combinaison d'utilisateur ou de groupe et de droit d'accès global.

Exemple

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --showUserHomeSites
--userName example\adminEast
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --showGroupHomeSites
--groupName example\adminEastGroup
```

Affichage du site de base effectif d'un utilisateur

Utilisez la commande `lmvutil` avec l'option `--resolveUserHomeSite` pour déterminer le site de base effectif d'un utilisateur spécifique. Comme les sites de base peuvent être attribués à des utilisateurs, à des groupes et à des droits d'accès globaux, il est possible de configurer plusieurs sites de base pour un utilisateur.

Syntaxe

```
lmvutil --resolveUserHomeSite --entitlementName name --userName domain\username
```

Notes d'utilisation

Cette commande renvoie un message d'erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée ou si le droit d'accès global ou l'utilisateur spécifié n'existe pas.

Options

Vous devez spécifier les options suivantes lorsque vous affichez le site de base effectif d'un utilisateur.

Tableau 5-18. Options permettant d'afficher le site de base effectif d'un utilisateur

Option	Description
<code>--entitlementName</code>	Nom d'un droit d'accès global. Cette option permet de déterminer le site de base effectif pour une combinaison d'utilisateur et de droit d'accès global. Ce site de base peut être différent du site de base configuré pour l'utilisateur.
<code>--userName</code>	Nom de l'utilisateur dont vous souhaitez répertorier le site de base. Utilisez le format <i>domain\username</i> .

Exemple

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--resolveUserHomeSite --userName domainEast\adminEast
```

Affichage de la liste des attributions de pool de postes de travail dédiés

Utilisez la commande `lmvutil` avec l'option `--listUserAssignments` pour répertorier les attributions de pools de postes de travail dédiés pour une combinaison d'utilisateur et de droit d'accès global.

Syntaxe

```
lmvutil --listUserAssignments {--userName domain\username | --entitlementName name | --podName name | --siteName name}
```

Notes d'utilisation

Les données produites par cette commande sont gérées en interne par le logiciel d'échanges Architecture Cloud Pod.

Cette commande renvoie une erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée ou si la commande ne peut pas trouver l'utilisateur, le droit d'accès global, l'espace ou le site spécifié.

Options

Vous devez spécifier l'une des options suivantes lorsque vous répertoriez les attributions d'un utilisateur.

Tableau 5-19. Options permettant d'afficher la liste des attributions d'un utilisateur

Option	Description
--userName	Nom de l'utilisateur pour lequel vous souhaitez répertorier les attributions. Utilisez le format <i>domain\username</i> . Cette option répertorie les attributions de droits d'accès globaux, d'espaces et de sites de l'utilisateur spécifié.
--entitlementName	Nom d'un droit d'accès global. Cette option répertorie les utilisateurs auxquels le droit d'accès global spécifié est accordé.
--podName	Nom d'un espace. Cette option répertorie les utilisateurs auxquels l'espace spécifié est accordé.
--siteName	Nom d'un site. Cette option répertorie les utilisateurs auxquels le site spécifié est accordé.

Exemple

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --listUserAssignments --podName "East Pod 1"
```

Affichage de la liste des espaces ou des sites dans une topologie Architecture Cloud Pod

Pour afficher les espaces dans la fédération d'espaces, utilisez la commande `lmvutil` avec l'option `--listPods`. Pour afficher les sites dans la fédération d'espaces, utilisez la commande `lmvutil` avec l'option `--listSites`.

Syntaxe

```
lmvutil --listPods
```

```
lmvutil --listSites
```

Notes d'utilisation

Ces commandes renvoient un message d'erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée ou si les commandes ne peuvent pas répertorier les espaces ou les sites.

Exemple

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --listPods
```

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*" --listSites
```

Gestion des certificats SSL

Vous pouvez utiliser les options de la commande `lmvutil` pour créer et activer les certificats SSL en attente dans un environnement Architecture Cloud Pod.

La fonctionnalité Architecture Cloud Pod utilise les certificats signés afin que les SSL bidirectionnels protègent et valident le canal de communication VIPA. Les certificats sont distribués dans la couche de données globale. La fonctionnalité Architecture Cloud Pod remplace ces certificats tous les sept jours.

Pour modifier un certificat pour une instance du Serveur de connexion spécifique, créez un certificat en attente, attendez que le processus de réplication de la couche de données globale distribue le certificat à toutes les instances du Serveur de connexion, puis activez le certificat.

Les options du certificat de la commande `lmvutil` sont destinées à être utilisées uniquement si un certificat est compromis et qu'un administrateur Horizon souhaite mettre à jour le certificat avant l'expiration des sept jours. Ces options affectent uniquement l'instance du Serveur de connexion sur laquelle elles s'exécutent. Pour modifier tous les certificats, vous devez exécuter les options sur chaque instance du Serveur de connexion.

■ [Création d'un certificat en attente](#)

Utilisez la commande `lmvutil` avec l'option `--createPendingCertificate` pour créer un certificat SSL en attente.

■ [Activation d'un certificat en attente](#)

Utilisez la commande `lmvutil` avec l'option `--activatePendingCertificate` pour activer un certificat en attente.

Création d'un certificat en attente

Utilisez la commande `lmvutil` avec l'option `--createPendingCertificate` pour créer un certificat SSL en attente.

Syntaxe

```
lmvutil --createPendingCertificate
```


Notes d'utilisation

Cette commande renvoie un message d'erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée ou si la commande ne peut pas créer le certificat.

Exemple

```
LMVUtil --authAs adminEast --authDomain domainEast --authPassword "*"
--createPendingCertificate
```

Activation d'un certificat en attente

Utilisez la commande `lmvutil` avec l'option `--activatePendingCertificate` pour activer un certificat en attente.

Syntaxe

```
lmvutil --activatePendingCertificate
```

Notes d'utilisation

Vous devez utiliser la commande `lmvutil` avec l'option `--createPendingCertificate` pour créer un certificat en attente avant de pouvoir utiliser cette commande. Attendez que le processus de réplication de la couche de données globale distribue le certificat à toutes les instances du Serveur de connexion avant d'activer le certificat en attente. Des échecs de connexion VIPA et des problèmes de négociation qui en résultent peuvent se produire si vous activez un certificat en attente avant qu'il ne soit entièrement répliqué sur toutes les instances du Serveur de connexion.

Cette commande renvoie un message d'erreur si la fonctionnalité Architecture Cloud Pod n'est pas initialisée ou si la commande ne peut pas activer le certificat.

Exemple

```
lmvutil --authAs adminEast --authDomain domainEast --authPassword "*"
--activatePendingCertificate
```