Utilisation du plan de contrôle Horizon de nouvelle génération, d'Horizon Cloud Service et d'une instance d'Horizon 8 connectée au cloud

Mise à jour pour le service à partir d'avril 2024

VMware Horizon Cloud Service - next-gen

vmware by Broadcom

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

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

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

Table des matières

Utilisation du plan de contrôle Horizon de nouvelle génération, d'Horizon Cloud Service et d'une instance d'Horizon 8 connectée au cloud

1

Le plan de contrôle Horizon est hébergé dans le cloud et fournit des services SaaS utilisés avec vos déploiements d'Horizon connectés au cloud.

Il existe deux cas d'utilisation principaux pour le plan de contrôle Horizon :

- Plate-forme de déploiement d'Horizon Cloud Service (DaaS). Actuellement, seul Horizon Cloud Service on Azure est disponible.
- Plan de contrôle pour la connexion à des espaces Horizon 8 et la distribution facultative de services SaaS communs. Les espaces Horizon 8 déployés sur site et sur des SDDC de cloud public peuvent être connectés au plan de contrôle Horizon et utiliser des services SaaS supplémentaires.

Cette publication est destinée aux administrateurs souhaitant fournir des applications et des postes de travail virtuels à grande échelle aux utilisateurs finaux de leur organisation et gérer efficacement ces applications et postes de travail virtuels à l'aide du plan de contrôle Horizon et de la console Horizon Universal Console. .

Avantages du plan de contrôle Horizon - Déploiements de Microsoft Azure en mode natif

Cette section répertorie les avantages du plan de contrôle Horizon de nouvelle génération pour les déploiements dans Microsoft Azure en mode natif.

Ceux-ci ne s'appliquent pas à l'autre cas d'utilisation d'espaces Horizon 8 se connectant au plan de contrôle Horizon consommant des services SaaS supplémentaires.

Note Reportez-vous à la section *Nouveautés* des Notes de mise à jour d'Horizon Cloud Service - next-gen pour connaître les fonctionnalités et capacités supplémentaires dès qu'elles seront disponibles.

Coût réduit

Un dispositif Horizon Edge avec une infrastructure légère de type thin-edge et des déploiements sans espace permet de réduire les coûts opérationnels, d'accélérer le retour

sur investissement et de réduire la maintenance en éliminant les composants d'infrastructure d'Horizon.

Amélioration de la visibilité et du dépannage

L'utilisation du même modèle sur toutes les plates-formes améliore la visibilité et les capacités de dépannage avec des alertes proactives et des rapports avancés via l'intégration à Workspace ONE Intelligence.

Expérience transparente dans plusieurs environnements

La proposition d'expériences communes aux administrateurs et aux utilisateurs finaux dans l'ensemble des environnements simplifie l'administration et augmente la productivité des utilisateurs finaux.

Automatisation avancée

La plate-forme basée sur l'API prend en charge l'automatisation avancée et l'intégration à des applications et à des services tiers pour les processus de jour 1 et de jour 2.

Évolutivité sans précédent

Un dispositif Horizon Edge avec une architecture légère de type thin-edge et une architecture cloud native augmente l'évolutivité sur l'ensemble des plates-formes.

Pour explorer la documentation de la famille Horizon 8 de solutions associées, reportez-vous à la section Documentation d'Horizon, d'Horizon 8, d'Horizon Cloud Service et des instances d'Horizon Client.

Lisez les sections suivantes :

- Caractéristiques d'architecture du Plan de contrôle Horizon - Déploiements de Microsoft Azure en mode natif

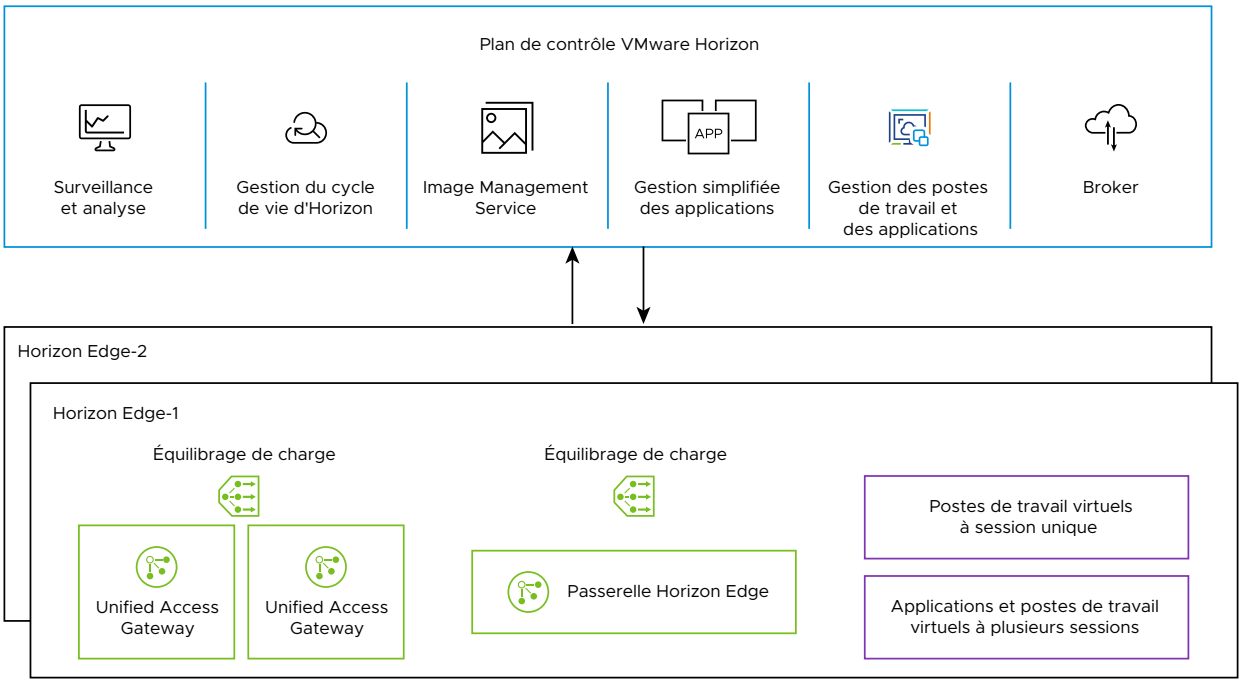
Caractéristiques d'architecture du Plan de contrôle Horizon - Déploiements de Microsoft Azure en mode natif

Plusieurs caractéristiques d'architecture définissent le fonctionnement du service Horizon Cloud Service - next-gen et également comment ce service s'améliore par rapport à celui de l'instance d'Horizon Cloud Service - first-gen précédente.

Cette section couvre les caractéristiques spécifiques d'Horizon Cloud Service - next-gen, actuellement disponibles pour Microsoft Azure en mode natif. Elle ne traite pas du cas d'utilisation des espaces Horizon 8 qui se connectent au Plan de contrôle Horizon et consomment des services SaaS supplémentaires.

Cette architecture fournit des déploiements basés sur le cloud faciles à configurer, à utiliser et à gérer.

Le diagramme suivant illustre la relation entre le Plan de contrôle Horizon et un dispositif Horizon Edge initial déployé dans le cloud Microsoft Azure (`Horizon Edge-1`). Dans cet exemple, lors de l'utilisation de l'assistant de déploiement, l'administrateur a choisi d'utiliser deux instances de la passerelle Passerelle Horizon Edge.



Les éléments d'infrastructure de base suivants fournissent les services suivants :

- Plan de contrôle Horizon.
- Instance de Passerelle Horizon Edge. Pour le cloud Microsoft Azure en tant que fournisseur, le système de déploiement déploie un équilibrage de charge Microsoft Azure avec cette instance.
- Instances d'Unified Access Gateway et équilibrage de charge pour ces instances.

Pour plus d'informations sur l'architecture, reportez-vous à la section Architecture d'Horizon Cloud Service next-gen.

Différences par rapport à la première génération

Des améliorations et des comportements significatifs différencient Horizon Cloud Service - next-gen de ses instances d'Horizon Cloud Service - first-gen précédentes. L'un des principaux avantages d'Horizon Cloud Service - next-gen est que de nombreux composants d'infrastructure qui étaient précédemment déployés dans l'environnement de votre organisation résident désormais en tant que services dans Plan de contrôle Horizon.

Si vous avez effectué une migration d'Horizon Cloud Service - first-gen vers Horizon Cloud Service - next-gen, les différences d'expérience utilisateur sont présentées dans la section Migration en libre-service des déploiements d'Horizon Cloud on Microsoft Azure de première génération vers Horizon Cloud Service - next-gen. Pour connaître les ajouts actuels à Horizon Cloud Service - next-gen, reportez-vous à la section *Nouveautés* des Notes de mise à jour d'Horizon Cloud Service - next-gen.

Démarrage avec les déploiements du plan de contrôle Horizon, de Microsoft Azure et d'Horizon 8

2

L'intégration au service constitue la première étape de l'utilisation d'Horizon Cloud Service - next-gen ou du plan de contrôle Horizon.

Lorsque vous commencez le processus d'intégration, reportez-vous à la configuration système requise et aux conditions préalables d'abonnement suivantes.

1 Examinez la liste de vérification qui correspond à votre environnement et remplissez les conditions requises.

   - Liste de vérification des conditions requises pour le déploiement d'un dispositif Microsoft Azure Edge
   - Liste de vérification des conditions requises pour le déploiement d'un dispositif Horizon 8 Edge

2 Effectuez les étapes de préparation de l'environnement qui correspondent à votre type de déploiement.

   - Déploiements de Microsoft Azure Edge
   - Déploiements des dispositifs Horizon 8 Edge

3 Démarrez les étapes de déploiement et d'intégration décrites dans Chapitre 4 Intégration pour les administrateurs Horizon Cloud Service - next-gen.

Lisez les sections suivantes :

- Liste de vérification des conditions requises pour le déploiement d'un dispositif Horizon 8 Edge
- Liste de vérification des conditions requises pour le déploiement d'un dispositif Microsoft Azure Edge

Liste de vérification des conditions requises pour le déploiement d'un dispositif Horizon 8 Edge

Effectuez les tâches suivantes pour préparer les composants Horizon 8 à l'intégration au Plan de contrôle Horizon. Assurez-vous que les conditions requises sont remplies conformément aux sections suivantes afin de réussir l'intégration.

Public concerné par cette liste de vérification

Certaines des conditions requises répertoriées dans les sections suivantes sont nécessaires à l'intégration réussie des composants Horizon afin d'utiliser une licence d'abonnement avec un déploiement d'Horizon Edge. Certaines conditions sont nécessaires à l'exécution des tâches clés après cette intégration initiale pour permettre l'utilisation des services Plan de contrôle Horizon avec les composants d'Horizon.

Conditions requises pour Passerelle Horizon Edge et Horizon Connection Server

☐	Pour l'interopérabilité entre Passerelle Horizon Edge et Horizon, Horizon Connection Server doit être 7.13.2 ou version ultérieure. Ensuite, pour utiliser les derniers services et les dernières fonctionnalités du cloud avec le dispositif Horizon Edge connecté au cloud, Horizon Connection Server doit exécuter la version actuelle des services Horizon Edge.
☐	Pour les nouveaux déploiements, il est fortement recommandé d'utiliser la version la plus récente d'Passerelle Horizon Edge. La procédure de déploiement du dispositif Passerelle Horizon Edge utilise les éléments suivants : ■ IP statique ■ Enregistrements de recherche DNS directe et inversée
☐	Conditions requises en matière de ressources pour le dispositif virtuel Passerelle Horizon Edge. Les conditions requises en matière de ressources dépendent de l'architecture d'Horizon Edge déployée. Les listes ci-dessous indiquent les versions actuellement prises en charge pour les nouveaux déploiements pour chaque conception. **Version 2.2.0** 8 vCPU, mémoire de 16 Go (RAM), banque de données de 40 Go.

Conditions requises de DNS, ports et protocoles

☐	Des ports et des protocoles spécifiques sont requis pour l'intégration d'un espace Horizon à Horizon Cloud et pour les opérations en cours de l'espace avec l'instance d'Passerelle Horizon Edge couplée avec cet espace, et la passerelle Passerelle Horizon Edge avec le Plan de contrôle Horizon. Reportez-vous à la section Rendre les URL de destination appropriées accessibles pour déployer une passerelle Passerelle Horizon Edge dans un environnement Horizon 8.

Attribution de licence pour les systèmes d'exploitation Microsoft Windows

Horizon Cloud n'attribue aucune licence de système d'exploitation invité requise pour utiliser les systèmes d'exploitation Microsoft Windows que vous utilisez dans le cadre de l'utilisation des workflows Horizon Cloud. En tant que client, il vous incombe de disposer de licences Microsoft valides et éligibles qui vous autorisent à créer et à utiliser des VM de poste de travail Windows et des VM RDSH que vous choisissez d'utiliser dans votre environnement de locataire Horizon Cloud. Vous êtes également autorisé à effectuer des workflows sur ces VM. L'attribution de licence requise dépend de votre utilisation prévue.

☐	Attribution de licence pour un ou plusieurs des types suivants : Microsoft Windows 7, Microsoft Windows 10
☐	Attribution de licence pour un ou plusieurs des types suivants : Microsoft Windows Server 2012 R2, Microsoft Server 2016, Microsoft Server 2019
☐	Serveurs de licences RDS Microsoft Windows : pour la haute disponibilité, des serveurs de licence redondants sont recommandés.
☐	Licences d'accès client pour appareil et/ou utilisateur RDS Microsoft.

Configuration requise des ports et des protocoles pour le déploiement d'Horizon 8 Edge

Cette page est une référence pour tous les ports et protocoles possibles utilisés pour la communication d'un dispositif Horizon Edge standard avec Horizon Connection Server. Utilisez ce tableau pour vous assurer que votre configuration réseau et vos pare-feu autoriseront le trafic de communication requis pour un déploiement réussi et des opérations quotidiennes.

Les ports et protocoles spécifiques requis pour votre déploiement particulier dépendront en partie des fonctionnalités que vous choisissez d'utiliser pour vos déploiements d'Horizon Edge. Si vous ne prévoyez pas d'utiliser Splunk Enterprise pour la surveillance, vous pouvez ignorer les ports associés à Splunk Enterprise.

Important Outre les ports et protocoles décrits ici, les conditions requises du DNS pour le déploiement d'un dispositif Horizon Edge et ses opérations quotidiennes sont spécifiques. Pour plus d'informations, reportez-vous à la section Rendre les URL de destination appropriées accessibles pour déployer une passerelle Passerelle Horizon Edge dans un environnement Horizon 8.

Ports et protocoles requis par Horizon Edge

Lorsque vous activez Surveillance de l'infrastructure Horizon, Horizon Edge est déployé et configuré dans l'abonnement associé. Le tableau suivant répertorie les ports et les protocoles nécessaires lors du processus d'activation qui déploie le dispositif et configure les VM du gestionnaire afin que le dispositif puisse collecter les données de surveillance qu'il vise à collecter à partir de ces composants. Ce tableau répertorie également les ports et les protocoles qui sont nécessaires en période de stabilité pendant les opérations de collecte des données que le dispositif vise à collecter.

Tableau 2-1.

Source	Cible	Ports	Protocoles	Objectif
Horizon Edge	Horizon Connection Server	443	HTTPS	Configuration de la licence
Horizon Edge	Splunk Enterprise	8000 et 8088	HTTP HTTPS	Surveillance de la collecte de données
Horizon Edge	Serveur DNS	53 et 853	TCP UDP	Services DNS

Tableau 2-1. (suite)

Source	Cible	Ports	Protocoles	Objectif
Horizon Edge	*.blob.core.windows.net	443	TCP	Utilisé pour l'accès par programme au stockage Blob Azure et pour charger les journaux Horizon Edge le cas échéant. Utilisé pour le téléchargement des images du Docker afin de créer les modules Horizon Edge requis qui sont utiles pour la surveillance, SSO, les mises à jour d'UAG, etc.
Horizon Edge	horizonedgeprod.azurecr.io	443	TCP	Utilisé pour l'authentification lors du téléchargement des images du Docker afin de créer les modules Horizon Edge requis, qui sont utiles pour la surveillance, SSO, les mises à jour d'UAG, etc.
Horizon Edge	*.azure-devices.net	443	TCP	Dispositif utilisé pour communiquer avec le plan de contrôle du cloud, télécharger les configurations du module du dispositif et mettre à jour l'état d'exécution du module du dispositif. Les points de terminaison concrets actuels sont les suivants : Amérique du Nord : ■ edgehubprodna.azure-devices.net Europe : ■ edgehubprodeu.azure-devices.net Japon : ■ edgehubprodjp.azure-devices.net

Tableau 2-1. (suite)

Source	Cible	Ports	Protocoles	Objectif
Horizon Edge	vmwareprod.wavefront.com	443	TCP	Utilisé pour l'envoi de mesures d'opération à VMware Tanzu® Observability™ by Wavefront. Les opérateurs VMware reçoivent les données avec lesquelles prendre en charge les clients. Tanzu Observability est une plate-forme d'analyse en continu. Vous pouvez envoyer vos données à Tanzu Observability, et afficher les données et interagir avec celles-ci dans des tableaux de bord personnalisés. Reportez-vous à la documentation de VMware Tanzu Observability by Wavefront.

Tableau 2-1. (suite)

Source	Cible	Ports	Protocoles	Objectif
Horizon Edge	*.data.vmwservices.com	443	TCP	Pour envoyer des événements ou des mesures à Workspace ONE Intelligence pour la surveillance des données. Reportez-vous à Workspace ONE Intelligence. Les points de terminaison concrets actuels sont les suivants : ■ eventproxy.na1.data.vmwservices.com ■ eventproxy.eu1.data.vmwservices.com ■ eventproxy.eu2.data.vmwservices.com ■ eventproxy.uk1.data.vmwservices.com ■ eventproxy.ca1.data.vmwservices.com ■ eventproxy.ap1.data.vmwservices.com ■ eventproxy.au1.data.vmwservices.com ■ eventproxy.in1.data.vmwservices.com
Horizon Edge	login.microsoftonline.com	443	TCP	Généralement utilisé par les applications pour s'authentifier auprès du service Microsoft Azure.

Tableau 2-1. (suite)

Source	Cible	Ports	Protocoles	Objectif
Horizon Edge	management.azure.com	443	TCP	Utilisé pour les demandes d'API du dispositif Edge aux points de terminaison de Microsoft Azure Resource Manager pour utiliser les services de Microsoft Azure Resource Manager. Microsoft Azure Resource Manager fournit une couche de gestion cohérente pour effectuer des tâches via Azure PowerShell, Azure CLI, le portail Azure, REST API et les SDK client.
Horizon Edge	Serveur NTP	123	UDP	Services NTP
Horizon Agent	Horizon Edge	31883	TCP MQTT UDP	Horizon Agent s'exécutant sur la VM vers le protocole MQTT s'exécutant sur Edge.
Horizon Edge	Horizon Connection Server	4002	TCP	Horizon Edge vers Horizon Connection Server sur Java Messaging Service (JMS).

Rendre les URL de destination appropriées accessibles pour déployer une passerelle Passerelle Horizon Edge dans un environnement Horizon 8

Pour créer un déploiement d'Horizon Edge et installer ou mettre à jour des modules de dispositif, vous devez autoriser les URL appropriées sur les ports correspondants.

Pour le tableau suivant, les fins répertoriées sont utilisées dans le cadre d'une passerelle Passerelle Horizon Edge avec Horizon Connection Server.

Autoriser les URL pour le sous-réseau de gestion

Autorisez les URL appropriées et les sous-domaines génériques en fonction de l'emplacement et des besoins de votre site. Plus particulièrement, effectuez les tâches suivantes.

- Autorisez les URL et les sous-domaines génériques dans le tableau suivant. Par exemple, en ajoutant les URL et le sous-domaine générique à une liste autorisée pour le pare-feu.
- Contournez l'inspection approfondie des paquets SSL comme suit.
  - Dans le pare-feu pour les URL et les sous-domaines génériques dans le tableau suivant.
  - Dans le serveur proxy, le cas échéant.

    Par conséquent, si le système Passerelle Horizon Edge est connecté au plan de contrôle Horizon Cloud via un serveur proxy, contournez l'inspection approfondie des paquets SSL dans le serveur proxy pour les URL et les sous-domaines génériques dans le tableau suivant.

Destination (nom de DNS)	Port	Protocole	Objectif
*.blob.core.windows.net	443	TCP	Utilisé pour l'accès par programme au stockage Blob Azure et pour charger les journaux Horizon Edge le cas échéant. Utilisé pour le téléchargement des images du Docker afin de créer les modules Horizon Edge requis qui sont utiles pour la surveillance, SSO, les mises à jour d'UAG, etc.
horizonedgeprod.azurecr.io	443	TCP	Utilisé pour l'authentification lors du téléchargement des images du Docker afin de créer les modules Horizon Edge requis, qui sont utiles pour la surveillance, SSO, les mises à jour d'UAG, etc.

Destination (nom de DNS)	Port	Protocole	Objectif
*.azure-devices.net ou l'un des noms spécifiques à la région ci-dessous, selon le plan de contrôle régional qui s'applique à votre compte de locataire : Amérique du Nord : ■ edgehubprodna.azure-devices.net Europe : ■ edgehubprodeu.azure-devices.net Japon : ■ edgehubprodjp.azure-devices.net	443	TCP (condition requise : HTTP, HTTPS et WSS)	Utilisé pour connecter le dispositif au plan de contrôle Horizon Cloud, pour télécharger les configurations du module du dispositif et pour mettre à jour l'état d'exécution du module du dispositif.
*.data.vmwservices.com ou l'un des noms spécifiques à la région ci-dessous, selon la cible Workspace ONE Intelligence régionale qui s'applique à votre compte de locataire : ■ eventproxy.na1.data.vmwservices.com ■ eventproxy.eu1.data.vmwservices.com ■ eventproxy.eu2.data.vmwservices.com ■ eventproxy.uk1.data.vmwservices.com ■ eventproxy.ca1.data.vmwservices.com ■ eventproxy.ap1.data.vmwservices.com ■ eventproxy.au1.data.vmwservices.com ■ eventproxy.in1.data.vmwservices.com	443	TCP	Utilisé pour l'envoi d'événements ou de mesures à Workspace ONE Intelligence. Reportez-vous à Workspace ONE Intelligence.

Liste de vérification des conditions requises pour le déploiement d'un dispositif Microsoft Azure Edge

L'objectif de cette liste de vérification est de vous informer des éléments requis pour effectuer un déploiement de Microsoft Azure en mode natif à l'aide du Plan de contrôle Horizon.

Important Un déploiement d'Horizon Cloud on Microsoft Azure fait référence à une infrastructure Microsoft Azure en mode natif.

Public concerné par cette liste de vérification

Cette liste de vérification s'applique aux comptes clients Horizon Cloud qui n'ont jamais présenté de déploiement d'Horizon Cloud on Microsoft Azure dans leur environnement de locataire. Ces locataires peuvent être appelés environnements entièrement nouveaux ou vierges.

Vous devez effectuer certains éléments qui suivent avant de déployer Horizon Cloud. Vous pouvez différer certains éléments jusqu'à ce que le déploiement soit terminé et en cours d'exécution.

Conditions requises pour les abonnements Microsoft Azure

Pour connaître les limites de configuration, reportez-vous au Dimensionnement de votre déploiement d'Horizon Cloud Service - next-gen, qui inclut des informations sur l'utilisation de l'outil Valeurs maximales de configuration VMware. À partir de la page Valeurs maximales de configuration, sélectionnez **Afficher les limites**, **VMware Horizon Cloud Service - next-gen**, la version la plus récente et les catégories à afficher.

☐	Abonnements Microsoft Azure valides dans un environnement Microsoft Azure pris en charge (Azure Commercial). Si vous souhaitez déployer des dispositifs Horizon Edge, ce qui inclut des instances de la passerelle Passerelle Horizon Edge et d'Unified Access Gateway, dans leur propre fournisseur dédié (abonnement Microsoft Azure), procurez-vous un autre abonnement Microsoft Azure valide pour déployer des pools. **Note** Horizon Cloud prend en charge la plupart des régions Microsoft Azure.
☐	Privilèges d'administration Microsoft Azure valides dans chaque abonnement Microsoft Azure, pour que vous utilisiez le portail Microsoft Azure et effectuiez les Déploiements de Microsoft Azure Edge.
☐	Créez un ou plusieurs principaux de service dans chaque abonnement Microsoft Azure, en notant l'ID d'abonnement, l'ID d'annuaire et l'ID d'application, et attribuez le rôle approprié à chaque principal de service dans vos abonnements. ■ Reportez-vous à la section Créer un principal de service pour l'abonnement Microsoft Azure. ■ Pour utiliser un rôle personnalisé pour votre principal de service, reportez-vous à la section Pour utiliser un rôle personnalisé pour l'enregistrement d'applications Horizon Cloud. **Note** Lorsque vous créez plusieurs principaux de service, ils partagent l'ID d'abonnement et l'ID d'annuaire, mais chaque principal de service dispose de son propre ID d'application.
☐	Déterminez le type de format Microsoft Azure Edge que vous souhaitez déployer. Les options suivantes sont disponibles. ■ Passerelle Edge (VM) = Machine virtuelle de la passerelle Edge La passerelle Edge (VM) est destinée aux déploiements plus petits sans haute disponibilité. ■ Passerelle Edge (AKS) = Azure Kubernetes Service de la passerelle Edge La passerelle Edge (AKS) fournit une haute disponibilité.
☐	Pour déployer une passerelle Edge (AKS), créez une identité gérée par l'utilisateur Microsoft Azure. Horizon Edge utilisant un cluster AKS nécessite une identité gérée par l'utilisateur avec le rôle Contributeur de réseaux dans la portée du groupe de ressources du réseau virtuel de gestion et le rôle Opérateur d'identité gérée dans la portée de l'abonnement Microsoft Azure. Reportez-vous à la documentation de Microsoft sur la gestion des identités attribuées par l'utilisateur. Si votre sous-réseau de gestion dispose d'une table de routage et que le groupe de ressources de celle-ci est différent de celui du réseau virtuel, le rôle Contributeur de réseaux doit également être attribué au groupe de ressources de la table de routage.
☐	Enregistrez les fournisseurs de ressources requis pour votre abonnement Microsoft Azure. Reportez-vous à la section Confirmer que les fournisseurs de ressources requis sont enregistrés dans votre abonnement Microsoft Azure.

☐	Créez un rôle personnalisé qui fournit des autorisations READ aux galeries de calcul Azure dans vos abonnements et attribuez ce rôle personnalisé à tous les principaux de service configurés pour un dispositif Horizon Edge donné.
☐	L'abonnement doit autoriser la création de groupes de ressources qui ne contiennent pas de balises.

Configurations requises pour la capacité Microsoft Azure

Lorsque le tableau suivant fait référence à la capacité Microsoft Azure, aucune installation manuelle n'est nécessaire. Tant que les capacités indiquées sont disponibles dans l'abonnement, le système de déploiement instancie automatiquement les VM décrites.

☐	Capacité Microsoft Azure pour les ressources Horizon Edge principales à déployer dans cet abonnement. Notez que les capacités requises varient selon le format Microsoft Azure Edge que vous déployez, la passerelle Edge (AKS) ou la passerelle Edge (VM). ■ **Passerelle Edge (AKS)** : quota suffisant pour un cluster AKS à 4 nœuds et un nœud supplémentaire pendant les mises à niveau. ■ Un déploiement de passerelle Edge (AKS) utilise un cluster Azure Kubernetes Service (AKS), qui nécessite quatre nœuds de l'une des tailles de VM prises en charge pour la capacité. Vous trouverez ci-dessous la liste des tailles de SKU de VM prises en charge pour un déploiement de passerelle Edge (AKS) dans l'ordre de priorité décroissant. Si votre abonnement Microsoft Azure dispose d'une capacité pour au moins l'une des tailles de SKU de VM suivantes, le déploiement de dispositifs Edge est accepté. Sinon, le déploiement de dispositifs Edge est refusé. ■ Standard_D2s_v3 - 2 vCPU, 8 Go de mémoire ■ Standard_D2ds_v5 - 2 vCPU, 8 Go de mémoire ■ Standard_D2a_v4 - 2 vCPU, 8 Go de mémoire Lorsque le cluster AKS fonctionne normalement, quatre nœuds de VM sont requis. Un nœud supplémentaire est requis et utilisé pendant le processus de mise à niveau. ■ **Passerelle Edge (VM)** : quota suffisant pour une machine virtuelle unique. Vous trouverez ci-dessous la liste des tailles de SKU de VM prises en charge pour un déploiement de passerelle Edge (VM) dans l'ordre de priorité décroissant. Si votre abonnement Microsoft Azure dispose d'une capacité pour au moins l'une des tailles de SKU de VM suivantes, le déploiement de dispositifs Edge est accepté. Sinon, le déploiement de dispositifs Edge est refusé. ■ Standard_D4s_v3 - 4 vCPU, mémoire de 16 Go ■ Standard_D4s_v4 - 4 vCPU, mémoire de 16 Go ■ Standard_D4s_v5 - 4 vCPU, mémoire de 16 Go ■ Exécutez des commandes pour vérifier la disponibilité du modèle de VM Microsoft Azure et pour vérifier la sortie de CPU régionale. Reportez-vous à la section Vérifier la disponibilité du modèle de VM Microsoft Azure. ■ Instances d'Unified Access Gateway : au moins 2 des tailles prises en charge qui suivent. La taille par défaut et recommandée est Standard_F8s_v2. ■ Standard_A4_v2 ■ Standard_D8s_v4 ■ Standard_D16s_v4 ■ Standard_D8s_v5 ■ Standard_D16s_v5 ■ Standard_F8s_v2 ■ Standard_F16s_v2 **Note** Le modèle de VM `A4_v2` suffit uniquement pour les validations de concept (PoC), les pilotes ou les environnements plus petits dans lesquels vous savez que vous ne dépasserez pas 1 000 sessions actives sur Horizon Edge. Lorsque votre instance d'Horizon Edge est prête à l'emploi, votre capacité dans le cloud Microsoft Azure doit également intégrer les VM importées, les images, les VM de pool et les VM de capture d'application App Volumes que vous créez dans cette instance d'Horizon Edge. Reportez-vous à la section Image Management System Requirements.

Conditions requises pour le réseau

La configuration réseau requise suivante inclut les détails nécessaires au déploiement et à l'utilisation d'un dispositif Horizon Edge. Les deux tableaux suivants sont semblables, mais différents. Utilisez le tableau qui s'applique au type de format Microsoft Azure Edge que vous prévoyez de déployer, Passerelle Edge (VM) ou Passerelle Edge (AKS).

Passerelle Edge (VM)

Utilisez le tableau suivant pour un déploiement de passerelle Edge (VM).

Tableau 2-2. Configuration réseau requise pour une passerelle Edge (VM)

☐	Réseau virtuel Microsoft Azure créé dans la région Microsoft Azure cible avec l'espace d'adresses applicable pour couvrir les sous-réseaux requis. Reportez-vous à la section Configurer les paramètres réseau pour les régions Microsoft Azure.
☐	Les conditions requises suivantes pour le sous-réseau sont minimales. Pour des environnements plus grands, des sous-réseaux de taille plus grande peuvent être requis. ■ Sous-réseau de gestion : /26 minimum ■ Sous-réseau de poste de travail (locataire) - principal : /27 minimum, mais d'une taille appropriée en fonction du nombre de postes de travail et de serveurs RDS. Vous pouvez ajouter d'autres sous-réseaux si nécessaire. ■ Sous-réseau de zone DMZ : /27 minimum pour le cluster d'instances d'Unified Access Gateway (non requis pour le type d'accès à l'instance interne d'Unified Access Gateway). Vous devez créer manuellement des sous-réseaux sur le réseau virtuel comme condition préalable. Reportez-vous à la section Configurer les paramètres réseau pour les régions Microsoft Azure. Il est recommandé de ne pas attacher d'autres ressources aux sous-réseaux. Si vous choisissez d'utiliser un fournisseur dédié pour déployer des dispositifs de passerelle Horizon (Passerelle Horizon Edge et Unified Access Gateway), vous devez créer des sous-réseaux principaux dans le fournisseur à partir duquel les postes de travail seront déployés.
☐	Configurez le serveur DNS du réseau virtuel, pointant vers un serveur DNS valide qui peut résoudre les noms de machines internes et externes. Reportez-vous à la section Configurer les enregistrements DNS requis après le déploiement de la passerelle Passerelle Horizon Edge et d'Unified Access Gateway. Pour les points de terminaison internes, le serveur AD en est un exemple. Pour les points de terminaison externes, l'accès Internet sortant sur les réseaux virtuels que vous utilisez pour le déploiement de la passerelle doit résoudre et atteindre des noms DNS spécifiques à l'aide de ports et de protocoles spécifiques. Cette condition est requise pour le déploiement et les opérations en cours.
☐	L'accès Internet sortant sur les réseaux virtuels que vous utilisez pour le déploiement d'Horizon Edge doit résoudre et atteindre des noms DNS spécifiques à l'aide de ports et de protocoles spécifiques. Cette condition est requise pour le déploiement et les opérations en cours. Pour obtenir la liste des noms et des ports DNS, reportez-vous à la section Rendre les URL de destination appropriées accessibles pour déployer une passerelle Passerelle Horizon Edge dans un environnement Microsoft Azure.
☐	Facultatif. Informations sur le serveur proxy, si cela s'avère nécessaire pour l'accès Internet sortant sur le réseau virtuel qui est utilisé pendant le déploiement et les opérations en cours de l'environnement Horizon Cloud.
☐	Facultatif. Microsoft Azure VPN/Express Route configurés, lorsque vous souhaitez établir une mise en réseau entre le réseau virtuel et votre réseau d'entreprise sur site.

Passerelle Edge (AKS)

Utilisez le tableau suivant pour un déploiement de passerelle Edge (AKS). Ces conditions requises incluent la prise en charge de la configuration de la passerelle Passerelle Horizon Edge à l'aide d'un cluster AKS. La configuration de la passerelle Passerelle Horizon Edge à l'aide d'un cluster AKS fournit une solution plus facilement évolutive.

Tableau 2-3. Configuration réseau requise pour une passerelle Edge (AKS)

☐	Réseau virtuel Microsoft Azure créé dans la région Microsoft Azure cible avec l'espace d'adresses applicable pour couvrir les sous-réseaux requis. Reportez-vous à la section Configurer les paramètres réseau pour les régions Microsoft Azure.
☐	Les conditions requises suivantes pour le sous-réseau sont minimales. Pour des environnements plus grands, des sous-réseaux de taille plus grande peuvent être requis. ■ Sous-réseau de gestion : /26 minimum En cas de déploiement d'une passerelle Edge (AKS), configurez une passerelle NAT pour le sous-réseau de gestion, car un dispositif Horizon Edge utilisant un cluster AKS a besoin d'une passerelle NAT pour la connectivité sortante. ■ Sous-réseau de poste de travail (locataire) - principal : /27 minimum, mais d'une taille appropriée en fonction du nombre de postes de travail et de serveurs RDS. Vous pouvez ajouter d'autres sous-réseaux si nécessaire. ■ Sous-réseau de zone DMZ : /27 minimum pour le cluster d'instances d'Unified Access Gateway (non requis pour le type d'accès à l'instance interne d'Unified Access Gateway). Vous devez créer manuellement des sous-réseaux sur le réseau virtuel comme condition préalable. Reportez-vous à la section Configurer les paramètres réseau pour les régions Microsoft Azure. Il est recommandé de ne pas attacher d'autres ressources aux sous-réseaux. Si vous choisissez d'utiliser un fournisseur dédié pour déployer des dispositifs de passerelle Horizon (Passerelle Horizon Edge et Unified Access Gateway), vous devez créer des sous-réseaux principaux dans le fournisseur à partir duquel les postes de travail seront déployés.
☐	Si vous déployez une passerelle Edge (AKS) et que vous sélectionnez la valeur de type de cluster sortant comme passerelle NAT au moment de la création du dispositif Edge, configurez une passerelle NAT sur le sous-réseau de gestion pour activer la connectivité sortante du dispositif Passerelle Horizon Edge. Si vous sélectionnez la valeur de type de cluster sortant comme routes définies par l'utilisateur lors de la création du dispositif Edge, configurez une table de routage sur le sous-réseau de gestion avec la route par défaut 0.0.0.0/0 pointant vers un tronçon suivant de type **VirtualAppliance** ou **VirtualNetworkGateway**.
☐	Collectez les plages d'adresses IP CIDR suivantes pour lesquelles vous devez configurer Passerelle Horizon Edge pendant le déploiement. **Note** Assurez-vous que ces plages ne sont pas en conflit avec les autres plages utilisées dans votre environnement. ■ CIDR de service : /27 minimum ■ CIDR d'espace : /21 minimum Si vous déployez une passerelle Edge (AKS), vous devez vous conformer à la condition requise suivante de Microsoft Azure pour déployer le cluster AKS. Lorsque vous déployez Horizon Edge à l'aide d'Horizon Universal Console, assurez-vous que le CIDR de service, le CIDR d'espace et l'espace d'adresses du réseau virtuel du sous-réseau de gestion ne sont pas en conflit avec les plages d'adresses IP suivantes : ■ 169.254.0.0/16 ■ 172.30.0.0/16 ■ 172.31.0.0/16 ■ 192.0.2.0/24

Tableau 2-3. Configuration réseau requise pour une passerelle Edge (AKS) (suite)

☐	Configurez le serveur DNS du réseau virtuel, pointant vers un serveur DNS valide qui peut résoudre les noms de machines internes et externes. Reportez-vous à la section Configurer les enregistrements DNS requis après le déploiement de la passerelle Passerelle Horizon Edge et d'Unified Access Gateway. Pour les points de terminaison internes, le serveur AD en est un exemple. Pour les points de terminaison externes, l'accès Internet sortant sur les réseaux virtuels que vous utilisez pour le déploiement de la passerelle doit résoudre et atteindre des noms DNS spécifiques à l'aide de ports et de protocoles spécifiques. Cette condition est requise pour le déploiement et les opérations en cours.
☐	L'accès Internet sortant sur les réseaux virtuels que vous utilisez pour le déploiement d'Horizon Edge doit résoudre et atteindre des noms DNS spécifiques à l'aide de ports et de protocoles spécifiques. Cette condition est requise pour le déploiement et les opérations en cours. Pour obtenir la liste des noms et des ports DNS, reportez-vous à la section Rendre les URL de destination appropriées accessibles pour déployer une passerelle Passerelle Horizon Edge dans un environnement Microsoft Azure.
☐	Facultatif. Informations sur le serveur proxy, si cela s'avère nécessaire pour l'accès Internet sortant sur le réseau virtuel qui est utilisé pendant le déploiement et les opérations en cours de l'environnement Horizon Cloud.
☐	Facultatif. Microsoft Azure VPN/Express Route configurés, lorsque vous souhaitez établir une mise en réseau entre le réseau virtuel et votre réseau d'entreprise sur site.
☐	Si vous déployez une passerelle Edge (AKS), concernant l'utilisation d'un cluster AKS par le dispositif Horizon Edge, si le réseau virtuel que vous utilisez pour le déploiement d'Horizon Edge dispose d'un serveur DNS personnalisé, vous pouvez ajouter l'adresse IP 168.63.129.16 de DNS Microsoft Azure comme redirecteur DNS pour la résolution des noms externes.

Conditions requises pour les ports et les protocoles

☐	Des ports et protocoles spécifiques sont requis pour le déploiement et les opérations en cours de votre environnement Horizon Cloud. Reportez-vous à la section Conditions requises pour les ports et les protocoles pour votre déploiement d'Horizon Cloud dans Microsoft Azure.

Conditions requises pour Unified Access Gateway

Un cluster de VM Unified Access Gateway est associé à un pool qui permet aux clients de disposer de connexions HTML Access approuvées aux VM de ce pool.

Utilisez Horizon Universal Console pour configurer Horizon Cloud avec Unified Access Gateway. Les éléments ci-dessous sont requis pour ce type de configuration.

☐	L'accès Internet sortant à *.horizon.vmware.com est requis dans tous les types de configuration. Lorsque l'option **Autoriser l'accès interne sur un réseau d'entreprise** est le **Type d'accès à Unified Access Gateway**, vous pouvez appliquer le routage défini par l'utilisateur ou la passerelle NAT au sous-réseau de gestion pour autoriser le trafic sortant. Lorsque le **Type d'accès à Unified Access Gateway** est configuré en externe avec un réseau DMZ, vous devez configurer l'accès externe à *.horizon.vmware.com sur le réseau DMZ.
☐	Le nom de domaine complet est requis pour la configuration d'Unified Access Gateway.
☐	Un ou plusieurs certificats pour Unified Access Gateway au format PEM correspondant au nom de domaine complet. **Note** Si le ou les certificats que vous fournissez à cet effet utilisent des paramètres CRL (listes de révocation des certificats) ou OCSP (Online Certificate Status Protocol) qui font référence à des noms DNS spécifiques, vous devez vous assurer que l'accès Internet sortant sur le réseau virtuel peut être résolu et accessible. Lors de la configuration de votre certificat fourni dans la configuration d'Unified Access Gateway, le logiciel Unified Access Gateway accède à ces noms DNS pour vérifier l'état de révocation du certificat. Si ces noms DNS ne sont pas accessibles, le déploiement échoue. Ces noms dépendent beaucoup de l'autorité de certification que vous avez utilisée pour obtenir les certificats, ce qui est en dehors du contrôle de VMware.

Présentation de l'identité d'utilisateur et de l'identité de machine

Horizon Cloud Service - next-gen diffère des autres environnements dans la manière dont il gère l'identité. Dans Horizon Cloud Service - next-gen, le service fait la distinction entre l'identité d'utilisateur et l'identité de machine, et il s'appuie sur les deux types d'identité lors de l'établissement d'une connexion sécurisée entre un client et une application ou un poste de travail distant.

Note Cette distinction entre identité d'utilisateur et identité de machine peut vous sembler nouvelle si vous connaissez mieux les environnements qui utilisent un fournisseur d'identité unique pour authentifier à la fois l'identité d'utilisateur et de machine, comme l'environnement Horizon Cloud de première génération ou un environnement Horizon 8 sur site.

Dans Horizon Cloud Service - next-gen, vous devez configurer une configuration d'identité composée d'un fournisseur d'identité pour authentifier l'identité d'utilisateur et d'un fournisseur d'identité pour authentifier l'identité de machine.

Identité d'utilisateur

Horizon Cloud Service - next-gen nécessite l'enregistrement d'un fournisseur d'identité utilisateur. Le service utilise ce fournisseur d'identité pour authentifier les utilisateurs clients qui tentent d'accéder à des applications et des postes de travail distants.

Identité de machine

Horizon Cloud Service - next-gen nécessite également l'enregistrement d'un fournisseur d'identité de machine. Le service utilise ce fournisseur d'identité pour établir l'identité de machine des machines virtuelles qui fournissent des applications et des postes de travail distants.

Par le biais du fournisseur d'identité de machine, le service joint les postes de travail distants et les sources de machines virtuelles pour les applications distantes au domaine de réseau approuvé auquel les utilisateurs clients sont autorisés à accéder.

Configurations d'identité prises en charge

Horizon Cloud Service - next-gen nécessite l'enregistrement d'une configuration d'identité qui se compose d'un fournisseur d'identité d'utilisateur et d'un fournisseur d'identité de machine. Les capacités de la fonctionnalité peuvent varier en fonction des fournisseurs d'identité particuliers inclus dans la configuration.

Horizon Cloud Service - next-gen prend en charge les configurations d'identité suivantes.

Tableau 2-4. Configurations d'identité prises en charge pour Horizon Cloud Service - next-gen

Configuration de l'identité	Fournisseur d'identité d'utilisateur	Fournisseur d'identité de machine	Considérations relatives aux fonctionnalités
A	Microsoft Entra ID	Active Directory	■ Prend en charge SSO pour des applications et des postes de travail distants
B	Microsoft Entra ID	Microsoft Entra ID	■ Ne prend pas en charge Single Sign-On (SSO) pour des applications et des postes de travail distants
C	Workspace ONE Access	Active Directory	■ Prend en charge SSO pour des applications et des postes de travail distants ■ Prend en charge l'intégration à Workspace ONE

Les sections suivantes de cette page décrivent les conditions requises détaillées pour chaque fournisseur d'identité d'utilisateur et fournisseur d'identité de machine pris en charge.

Conditions requises pour l'identité d'utilisateur

Cette section décrit les conditions requises pour le fournisseur d'identité d'utilisateur que vous choisissez d'utiliser dans votre configuration d'identité. Horizon Cloud Service - next-gen prend en charge Microsoft Entra ID et Workspace ONE Access comme fournisseurs d'identité d'utilisateur.

Outre les conditions requises décrites dans cette section, reportez-vous à Configurations d'identité prises en charge pour plus d'informations sur les considérations relatives aux fonctionnalités et les fournisseurs d'identité de machine que vous pouvez utiliser avec chaque fournisseur d'identité d'utilisateur. Pour obtenir une présentation de la manière dont Horizon Cloud Service - next-gen gère les identités, reportez-vous à la section Présentation de l'identité d'utilisateur et de l'identité de machine.

Microsoft Entra ID

☐	Lorsque Microsoft Entra ID est votre fournisseur d'identité, un utilisateur disposant de privilèges d'administrateur global doit effectuer les opérations suivantes. ■ Approuvez les autorisations demandées. ■ Donnez votre consentement à l'ensemble de l'organisation.

Workspace ONE Access

☐	Lorsque Workspace ONE Access Workspace ONE Access est votre fournisseur d'identité d'utilisateur, un utilisateur disposant de privilèges d'administrateur doit effectuer les opérations suivantes. ■ Approuvez les autorisations demandées. ■ Donnez votre consentement à l'ensemble de l'organisation.

Conditions requises pour l'identité de machine

Cette section décrit les conditions requises pour le fournisseur d'identité de machine que vous choisissez d'utiliser dans votre configuration d'identité. Horizon Cloud Service - next-gen prend en charge Microsoft Entra ID et Active Directory comme fournisseurs d'identité de machine.

Outre les conditions requises décrites dans cette section, reportez-vous à Configurations d'identité prises en charge pour plus d'informations sur les considérations relatives aux fonctionnalités et les fournisseurs d'identité d'utilisateur que vous pouvez utiliser avec chaque fournisseur d'identité de machine. Pour obtenir une présentation de la manière dont Horizon Cloud Service - next-gen gère les identités, reportez-vous à la section Présentation de l'identité d'utilisateur et de l'identité de machine.

Microsoft Entra ID

☐	Pour activer la suppression d'un pool ou d'une VM, le principal de service doit disposer des autorisations de suppression de l'entrée de périphérique à partir de Microsoft Entra ID. Les autorisations sont les suivantes : ■ `Scope: https://graph.microsoft.com/` ■ `Permission : Device.ReadWrite.All` ■ `Read and write devices` ■ `Admin Consent : Yes` L'autorisation peut être accordée en accédant à l'emplacement suivant : **Abonnement -> Azure Active Directory -> Enregistrements d'applications -> Sélectionner l'application à laquelle l'autorisation doit être accordée -> Autorisation d'API -> Sélectionner Microsoft Graph -> Sélectionner Device.ReadWriteAll**
☐	Configurez RBAC dans Microsoft Entra ID. Cette configuration garantit que seuls les utilisateurs ou les groupes d'utilisateurs disposant d'un rôle **Connexion d'administrateur de machine virtuelle** ou **Connexion d'utilisateur de machine virtuelle** peuvent se connecter à leurs droits.

Active Directory

☐	Serveur Active Directory avec une vue directe sur les instances de la passerelle Horizon Edge et les sous-réseaux de poste de travail. Par exemple : ■ Serveur Active Directory sur site connecté via un VPN/Express Route ■ Un serveur Active Directory situé dans Microsoft Azure
☐	Si vous prévoyez de connecter votre annuaire Active Directory avec LDAPS, collectez les certificats d'autorité de certification racine et intermédiaire codés au format PEM pour votre domaine Active Directory. Lorsque vous utilisez Horizon Universal Console pour configurer votre domaine Active Directory, vous êtes alors invité à charger les certificats d'autorité de certification racine et intermédiaire codés au format PEM.
☐	Niveaux fonctionnels de domaine des services de domaine Microsoft Windows Active Directory (AD DS) pris en charge. ■ Windows Server 2016 ■ Windows Server 2012 R2 ■ Windows Server 2012 Versions de SE des services de domaine Microsoft Windows Active Directory (AD DS) prises en charge. ■ Windows Server 2019 ■ Windows Server 2016 ■ Windows Server 2012 R
☐	**Compte de liaison de domaine** Compte de liaison de domaine Active Directory (utilisateur standard avec accès en lecture) disposant de l'attribut sAMAccountName. La longueur de l'attribut sAMAccountName ne doit pas dépasser 20 caractères et il ne peut contenir aucun des caractères suivants : `" / \ [ ] : ; | = , + * ? < >` Le compte doit disposer des autorisations suivantes : ■ Contenu de la liste ■ Toutes les propriétés - accès en lecture ■ Autorisations d'accès en lecture ■ tokenGroupsGlobalAndUniversal - accès en lecture (sous-entendu par Toutes les propriétés - accès en lecture) Définissez le mot de passe du compte sur N'expire jamais pour garantir un accès continu pour vous connecter à votre environnement Horizon Cloud. ■ Si vous connaissez bien l'offre Horizon sur site, les autorisations ci-dessus sont les mêmes que celles requises pour les comptes d'informations d'identification secondaires de l'offre Horizon sur site. ■ Les comptes de liaison de domaine se voient accorder les autorisations prêtes à l'emploi liées à l'accès en lecture par défaut et en général accordées aux Utilisateurs authentifiés dans un déploiement de Microsoft Active Directory. Cependant, si les administrateurs AD de votre organisation ont choisi de verrouiller les autorisations liées à l'accès en lecture pour les utilisateurs standard, vous devez demander aux administrateurs AD de conserver les valeurs standard par défaut des utilisateurs authentifiés pour les comptes de liaison de domaine que vous utiliserez pour Horizon Cloud. Référence : Création de comptes de liaison de domaine et de jonction de domaine dans Active Directory

☐	**Compte de liaison de domaine auxiliaire** Doit être distinct du compte de liaison de domaine principal. L'interface utilisateur empêche la réutilisation du même compte dans les deux champs. Compte de liaison de domaine Active Directory (utilisateur standard avec accès en lecture) disposant de l'attribut sAMAccountName. La longueur de l'attribut sAMAccountName ne doit pas dépasser 20 caractères et il ne peut contenir aucun des caractères suivants : `" / \ [ ] : ; | = , + * ? < >` Le compte doit disposer des autorisations suivantes : ■ Contenu de la liste ■ Toutes les propriétés - accès en lecture ■ Autorisations d'accès en lecture ■ tokenGroupsGlobalAndUniversal - accès en lecture (sous-entendu par Toutes les propriétés - accès en lecture) Définissez le mot de passe du compte sur N'expire jamais pour garantir un accès continu pour vous connecter à votre environnement Horizon Cloud. ■ Si vous connaissez bien l'offre Horizon sur site, les autorisations ci-dessus sont les mêmes que celles requises pour les comptes d'informations d'identification secondaires de l'offre Horizon sur site. ■ Les comptes de liaison de domaine se voient accorder les autorisations prêtes à l'emploi liées à l'accès en lecture par défaut et en général accordées aux Utilisateurs authentifiés dans un déploiement de Microsoft Active Directory. Cependant, si les administrateurs AD de votre organisation ont choisi de verrouiller les autorisations liées à l'accès en lecture pour les utilisateurs standard, vous devez demander aux administrateurs AD de conserver les valeurs standard par défaut des utilisateurs authentifiés pour les comptes de liaison de domaine que vous utiliserez pour Horizon Cloud.

☐	**Compte de jonction de domaine** Compte de jonction de domaine Active Directory qui peut être utilisé par le système pour effectuer des opérations Sysprep et joindre les ordinateurs virtuels au domaine. Généralement, il s'agit d'un nouveau compte que vous créez dans ce but explicite. (Un compte d'utilisateur de jonction de domaine) Le compte doit disposer de l'attribut sAMAccountName. La longueur de l'attribut sAMAccountName ne doit pas dépasser 20 caractères et il ne peut contenir aucun des caractères suivants : `" / \ [ ] : ; | = , + * ? < >` L'utilisation d'espaces blancs dans le nom d'utilisateur du compte n'est actuellement pas prise en charge. Définissez le mot de passe du compte sur N'expire jamais pour qu'Horizon Cloud puisse continuer à effectuer les opérations Sysprep et à joindre les ordinateurs virtuels au domaine. Ce compte nécessite les autorisations Active Directory suivantes, appliquées à l'unité d'organisation Ordinateurs ou à l'unité d'organisation que vous entrez dans l'interface utilisateur de jonction de domaine de la console. ■ Toutes les propriétés - accès en lecture : cet objet uniquement ■ Créer des objets ordinateur : cet objet et tous les objets descendants ■ Supprimer les objets ordinateur : cet objet et tous les objets descendants ■ Toutes les propriétés - accès en écriture : objets ordinateur descendants ■ Réinitialiser le mot de passe : objets ordinateur descendants En ce qui concerne l'unité d'organisation (OU) cible que vous prévoyez d'utiliser pour les pools, ce compte nécessite également l'autorisation Active Directory nommée Toutes les propriétés - accès en écriture sur tous les objets descendants de cette unité d'organisation (OU) cible. Pour plus d'informations sur la création et la réutilisation de comptes de jonction de domaine, reportez-vous à la section Création de comptes de liaison de domaine et de jonction de domaine dans Active Directory. Dans Microsoft Active Directory, lorsque vous créez une unité d'organisation, le système peut définir automatiquement l'attribut `Prevent Accidental Deletion` qui applique un `Deny` à l'autorisation Supprimer tous les objets enfants de l'unité d'organisation récemment créée et de tous les objets descendants. Par conséquent, si vous avez explicitement attribué l'autorisation Supprimer des objets de l'ordinateur au compte de jonction de domaine, dans le cas d'une unité d'organisation récemment créée, Active Directory peut avoir appliqué un remplacement à cette autorisation de suppression d'objets de l'ordinateur explicitement attribuée. Étant donné que l'effacement de l'indicateur **Empêcher la suppression accidentelle** peut ne pas effacer automatiquement le `Deny` qu'Active Directory a appliqué à l'autorisation de suppression de tous les objets enfants, dans le cas d'une unité d'organisation récemment ajoutée, vous devrez peut-être vérifier et effacer manuellement l'autorisation `Deny` définie pour supprimer tous les objets enfants dans l'unité d'organisation et toutes les unités d'organisation enfants avant d'utiliser le compte de jonction de domaine dans la console Horizon Cloud.

☐	**Compte de jonction de domaine auxiliaire facultatif** Compte de jonction de domaine Active Directory qui peut être utilisé par le système pour effectuer des opérations Sysprep et joindre les ordinateurs virtuels au domaine. Généralement, il s'agit d'un nouveau compte que vous créez dans ce but explicite. (Un compte d'utilisateur de jonction de domaine) Le compte doit disposer de l'attribut sAMAccountName. La longueur de l'attribut sAMAccountName ne doit pas dépasser 20 caractères et il ne peut contenir aucun des caractères suivants : `"/ \ [ ] : ; | = , + * ? < >` L'utilisation d'espaces blancs dans le nom d'utilisateur du compte n'est actuellement pas prise en charge. Définissez le mot de passe du compte sur N'expire jamais pour qu'Horizon Cloud puisse continuer à effectuer les opérations Sysprep et à joindre les ordinateurs virtuels au domaine. Ce compte nécessite les autorisations Active Directory suivantes, appliquées à l'unité d'organisation Ordinateurs ou à l'unité d'organisation que vous entrez dans l'interface utilisateur de jonction de domaine de la console. ■ Toutes les propriétés - accès en lecture : cet objet uniquement ■ Créer des objets ordinateur : cet objet et tous les objets descendants ■ Supprimer les objets ordinateur : cet objet et tous les objets descendants ■ Toutes les propriétés - accès en écriture : objets ordinateur descendants ■ Réinitialiser le mot de passe : objets ordinateur descendants En ce qui concerne l'unité d'organisation (OU) cible que vous prévoyez d'utiliser pour les pools, ce compte nécessite également l'autorisation Active Directory nommée Toutes les propriétés - accès en écriture sur tous les objets descendants de cette unité d'organisation (OU) cible. Dans Microsoft Active Directory, lorsque vous créez une unité d'organisation, le système peut définir automatiquement l'attribut `Prevent Accidental Deletion` qui applique un `Deny` à l'autorisation Supprimer tous les objets enfants de l'unité d'organisation récemment créée et de tous les objets descendants. Par conséquent, si vous avez explicitement attribué l'autorisation Supprimer des objets de l'ordinateur au compte de jonction de domaine, dans le cas d'une unité d'organisation récemment créée, Active Directory peut avoir appliqué un remplacement à cette autorisation de suppression d'objets de l'ordinateur explicitement attribuée. Étant donné que l'effacement de l'indicateur **Empêcher la suppression accidentelle** peut ne pas effacer automatiquement le `Deny` qu'Active Directory a appliqué à l'autorisation de suppression de tous les objets enfants, dans le cas d'une unité d'organisation récemment ajoutée, vous devrez peut-être vérifier et effacer manuellement l'autorisation `Deny` définie pour supprimer tous les objets enfants dans l'unité d'organisation et toutes les unités d'organisation enfants avant d'utiliser le compte de jonction de domaine dans la console Horizon Cloud.
☐	Unités d'organisation Active Directory pour les postes de travail virtuels et les postes de travail basés sur une session RDS et/ou les applications publiées. Dans Microsoft Active Directory, lorsque vous créez une unité d'organisation, le système peut définir automatiquement l'attribut `Prevent Accidental Deletion` qui applique un `Deny` à l'autorisation Supprimer tous les objets enfants de l'unité d'organisation récemment créée et de tous les objets descendants. Par conséquent, si vous avez explicitement attribué l'autorisation Supprimer des objets de l'ordinateur au compte de jonction de domaine, dans le cas d'une unité d'organisation récemment créée, Active Directory peut avoir appliqué un remplacement à cette autorisation de suppression d'objets de l'ordinateur explicitement attribuée. Étant donné que l'effacement de l'indicateur **Empêcher la suppression accidentelle** peut ne pas effacer automatiquement le `Deny` qu'Active Directory a appliqué à l'autorisation de suppression de tous les objets enfants, dans le cas

	d'une unité d'organisation récemment ajoutée, vous devrez peut-être vérifier et effacer manuellement l'autorisation `Deny` définie pour supprimer tous les objets enfants dans l'unité d'organisation et toutes les unités d'organisation enfants avant d'utiliser le compte de jonction de domaine dans la console Horizon Cloud.

Image Management System Requirements

Votre abonnement Microsoft Azure doit intégrer les conditions requises suivantes en fonction des types d'images à provisionner à partir du dispositif Horizon Edge déployé.

☐	Base de l'image. Une ou plusieurs des configurations de VM Microsoft Azure prises en charge. ■ Les VM Microsoft Azure de génération 1 et 2 sont prises en charge. Assurez-vous que vous disposez d'un quota suffisant pour le modèle à utiliser pour la VM de base. Les types de modèles suivants sont définis par défaut et recommandés. **Sans GPU :** ■ Standard_DS2_v2 **GPU activé :** ■ Standard_NV12s_v3 Outre les types répertoriés **Sans GPU** et **Avec GPU activé**, les types de modèles sont pris en charge, mais pas nécessairement vérifiés. Assurez-vous que vous disposez d'un quota suffisant dans votre abonnement si vous sélectionnez l'un de ces modèles.

Configuration requise pour les VM de pool

Votre abonnement Microsoft Azure doit intégrer les conditions requises suivantes en fonction des types de VM de pool à provisionner à partir du dispositif Horizon Edge déployé.

☐	Sélection du modèle de VM dans les pools : toutes les configurations de VM Microsoft Azure disponibles dans la région Microsoft Azure, à l'exception de celles qui ne sont pas compatibles avec les opérations de poste de travail Horizon Cloud. Tenez compte des détails suivants lors de la sélection d'un modèle de VM. ■ La décision de choisir entre un type de modèle avec GPU activé et un type de modèle sans GPU dépend de la VM sélectionnée lors de la création de l'image. ■ Pour créer un pool à plusieurs sessions, sélectionnez une image créée à l'aide d'un système d'exploitation à plusieurs sessions. ■ Pour les environnements de production, le test de dimensionnement recommande d'utiliser des modèles disposant d'au moins 2 CPU. ■ Reportez-vous à la section Types et tailles de VM Microsoft Azure pour Horizon Cloud Service - next-gen (89090) pour en savoir plus sur la compatibilité des différents types et des différentes tailles de VM Microsoft Azure avec VMware Horizon Cloud Service - next-gen. ■ Les VM Microsoft Azure de génération 1 et 2 sont prises en charge dans les pools.

Conditions requises pour Horizon Client et Horizon HTML Access (client Web)

☐	Pour activer l'accès des utilisateurs finaux aux ressources autorisées dans votre environnement Horizon Cloud, assurez-vous qu'ils utilisent l'un des clients pris en charge suivants. **Horizon Client** Les utilisateurs finaux peuvent utiliser les versions d'Horizon Client suivantes : ■ Horizon Client pour Windows 2111 ou version ultérieure ■ Horizon Client pour Mac 2111 ou version ultérieure ■ Horizon Client pour Linux 2206 ou version ultérieure ■ Horizon Client 2303 pour Android ou une version ultérieure ■ Horizon Client 2303 pour iOS ou une version ultérieure ■ Horizon Client 2306 pour Chrome ou une version ultérieure **Horizon HTML Access** Les utilisateurs finaux peuvent se connecter à la version d'HTML Access intégrée à l'environnement Horizon Cloud.

Conditions requises pour les ports et les protocoles pour votre déploiement d'Horizon Cloud dans Microsoft Azure

Cette page est une référence pour tous les ports et protocoles possibles utilisés pour la communication dans un déploiement d'Horizon Cloud Service on Microsoft Azure standard d'Horizon Cloud Service - next-gen. Utilisez ces tableaux pour vous assurer que votre configuration réseau et vos pare-feu autoriseront le trafic de communication requis pour un déploiement réussi et des opérations quotidiennes.

Les ports et protocoles spécifiques requis pour votre déploiement particulier dépendront en partie des fonctionnalités que vous choisissez d'utiliser pour votre déploiement d'Horizon Cloud Service on Microsoft Azure. Si vous ne prévoyez pas d'utiliser un composant ou un protocole spécifique, le trafic de communication requis n'est pas nécessaire à vos objectifs. Vous pouvez alors ignorer les ports associés à ce composant. Par exemple, il n'est pas nécessaire d'autoriser les ports PCoIP si vos utilisateurs finaux n'utilisent que le protocole d'affichage Blast Extreme.

Important Outre les ports et protocoles décrits ici, les conditions requises du DNS pour le déploiement d'un dispositif Horizon Edge et ses opérations quotidiennes sont spécifiques. Pour plus d'informations, reportez-vous à la section Rendre les URL de destination appropriées accessibles pour déployer une passerelle Passerelle Horizon Edge dans un environnement Microsoft Azure.

Ports et protocoles requis par Horizon Edge

Lorsque vous activez Surveillance de l'infrastructure Horizon, Horizon Edge est déployé et configuré dans l'abonnement associé. Le tableau suivant répertorie les ports et les protocoles nécessaires lors du processus d'activation qui déploie le dispositif et configure les VM du gestionnaire afin que le dispositif puisse collecter les données de surveillance qu'il vise à collecter à partir de ces composants. Ce tableau répertorie également les ports et les protocoles qui sont nécessaires en période de stabilité pendant les opérations de collecte des données que le dispositif vise à collecter.

Tableau 2-5.

Source	Cible	Ports	Protocoles	Objectif
Horizon Edge	VM Unified Access Gateway	9443	HTTPS	Ce port est utilisé par la VM Edge sur le sous-réseau de gestion pour configurer les paramètres de la configuration d'Unified Access Gateway du dispositif Edge. Cette condition requise de port s'applique lors du déploiement initial d'une configuration d'Unified Access Gateway et lors de la modification d'un dispositif Edge pour ajouter une configuration d'Unified Access Gateway, ou les paramètres de mise à jour de cette configuration d'Unified Access Gateway surveillent également les statistiques de session à partir d'Unified Access Gateway.
Horizon Edge	Contrôleur de domaine	Kerberos : 88 LDAP : 389, 3268 LDAPS : 636, 3269	TCP UDP	Enregistrement de votre instance d'Horizon Cloud NextGen dans le domaine, ainsi que pour la connexion SSO et la détection périodique des contrôleurs de domaine. Ces ports sont requis pour les services LDAP ou LDAPS lorsque LDAP/LDAPS sera spécifié dans ce workflow. LDAP est la valeur par défaut pour la plupart des locataires.

Tableau 2-5. (suite)

Source	Cible	Ports	Protocoles	Objectif
				La cible est le serveur qui contient un rôle de contrôleur de domaine dans la configuration d'Active Directory.
Horizon Edge	Services de certificats AD	135 et un port compris entre 49152 et 65535	RPC/TCP	Connexion à l'autorité de certification d'entreprise Microsoft (AD CS) pour obtenir des certificats de courte durée pour True SSO. Horizon Edge utilise le port TCP 135 pour la communication RPC initiale et un port compris entre 49152 et 65535 pour communiquer avec les Services de certificats Active Directory (AD CS).
Horizon Edge	Serveur DNS	53 et 853	TCP UDP	Services DNS.
Horizon Edge	*.file.core.windows.net	445	TCP	Accédez aux partages de fichiers provisionnés pour les workflows App Volumes d'importation de modules et de réplication de ces derniers dans les partages de fichiers.

Tableau 2-5. (suite)

Source	Cible	Ports	Protocoles	Objectif
Horizon Edge	■ *.blob.core.windows.net ■ *.blob.storage.azure.net	443	TCP	Utilisé pour l'accès par programme au stockage Blob Azure et pour charger les journaux Horizon Edge le cas échéant. Utilisé pour le téléchargement des images du Docker afin de créer les modules Horizon Edge requis qui sont utiles pour la surveillance, SSO, les mises à jour d'UAG, etc.
Horizon Edge	horizonedgeprod.azurecr.io	443	TCP	Utilisé pour l'authentification lors du téléchargement des images du Docker afin de créer les modules Horizon Edge requis, qui sont utiles pour la surveillance, SSO, les mises à jour d'UAG, etc.
Horizon Edge	*.azure-devices.net	443	TCP	Dispositif utilisé pour communiquer avec le plan de contrôle du cloud, télécharger les configurations du module du dispositif et mettre à jour l'état d'exécution du module du dispositif. Les points de terminaison concrets actuels sont les suivants : Amérique du Nord : ■ edgehubprodna.azure-devices.net Europe : ■ edgehubprodeu.azure-devices.net Japon : ■ edgehubprodjp.azure-devices.net

Tableau 2-5. (suite)

Source	Cible	Ports	Protocoles	Objectif
Horizon Edge	vmwareprod.wavefront.com	443	TCP	Utilisé pour l'envoi de mesures d'opération à VMware Tanzu Observability by Wavefront. Les opérateurs VMware reçoivent les données avec lesquelles prendre en charge les clients. Tanzu Observability est une plate-forme d'analyse en continu. Vous pouvez envoyer vos données à Tanzu Observability, et afficher les données et interagir avec celles-ci dans des tableaux de bord personnalisés. Reportez-vous à la documentation de VMware Tanzu Observability by Wavefront.

Tableau 2-5. (suite)

Source	Cible	Ports	Protocoles	Objectif
Horizon Edge	*.data.vmwservices.com	443	TCP	Pour envoyer des événements ou des mesures à Workspace ONE Intelligence pour la surveillance des données. Reportez-vous à Workspace ONE Intelligence. Les points de terminaison concrets actuels sont les suivants : ■ eventproxy.na1.data.vmwservices.com ■ eventproxy.eu1.data.vmwservices.com ■ eventproxy.eu2.data.vmwservices.com ■ eventproxy.uk1.data.vmwservices.com ■ eventproxy.ca1.data.vmwservices.com ■ eventproxy.ap1.data.vmwservices.com ■ eventproxy.au1.data.vmwservices.com ■ eventproxy.in1.data.vmwservices.com
Horizon Edge	login.microsoftonline.com	443	TCP	Généralement utilisé par les applications pour s'authentifier auprès du service Microsoft Azure.

Tableau 2-5. (suite)

Source	Cible	Ports	Protocoles	Objectif
Horizon Edge	management.azure.com	443	TCP	Utilisé pour les demandes d'API du dispositif Edge aux points de terminaison de Microsoft Azure Resource Manager pour utiliser les services de Microsoft Azure Resource Manager. Microsoft Azure Resource Manager fournit une couche de gestion cohérente pour effectuer des tâches via Azure PowerShell, Azure CLI, le portail Azure, REST API et les SDK client.

Tableau 2-5. (suite)

Source	Cible	Ports	Protocoles	Objectif
Horizon Edge	*.horizon.vmware.com Spécifique de la région États-Unis ■ cloud-sg-us-r-westus2.horizon.vmware.com ■ cloud-sg-us-r-eastus2.horizon.vmware.com ■ cloud-sg-us.horizon.vmware.com Union européenne ■ cloud-sg-eu-r-northeurope.horizon.vmware.com ■ cloud-sg-eu-r-germanywestcentral.horizon.vmware.com ■ cloud-sg-eu.horizon.vmware.com Japon ■ cloud-sg-jp-r-japaneast.horizon.vmware.com ■ cloud-sg-jp.horizon.vmware.com	443	TCP	Dispositif utilisé pour communiquer avec le plan de contrôle du cloud et pour les opérations de jour 2.
Horizon Edge	Serveur NTP	123	UDP	Services NTP

Conditions requises pour les ports et protocoles de la VM Unified Access Gateway

Outre la configuration requise pour les principaux ports et protocoles répertoriés dans le tableau ci-dessus, les ports et protocoles des tableaux suivants sont associés aux passerelles que vous avez configurées pour qu'elles fonctionnent lors des opérations en cours après le déploiement.

Pour les connexions configurées avec des instances d'Unified Access Gateway, le trafic doit être autorisé depuis des instances d'Unified Access Gateway vers des cibles répertoriées dans le tableau ci-dessous.

Tableau 2-6. Configuration requise pour les ports du trafic provenant des instances d'Unified Access Gateway

Source	Cible	Port	Protocole	Objectif
Unified Access Gateway	*.horizon.vmware.com	53 ou 443 sur le réseau DMZ	TCP UDP	Unified Access Gateway doit être en mesure de résoudre ces adresses à tout moment, ou l'utilisateur ne pourra pas lancer la session, car Unified Access Gateway extrait le JWK défini depuis : cloud-sg-<region>-r-<DC>.horizon.vmware.com. Les points de terminaison concrets actuels sont les suivants : ■ États-Unis ■ cloud.horizon.vmware.com cloud-sg-us-r-westus2.horizon.vmware.com cloud-sg-us-r-eastus2.horizon.vmware.com ■ cloud.horizon.vmware.com cloud-sg-us-r-westus2.horizon.vmware.com cloud-sg-us-r-eastus2.horizon.vmware.com ■ Union européenne ■ cloud.horizon.vmware.com cloud-sg-eu-r-northeurope.horizon.vmware.com cloud-sg-eu-r-germanywestcentral.horizon.vmware.com ■ Japon ■ cloud.horizon.vmware.com cloud-sg-jp-r-japaneast.horizon.vmware.com
Unified Access Gateway	Horizon Agent sur les machines virtuelles de poste de travail ou RDSH de batterie de serveurs	22443	TCP UDP	Blast Extreme Par défaut, le trafic de redirection de lecteur client (CDR) et le trafic USB sont à canal latéral dans ce port lorsque Blast Extreme est utilisé. Si vous préférez, le trafic CDR peut être séparé sur le port TCP 9427 et le trafic de redirection USB peut être séparé sur le port TCP 32111.
Unified Access Gateway	Horizon Agent sur les machines virtuelles de poste de travail ou RDSH de batterie de serveurs	9427	TCP	Facultatif pour le trafic de redirection CDR et multimédia (MMR).

Tableau 2-6. Configuration requise pour les ports du trafic provenant des instances d'Unified Access Gateway (suite)

Source	Cible	Port	Protocole	Objectif
Unified Access Gateway	Horizon Agent sur les machines virtuelles de poste de travail ou RDSH de batterie de serveurs	32111	TCP	Facultatif pour le trafic de redirection USB.
Unified Access Gateway	time.google.com	123	UDP	Services NTP
Unified Access Gateway	*.blob.core.windows.net *.blob.storage.azure.net	443	TCP	Utilisé pour l'accès par programme au stockage Blob Azure pour charger les journaux Unified Access Gateway le cas échéant.

Ports et protocoles App Volumes

Pour prendre en charge les fonctionnalités d'App Volumes à utiliser avec Horizon Cloud Service on Microsoft Azure, vous devez configurer le port 445 pour le trafic de protocole TCP vers le sous-réseau de locataire (postes de travail). Le port 445 est le port SMB standard pour accéder à un partage de fichiers SMB sur Microsoft Windows. Les AppStacks sont stockés dans un partage de fichiers SMB situé dans le même groupe de ressources que celui des VM du gestionnaire d'espace.

Tableau 2-7. Spécification des ports pour App Volumes

Source	Cible	Port	Protocole	Objectif
App Volumes Agent sur la machine virtuelle importée de base, les images standard, les machines virtuelles de poste de travail et les machines virtuelles RDSH de batterie de serveurs	*.file.core.windows.net	445	TCP	La virtualisation d'applications App Volumes sur les machines VDI et la capture de modules d'application sur les machines VDI dépendent de l'accès aux partages de fichiers.

Conditions requises pour les ports et protocoles VDI

Le tableau suivant fournit les ports et protocoles requis pour les sous-réseaux de poste de travail (VDI ou locataire) configurés dans votre environnement.

Tableau 2-8. Conditions requises pour les ports et protocoles VDI

Source	Cible	Port	Protocole	Objectif
Sous-réseau de poste de travail (locataire)	*.horizon.vmware.com	443	Protocole MQTT sur TCP	Pour les opérations liées à l'agent, telles que la signature de certificat à l'aide du Hub de VM et le renouvellement. Les points de terminaison concrets actuels sont les suivants : États-Unis : ■ cloud-sg-us-r-westus2.horizon.vmware.com ■ cloud-sg-us-r-westus2-mqtt.horizon.vmware.com ■ cloud-sg-us-r-eastus2.horizon.vmware.com ■ cloud-sg-us-r-eastus2-mqtt.horizon.vmware.com Union européenne : ■ cloud-sg-eu-r-northeurope.horizon.vmware.com ■ cloud-sg-eu-r-northeurope-mqtt.horizon.vmware.com ■ cloud-sg-eu-r-germanywestcentral.horizon.vmware.com ■ cloud-sg-eu-r-germanywestcentral-mqtt.horizon.vmware.com Japon : ■ cloud-sg-jp-r-japaneast.horizon.vmware.com ■ cloud-sg-jp-r-japaneast-mqtt.horizon.vmware.com
Sous-réseau de poste de travail (locataire)	Contrôleur de domaine	88	TCP UDP	Services Kerberos. La cible est le serveur qui contient un rôle de contrôleur de domaine dans une configuration Active Directory. L'enregistrement du dispositif Edge dans Active Directory est obligatoire.
Sous-réseau de poste de travail (locataire)	Contrôleur de domaine	Kerberos : 88 LDAP : 389, 3268 LDAPS : 636, 3269	TCP UDP	Ces ports sont requis pour les services LDAP ou LDAPS pour la connectivité entre la VM et le contrôleur de domaine si la VDI ne parvient pas à atteindre un contrôleur de domaine, le lancement de sessions est alors impossible.
Sous-réseau de poste de travail (locataire)	Serveur DNS	53 et 853	TCP UDP	Services DNS
Sous-réseau de poste de travail (locataire)	Serveur NTP	123	UDP	Services NTP

Tableau 2-8. Conditions requises pour les ports et protocoles VDI (suite)

Source	Cible	Port	Protocole	Objectif
Sous-réseau de poste de travail (locataire)	*.blob.core.windows.net	443	TCP	Chargement du bundle de journaux DCT. Lorsqu'un administrateur client clique sur la collecte des journaux DCT pour une VM après le traitement de la demande, le bundle est chargé de VDI vers blob pour que ce bundle puisse être téléchargé à partir d'Horizon Universal Console.
Sous-réseau de poste de travail (locataire)	Horizon Edge	31883	Protocole MQTT sur TCP UDP	Horizon Agent s'exécutant sur la VM vers le protocole MQTT s'exécutant sur Edge.
Sous-réseau de poste de travail (locataire)	Horizon Edge	32443	TCP	Single Sign-On lorsque le format de votre dispositif Microsoft Azure Edge est Passerelle Edge (VM).
Sous-réseau de poste de travail (locataire)	Horizon Edge	443	TCP	Single Sign-On lorsque le format de votre dispositif Microsoft Azure Edge est Passerelle Edge (AKS).
Sous-réseau de poste de travail (locataire) et sous-réseau de gestion	softwareupdate.vmware.com	443	TCP	Serveur de package logiciel VMware. Utilisé pour le téléchargement des mises à jour du logiciel lié à l'agent utilisé dans les opérations liées à l'image du système et le processus automatisé de mise à jour de l'agent.
Sous-réseau de poste de travail (locataire)	Point de terminaison de liaison privée	443	TCP	Connectivité du poste de travail au service de connexion dans le plan de contrôle du cloud.
Sous-réseau de poste de travail (locataire) et sous-réseau de gestion	Services de certificats AD	135 et 445, et un port compris entre 49152 et 6553	RPC/TCP	Pour ajouter des postes de travail au domaine.

Conditions requises pour les ports et protocoles de trafic de connexion des utilisateurs finaux

Pour obtenir des informations détaillées sur les différentes instances d'Horizon Client que vos utilisateurs finaux peuvent utiliser avec votre dispositif Dispositif virtuel Horizon Edge, reportez-vous à la page de documentation d'Horizon Client à l'adresse https://docs.vmware.com/fr/VMware-Horizon-Client/index.html. Le choix du mode de connexion de vos utilisateurs finaux détermine quels ports doivent être ouverts pour le trafic à partir des connexions des utilisateurs finaux pour accéder aux applications distantes et aux postes de travail virtuels.

Tableau 2-9. Ports et protocoles de trafic de connexion des utilisateurs finaux

Source	Cible	Port	Protocole	Objectif
Horizon Client	Équilibrage de charge Microsoft Azure pour ces instances d'Unified Access Gateway	443	TCP	Pour transporter le trafic de redirection CDR, MMR, USB et RDP par tunnel. Le protocole SSL (accès HTTPS) est activé par défaut pour les connexions client. Le port 80 (accès HTTP) peut être utilisé dans certains cas.
Horizon Client	Équilibrage de charge Microsoft Azure pour ces instances d'Unified Access Gateway	8443 ou 443	TCP	Blast Extreme via Blast Secure Gateway sur Unified Access Gateway pour le trafic de données à partir d'Horizon Client.
Horizon Client	Équilibrage de charge Microsoft Azure pour ces instances d'Unified Access Gateway	443	UDP	Blast Extreme via Unified Access Gateway pour le trafic de données.
Horizon Client	Équilibrage de charge Microsoft Azure pour ces instances d'Unified Access Gateway	8443	UDP	Blast Extreme via Blast Secure Gateway sur Unified Access Gateway pour le trafic de données (transport adaptatif).

Tableau 2-9. Ports et protocoles de trafic de connexion des utilisateurs finaux (suite)

Source	Cible	Port	Protocole	Objectif
Navigateur	Équilibrage de charge Microsoft Azure pour ces instances d'Unified Access Gateway	443	TCP	Pour transporter le trafic de redirection CDR, MMR, USB et RDP par tunnel. Le protocole SSL (accès HTTPS) est activé par défaut pour les connexions client. Le port 80 (accès HTTP) peut être utilisé dans certains cas.
Navigateur	Équilibrage de charge Microsoft Azure pour ces instances d'Unified Access Gateway	8443 ou 443	TCP	Blast Extreme via Blast Secure Gateway sur Unified Access Gateway pour le trafic de données à partir du client Horizon HTML Access (client Web).
Horizon Client/ navigateur	*.horizon.vmware.com	443	TCP	Après la connexion et la création de la liste des éléments de lancement, lorsque le client clique dessus pour lancer le poste de travail, la redirection du trafic de protocole vers Unified Access Gateway se produit à partir de l'une de ces URL en fonction de l'emplacement de l'organisation du client sélectionné lors de l'intégration. Les points de terminaison concrets actuels sont les suivants : ■ cloud-sg-us-r-westus2.horizon.vmware.com ■ cloud-sg-us-r-eastus2.horizon.vmware.com ■ cloud-sg-eu-r-northeurope.horizon.vmware.com ■ cloud-sg-eu-r-germanywestcentral.horizon.vmware.com ■ cloud-sg-jp-r-japaneast.horizon.vmware.com

Obtenir des licences pour les systèmes d'exploitation Microsoft Windows

Pour les déploiements sur Microsoft Azure, obtenez des licences Microsoft valides qui vous autorisent à créer, effectuer des workflows et à utiliser les VM de poste de travail basées sur Windows et les VM d'hôte de session Bureau à distance (RDSH) à utiliser dans votre environnement Horizon Cloud Service - next-gen.

Horizon Cloud ne nécessite aucune licence de système d'exploitation invité pour les systèmes d'exploitation Microsoft Windows que vous utilisez avec les workflows Horizon Cloud.

Pour obtenir une licence Microsoft, reportez-vous à la documentation de Microsoft concernant la licence Microsoft Azure Hybrid Benefit pour Windows Server.

VMware applique la licence d'accès client (CAL) RDS avec Software Assurance.

Rendre les URL de destination appropriées accessibles pour déployer une passerelle Passerelle Horizon Edge dans un environnement Microsoft Azure

Pour créer un déploiement d'Horizon Edge et installer ou mettre à jour des modules de dispositif dans votre environnement Horizon Cloud Service - next-gen, vous devez autoriser les URL appropriées sur les ports correspondants.

Pour les tableaux suivants, les fins répertoriées sont utilisées dans le cadre d'un déploiement d'Horizon Edge.

Autoriser les URL pour le sous-réseau de gestion et vérifier l'accès à celles-ci

Pour autoriser les URL et sous-domaines génériques appropriés en fonction de l'emplacement et des besoins de votre site, effectuez les tâches suivantes :

- Autorisez les URL et les sous-domaines génériques dans le tableau suivant. Par exemple, en ajoutant les URL et le sous-domaine générique à une liste autorisée pour le pare-feu et le groupe de sécurité réseau.
- Contournez l'inspection approfondie des paquets SSL comme suit.
  - Dans le pare-feu pour les URL et les sous-domaines génériques dans le tableau suivant.
  - Dans le serveur proxy, le cas échéant.

    Si le système Passerelle Horizon Edge est connecté à Horizon Agent via un serveur proxy, contournez l'inspection approfondie des paquets SSL dans le serveur proxy pour les URL et les sous-domaines génériques dans le tableau suivant.

Destination (nom de DNS)	Port	Protocole	Trafic du proxy (si configuré sur le déploiement)	Objectif
*.blob.core.windows.net	443	TCP	Oui	Utilisé pour l'accès par programme au stockage Blob Azure et pour charger les journaux Horizon Edge le cas échéant. Utilisé pour le téléchargement des images du Docker afin de créer les modules Horizon Edge requis qui sont utiles pour la surveillance, SSO, les mises à jour d'UAG, etc.
horizonedgeprod.azurecr.io	443	TCP	Oui	Utilisé pour l'authentification lors du téléchargement des images du Docker afin de créer les modules Horizon Edge requis, qui sont utiles pour la surveillance, SSO, les mises à jour d'UAG, etc.

Destination (nom de DNS)	Port	Protocole	Trafic du proxy (si configuré sur le déploiement)	Objectif
*.azure-devices.net ou l'un des noms spécifiques à la région ci-dessous, selon le plan de contrôle régional qui s'applique à votre compte de locataire : Amérique du Nord : ■ edgehubprodna.azure-devices.net Europe : ■ edgehubprodeu.azure-devices.net Japon : ■ edgehubprodjp.azure-devices.net	443/TCP	TCP	Oui	Utilisé pour connecter le dispositif au plan de contrôle Horizon Cloud, pour télécharger les configurations du module du dispositif et pour mettre à jour l'état d'exécution du module du dispositif.
vmwareprod.wavefront.com	443	TCP	Oui	Utilisé pour l'envoi de mesures d'opération à Tanzu Observability by Wavefront. Les opérateurs VMware reçoivent les données avec lesquelles prendre en charge les clients. Tanzu Observability est une plate-forme d'analyse en continu. Vous pouvez envoyer vos données à Tanzu Observability, et afficher les données et interagir avec celles-ci dans les tableaux de bord personnalisés. Reportez-vous à la documentation de Tanzu Observability by Wavefront.

Destination (nom de DNS)	Port	Protocole	Trafic du proxy (si configuré sur le déploiement)	Objectif
*.data.vmwservices.com ou l'un des noms spécifiques à la région ci-dessous, selon la cible Workspace ONE Intelligence régionale qui s'applique à votre compte de locataire : ■ eventproxy.na1.data.vmwservices.com ■ eventproxy.eu1.data.vmwservices.com ■ eventproxy.eu2.data.vmwservices.com ■ eventproxy.uk1.data.vmwservices.com ■ eventproxy.ca1.data.vmwservices.com ■ eventproxy.ap1.data.vmwservices.com ■ eventproxy.au1.data.vmwservices.com ■ eventproxy.in1.data.vmwservices.com	443	TCP	Oui	Utilisé pour l'envoi d'événements ou de mesures à Workspace ONE Intelligence. Reportez-vous à Workspace ONE Intelligence.
Si votre pare-feu ou groupe de sécurité réseau (NSG, Network Security Group) prend en charge l'utilisation des balises de service, appliquez la balise de service Azure `AzureCloud`. Si votre pare-feu ou votre NSG ne prend pas en charge l'utilisation de balises de service, utilisez le nom d'hôte `monitor.horizon.vmware.com`.	1514 et 1515	TCP	Non	Utilisé pour la surveillance du système.
azcopyvnext.azureedge.net	443	TCP	Oui	Utilisé pour charger les journaux de déploiement dans le stockage Blob Azure à des fins de dépannage.
■ management.azure.com ■ login.microsoftonline.com ■ mcr.microsoft.com ■ *.data.mcr.microsoft.com ■ packages.microsoft.com ■ acs-mirror.azureedge.net	443	HTTPS	Oui	Utilisé pour l'application de correctifs aux composants Microsoft de la passerelle Horizon Edge.
time.google.com	123	UDP	Oui	Utilisé pour la synchronisation de l'heure.

Destination (nom de DNS)	Port	Protocole	Trafic du proxy (si configuré sur le déploiement)	Objectif
■ security.ubuntu.com ■ azure.archive.ubuntu.com ■ changelogs.ubuntu.com ■ motd.ubuntu.com	80	HTTP	Oui	Utilisé pour l'application de correctifs aux composants Ubuntu.
*.file.core.windows.net	445	TCP	Non	Accédez aux partages de fichiers provisionnés pour les workflows App Volumes d'importation de packages et de réplication de ceux-ci dans les partages de fichiers.
softwareupdate.vmware.com	443	TCP	Oui	Serveur de module logiciel. Utilisé pour le téléchargement des mises à jour du logiciel lié à l'agent utilisé dans les opérations liées à l'image du système et le processus automatisé de mise à jour de l'agent.

Déterminer si les URL du sous-réseau de gestion sont accessibles

L'outil Vérificateur d'URL de sous-réseau du dispositif Edge Horizon Cloud Service - next-gen est disponible dans la zone Tech sur la page Utilitaires. Les informations associées sont disponibles sur la page Déploiement d'une passerelle Horizon Edge pour les environnements Horizon 8 de la zone Tech.

L'outil est fourni sous la forme d'un fichier `.exe`. Pour télécharger et utiliser l'outil Vérificateur d'URL de sous-réseau du dispositif Edge Horizon Cloud Service - next-gen sur une machine virtuelle Windows 10 ou version ultérieure sur le réseau sur lequel réside votre dispositif Horizon Edge, procédez comme suit.

1 Téléchargez le Vérificateur d'URL de sous-réseau du dispositif Edge Horizon Cloud Service - next-gen sur votre machine virtuelle Windows déployée sur le réseau Horizon Edge.

2 Double-cliquez sur le fichier pour lancer l'exécutable.

   Une boîte de dialogue apparaît.

3 Cliquez sur **Oui**.

4 Ouvrez le dossier de sortie dans `C:/VMwareURLCheckerOutput/`.

   Le dossier contient les fichiers de sortie de chaque plan de contrôle régional.

5 Ouvrez le fichier de sortie de la région dans laquelle vous déployez le dispositif Horizon Edge pour déterminer si les URL nécessaires sont accessibles.

Les détails suivants s'appliquent.

- Le fichier affiche l'état des URL requises pour le sous-réseau de gestion.
- L'état attendu pour chaque URL est ACCESSIBLE.
- Lorsque l'état de l'URL est INACCESSIBLE, affichez le message d'erreur et apportez les modifications nécessaires pour résoudre le problème.

6 Relancez l'exécutable si nécessaire jusqu'à ce que l'état de tous les domaines dans la région souhaitée soit ACCESSIBLE.

Autoriser l'URL pour le sous-réseau de locataire (poste de travail) - Nom d'hôte DNS Hub de VM global

Si l'utilisation d'une instance globale du Hub de VM répond aux besoins de votre site, autorisez l'URL suivante ainsi que ses paramètres lorsque vous déployez une passerelle Passerelle Horizon Edge.

Destination (Nom de DNS)	Port	Protocole	Objectif
*.horizon.vmware.com	443	TCP	Pour les opérations liées à l'agent, telles que la signature de certificat utilisant le Hub de VM et le renouvellement.

Autoriser les URL pour le sous-réseau de locataire (poste de travail) - noms d'hôtes DNS Hub de VM régionaux

Si l'utilisation d'instances régionales du Hub de VM répond aux besoins de votre site, utilisez les deux URL correspondantes lorsque vous déployez une passerelle Passerelle Horizon Edge dans une région donnée, comme indiqué.

Le port, le protocole et l'objectif de chaque instance régionale du Hub de VM correspondent à ceux d'une instance globale du Hub de VM, par exemple.

Port	443
Protocole	TCP
Objectif	Pour les opérations liées à l'agent, telles que la signature de certificat utilisant le Hub de VM et le renouvellement.

Pour les régions Azure suivantes	Autoriser les URL de destination (nom DNS) suivantes
■ westus2 ■ westus ■ westus3 ■ westcentralus ■ centralus	■ cloud-sg-us-r-westus2.horizon.vmware.com ■ cloud-sg-us-r-westus2-mqtt.horizon.vmware.com
■ eastus2 ■ eastus ■ southcentralus ■ northcentralus ■ canadacentral ■ canadaeast ■ brazilsouth ■ brazilsoutheast ■ usgovvirginia	■ cloud-sg-us-r-eastus2.horizon.vmware.com ■ cloud-sg-us-r-eastus2-mqtt.horizon.vmware.com
■ northeurope ■ norwaywest ■ norwayeast ■ uaecentral ■ uaenorth ■ uksouth ■ ukwest ■ westeurope	■ cloud-sg-eu-r-northeurope.horizon.vmware.com ■ cloud-sg-eu-r-northeurope-mqtt.horizon.vmware.com
■ germanywestcentral ■ germanynorth ■ swedencentral ■ swedensouth ■ francecentral ■ francesouth ■ switzerlandnorth ■ switzerlandwest	■ cloud-sg-eu-r-germanywestcentral.horizon.vmware.com ■ cloud-sg-eu-r-germanywestcentral-mqtt.horizon.vmware.com
■ japanwest ■ japaneast	■ cloud-sg-jp-r-japaneast.horizon.vmware.com ■ cloud-sg-jp-r-japaneast-mqtt.horizon.vmware.com
■ australiaeast ■ australiacentral ■ australiacentral2 ■ australiasoutheast	■ cloud-sg-jp-r-australiaeast.horizon.vmware.com ■ cloud-sg-jp-r-australiaeast-mqtt.horizon.vmware.com
■ centralindia ■ jioindiawest ■ jioindiacentral ■ southindia ■ westindia	■ cloud-sg-jp-r-centralindia.horizon.vmware.com ■ cloud-sg-jp-r-centralindia-mqtt.horizon.vmware.com

Autoriser les URL pour l'activation du proxy

Si vous prévoyez d'utiliser un serveur proxy pour contrôler le flux de trafic à partir de votre environnement, ouvrez les ports requis pour autoriser la passerelle Passerelle Horizon Edge à atteindre le serveur proxy. Lorsque le format de votre dispositif Microsoft Azure Edge est Passerelle Edge (AKS), reportez-vous à la section Règles de réseau sortant et de nom de domaine complet pour les clusters AKS (Azure Kubernetes Service).

Vérifier la disponibilité du modèle de VM Microsoft Azure

Pour vous assurer que vous disposez d'une capacité Microsoft Azure suffisante pour votre dispositif Microsoft Azure Edge, testez la disponibilité du modèle de VM Microsoft Azure et vérifiez la sortie de CPU régionale.

La procédure suivante est recommandée dans Configurations requises pour la capacité Microsoft Azure. Les étapes incluent des exemples de commandes et de sorties. Les commandes testent la disponibilité du modèle de VM Microsoft Azure qui sera utilisé pour la passerelle Passerelle Horizon Edge dans toutes les zones de disponibilité (1,2,3) d'une région spécifique.

Procédure

1 Exécutez une commande pour acquérir les restrictions de SKU régionales pour un type de machine, par exemple `Standard_D2`, comme l'illustrent l'exemple générique et l'exemple spécifique suivants.

```
az vm list-skus --location <azure_region_where_edge_is_being_deployed> --size Standard_D2
--all --output table
```

L'exemple de code suivant est un test spécifique pour les restrictions régionales dans `location westeurope`.

```
az vm list-skus --location westeurope --size Standard_D2 --all --output table
```

Voici des exemples de sortie de la commande précédente. Le premier exemple illustre un résultat réussi, indiquant l'absence de restrictions. Le deuxième exemple illustre un résultat d'échec, indiquant la présence de restrictions.

Sortie d'un résultat réussi, il n'existe aucune restriction

```
ResourceType     Locations    Name                 Zones    Restrictions
---------------  -----------  -------------------  -------  --------------
virtualMachines  westeurope   Standard_D2_v3       1,2,3    None
```

Sortie d'un résultat d'échec, il existe des restrictions

```
ResourceType     Locations    Name                 Zones    Restrictions
---------------  -----------  -------------------  -------  --------------
virtualMachines  westeurope   Standard_D2          1,2,3    'NotAvailableForSubscription,
type: Zone, locations: westeurope, zones: 1,2,3']
```

2 Exécutez une commande pour acquérir les restrictions de CPU régionales totales, comme l'illustrent l'exemple générique et l'exemple spécifique suivants.

```
az vm list-usage --location <azure_region_where_edge_is_being_deployed> -o table
```

L'exemple de code suivant est un test spécifique pour le nombre total de restrictions régionales de CPU dans `location westeurope`.

```
az vm list-usage --location westeurope -o table
```

Voici des exemples de sortie de la commande précédente. Le premier exemple illustre un résultat réussi selon lequel la valeur `CurrentValue` de `Total Regional vCPUs` est `25` ou supérieure (`26` dans ce cas), indiquant l'absence de restrictions. Le deuxième exemple illustre un résultat d'échec selon lequel la valeur `Limit` de `Total Regional vCPUs` est inférieure à `25` (`10` dans ce cas), indiquant des restrictions.

Sortie d'un résultat réussi, il n'existe aucune restriction

```
Name                                 CurrentValue    Limit
-----------------------------------  --------------  -------
Availability Sets                    1               2500
Total Regional vCPUs                 26              310
Virtual Machines                     11              25000
Virtual Machine Scale Sets           1               2500
Dedicated vCPUs                      0               3000
Cloud Services                       0               2500
```

Sortie d'un résultat d'échec, il existe des restrictions

```
Name                                 CurrentValue    Limit
-----------------------------------  --------------  -------
Availability Sets                    0               2500
Total Regional vCPUs                 0               10
Virtual Machines                     0               25000
Virtual Machine Scale Sets           0               2500
Dedicated vCPUs                      0               3000
Cloud Services                       0               2500
```

Étape suivante

- Nous vous recommandons de demander que Microsoft Azure rende la SKU disponible dans la région dans laquelle vous prévoyez de déployer la Passerelle Horizon Edge.
- Revenez à la Configurations requises pour la capacité Microsoft Azure.

.

Créer un principal de service pour l'abonnement Microsoft Azure

Pour les déploiements d'Horizon Cloud Service on Microsoft Azure, le service utilise des appels d'API pour déployer des ressources dans un abonnement Microsoft Azure et pour gérer ces

ressources. Pour permettre à Horizon Cloud d'utiliser ses appels d'API dans l'abonnement Microsoft Azure, créez un principal de service, appelé enregistrement d'application dans Microsoft Entra ID.

Créez un maximum de quatre principaux de service uniques pour un fournisseur. Pour prendre en charge un total de 5 000 VM, ajoutez quatre principaux de service. Lorsque vous disposez de plusieurs principaux de service, ils partagent l'ID d'abonnement et l'ID d'annuaire, mais chaque principal de service dispose de son propre ID d'application.

Important Utilisez le même rôle pour chaque principal de service.

Créez un principal de service pour accéder à la capacité de votre abonnement Microsoft Azure et l'utiliser pour Horizon Cloud. L'ID d'abonnement Microsoft Azure, l'ID d'annuaire, l'ID d'application et la clé sont utilisés dans Horizon Cloud.

Note Effectuez les tâches décrites dans cette section du portail Microsoft Azure. Vous trouverez les détails de la configuration dans la documentation de Microsoft, Utiliser le portail pour créer une application Azure AD et un principal de service pouvant accéder aux ressources. Alors que Microsoft recommande d'utiliser une authentification par certificat pour le principal de service, VMware requiert une authentification par clé ou secret pour le principal de service.

Un rôle doit être attribué au principal de service Horizon Cloud dans l'abonnement. En général, Horizon Cloud utilise le rôle `Contributor` intégré avec l'abonnement.

Le rôle `Contributor` est utilisé, car il couvre tous les appels d'API qu'Horizon Cloud doit effectuer dans l'abonnement. L'attribution de rôle doit être une attribution directe. L'utilisation d'une attribution basée sur un groupe d'un rôle, dans laquelle le rôle est attribué à un groupe et le principal de service est membre de ce groupe, n'est pas prise en charge.

Si votre organisation préfère éviter l'utilisation du rôle `Contributor` dans l'abonnement, Horizon Cloud prend en charge l'utilisation d'un rôle personnalisé à la place. S'il est utilisé, le rôle personnalisé doit fournir les appels d'API spécifiques qu'Horizon Cloud doit utiliser. Pour plus d'informations, reportez-vous à la section Pour utiliser un rôle personnalisé pour l'enregistrement d'applications Horizon Cloud.

Note Lors de la suppression d'un pool joint à Microsoft Entra ID ou d'une VM, le principal de service doit disposer des autorisations de suppression de l'entrée de périphérique à partir de Microsoft Entra ID.

Les autorisations sont les suivantes :

Portée : `https://graph.microsoft.com/`

Autorisation : `Device.ReadWrite.All Read and write devices`

Consentement administrateur : `Yes`

L'autorisation peut être accordée en accédant à l'emplacement suivant :

Abonnement > Azure Active Directory > Enregistrements d'applications > Sélectionner l'application à laquelle l'autorisation doit être accordée > Autorisation d'API > Sélectionner Microsoft Graph > Sélectionner Device.ReadWriteAll

Les étapes suivantes fournissent les paramètres à utiliser pour votre environnement Horizon Cloud :

Procédure

- Configurez jusqu'à quatre principaux de service et secrets du client pour l'abonnement.
  a. Définissez la durée d'expiration du secret du client sur votre longueur préférée, par exemple `24 Months`.
  b. Enregistrez une copie du secret du client pour référence ultérieure.
  c. Attribuez le rôle approprié à chaque principal de service pour permettre à ce dernier de gérer les ressources dans l'abonnement.

Étape suivante

Enregistrez les fournisseurs de ressources requis. Reportez-vous à la section Confirmer que les fournisseurs de ressources requis sont enregistrés dans votre abonnement Microsoft Azure.

Confirmer que les fournisseurs de ressources requis sont enregistrés dans votre abonnement Microsoft Azure

Dans votre abonnement Microsoft Azure pour Horizon Cloud Service - next-gen, l'état de plusieurs fournisseurs de ressources doit être enregistré.

Assurez-vous que l'état des fournisseurs de ressources répertoriés est enregistré avant de déployer un dispositif Horizon Edge. L'étape finale du déploiement d'Horizon Edge confirme que l'état de ces fournisseurs de ressources est enregistré et empêche le démarrage du déploiement d'Horizon Edge si l'un d'entre eux est désinscrit.

Notez que contrairement à d'autres fournisseurs de ressources, certains d'entre eux peuvent être dotés de l'état enregistré. Cette variation potentielle de l'état est due au comportement standard de Microsoft Azure, dans lequel un ensemble de fournisseurs de ressources est enregistré pour tous les abonnements Microsoft Azure.

Les fournisseurs de ressources requis suivants doivent être enregistrés dans l'abonnement Microsoft Azure :

- Microsoft.Authorization
- Microsoft.Compute
- Microsoft.ContainerService
- Microsoft.KeyVault
- Microsoft.MarketplaceOrdering
- Microsoft.ResourceGraph
- Microsoft.Network
- Microsoft.Resources
- Microsoft.Security
- Microsoft.Storage
- Microsoft.ManagedIdentity

Vérifiez que les fournisseurs de ressources ci-dessus sont enregistrés dans l'abonnement Microsoft Azure à l'aide de la procédure suivante :

1 Connectez-vous au portail Microsoft Azure et recherchez l'abonnement dans lequel vous prévoyez de déployer l'instance d'Horizon Edge.

2 Cliquez sur le nom de l'abonnement et faites défiler l'écran vers le bas jusqu'à ce que l'élément de menu **Fournisseurs de ressources** s'affiche.

3 Recherchez les fournisseurs de ressources répertoriés ci-dessus et vérifiez qu'ils affichent chacun un état coché **Enregistré**.

   Utilisez le portail Microsoft Azure pour enregistrer un fournisseur de ressources de la liste précédente dont l'état est **Non enregistré**.

Pour utiliser un rôle personnalisé pour l'enregistrement d'applications Horizon Cloud

Le rôle `Contributor` est généralement utilisé pour activer le processus d'enregistrement d'applications Horizon Cloud afin d'effectuer des appels d'API dans l'abonnement Microsoft Azure. Si vous préférez éviter l'utilisation du rôle `Contributor`, vous pouvez créer un rôle

personnalisé à cette fin. Le rôle personnalisé dispose de certaines autorisations requises et facultatives que vous devez connaître lorsque vous créez un principal de service.

Pour créer un rôle personnalisé, utilisez un outil, tel qu'Azure PowerShell ou Azure CLI, et créez une définition de rôle personnalisé qui, au minimum, inclut les autorisations obligatoires répertoriées dans cette rubrique. Reportez-vous à l'exemple JSON ci-après. Pour plus d'informations sur les autorisations Microsoft Azure spécifiques répertoriées sur cette page, reportez-vous à la section Opérations du fournisseur de ressources Azure.

Autorisations obligatoires

Tableau 2-10. Opérations sur les ressources Microsoft Azure qui doivent être autorisées dans le rôle personnalisé lors de l'attribution d'autorisations au niveau de l'abonnement

Opération
Microsoft.Authorization/*/read
Microsoft.Compute/*/read
Microsoft.Compute/availabilitySets/*
Microsoft.Compute/disks/*
Microsoft.Compute/galleries/read Microsoft.Compute/galleries/write Microsoft.Compute/galleries/delete Microsoft.Compute/galleries/images/* Microsoft.Compute/galleries/images/versions/*
Microsoft.Compute/images/*
Microsoft.Compute/locations/*
Microsoft.Compute/snapshots/*
Microsoft.Compute/virtualMachines/*
Microsoft.Compute/virtualMachineScaleSets/*
Microsoft.ContainerService/managedClusters/delete
Microsoft.ContainerService/managedClusters/read
Microsoft.ContainerService/managedClusters/write
Microsoft.ContainerService/managedClusters/commandResults/read
Microsoft.ContainerService/managedClusters/runcommand/action
Microsoft.ContainerService/managedClusters/upgradeProfiles/read
Microsoft.ManagedIdentity/userAssignedIdentities/*/assign/action
Microsoft.ManagedIdentity/userAssignedIdentities/*/read

Tableau 2-10. Opérations sur les ressources Microsoft Azure qui doivent être autorisées dans le rôle personnalisé lors de l'attribution d'autorisations au niveau de l'abonnement (suite)

Opération
Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write
Microsoft.Network/loadBalancers/*
Microsoft.Network/networkInterfaces/*
Microsoft.Network/networkSecurityGroups/*
Microsoft.Network/virtualNetworks/read
Microsoft.Network/virtualNetworks/write
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read
Microsoft.Network/virtualNetworks/subnets/*
Microsoft.Network/virtualNetworks/virtualNetworkPeerings/read
Microsoft.ResourceGraph/*
Microsoft.Resources/deployments/*
Microsoft.Resources/subscriptions/read
Microsoft.Resources/subscriptions/resourceGroups/*
Microsoft.ResourceHealth/availabilityStatuses/read
Microsoft.Storage/*/read
Microsoft.Storage/storageAccounts/*

Si vous prévoyez d'utiliser App Volumes, assurez-vous d'avoir configuré les autorisations répertoriées dans le tableau au niveau de l'abonnement. Pour plus d'informations sur ces autorisations, reportez-vous à la section Point de terminaison privé Azure pour un compte de stockage d'applications App Volumes.

Opération
Microsoft.Network/locations/availablePrivateEndpointTypes/read
Microsoft.Network/privateEndpoints/read
Microsoft.Network/privateEndpoints/write
Microsoft.Network/privateEndpoints/delete
Microsoft.Network/virtualNetworks/read
Microsoft.Network/virtualNetworks/subnets/read

Opération
Microsoft.Network/virtualNetworks/subnets/write
Microsoft.Network/virtualNetworks/subnets/join/action
Microsoft.Resources/deployments/*
Microsoft.Resources/subscriptions/read
Microsoft.Resources/subscriptions/resourceGroups/read

Autorisations facultatives

Les autorisations suivantes ne sont pas obligatoires pour le déploiement d'Horizon Edge dans Microsoft Azure. Cependant, les fonctionnalités d'Horizon Universal Console qui reposent sur ces autorisations facultatives ne fonctionnent pas si vous ne les incluez pas.

Tableau 2-11. Opérations sur les ressources Microsoft Azure qui sont facultatives dans le rôle personnalisé lors de l'attribution d'autorisations au niveau de l'abonnement

Opération	
Microsoft.KeyVault/*/read Microsoft.KeyVault/vaults/* Microsoft.KeyVault/vaults/secrets/*	Des autorisations du coffre de clés sont requises pour le chiffrement du disque des VM de pool.
Microsoft.Network/natGateways/join/action	Cette autorisation est requise lorsque le type de connectivité **Azure Private Link** est sélectionné lors de la création d'Horizon Edge et qu'une passerelle NAT est associée au sous-réseau de gestion. L'autorisation est requise pour créer les ressources de point de terminaison privé.

Tableau 2-11. Opérations sur les ressources Microsoft Azure qui sont facultatives dans le rôle personnalisé lors de l'attribution d'autorisations au niveau de l'abonnement (suite)

Opération	
`Microsoft.Network/natGateways/read`	Cette autorisation est requise pour confirmer que la passerelle NAT du sous-réseau de gestion est, le cas échéant, correctement configurée, lorsque le type de cluster sortant est sélectionné comme passerelle NAT pour Horizon Edge.
`Microsoft.Network/privateEndpoints/write` `Microsoft.Network/privateEndpoints/read`	Des autorisations de point de terminaison privé sont requises pour déployer Horizon Edge avec Azure Private Link.
`Microsoft.Network/publicIPAddresses/*`	Une autorisation d'adresse IP publique est requise pour déployer une instance d'Horizon Edge avec des instances d'Unified Access Gateway derrière un équilibrage de charge avec une adresse IP publique. En outre, cette autorisation est requise. pour déployer et pour ajouter une adresse IP publique à une image.

Tableau 2-11. Opérations sur les ressources Microsoft Azure qui sont facultatives dans le rôle personnalisé lors de l'attribution d'autorisations au niveau de l'abonnement (suite)

Opération	
`Microsoft.Network/routeTables/join/action`	Cette autorisation est requise lorsque le type de connectivité **Azure Private Link** est sélectionné lors de la création d'Horizon Edge et qu'une table de routage est associée au sous-réseau de gestion. L'autorisation est requise pour créer les ressources de point de terminaison privé.
`Microsoft.Network/routeTables/read`	Cette autorisation est requise si le type de cluster sortant sélectionné pour Horizon Edge correspond aux routes définies par l'utilisateur. Il est nécessaire de valider la table de routage associée du sous-réseau de gestion pour s'assurer que la route par défaut est configurée correctement.

Note Lors de la suppression d'un pool joint à Microsoft Entra ID ou d'une VM, le principal de service doit disposer des autorisations de suppression de l'entrée de périphérique à partir de Microsoft Entra ID.

Les autorisations sont les suivantes :

Portée : `https://graph.microsoft.com/`

Autorisation : `Device.ReadWrite.All Read and write devices`

Consentement administrateur : `Yes`

L'autorisation peut être accordée en accédant à l'emplacement suivant :

Abonnement > Azure Active Directory > Enregistrements d'applications > Sélectionner l'application à laquelle l'autorisation doit être accordée > Autorisation d'API > Sélectionner Microsoft Graph > Sélectionner Device.ReadWriteAll

Exemple JSON de rôle personnalisé Microsoft Azure

Le bloc de code JSON suivant est un exemple permettant d'illustrer l'apparence éventuelle d'une définition de rôle personnalisé nommée `Rôle Horizon Cloud personnalisé - Titan` lorsqu'elle dispose de l'ensemble des opérations obligatoires et facultatives précédentes. L'ID est l'ID unique du rôle personnalisé. Lorsque vous utilisez Azure PowerShell ou Azure CLI pour créer un rôle personnalisé, le processus génère automatiquement cet ID. Pour la variable *my_subscription_ID*, remplacez les ID des abonnements dans lesquels le rôle personnalisé sera utilisé.

Dans la section `assignableScopes`, vous pouvez utiliser plusieurs ID d'abonnements « */subscriptions/my_subscription_ID* » pour permettre l'utilisation du rôle personnalisé dans plusieurs abonnements.

Tableau 2-12. Exemple de JSON pour un rôle autorisant les opérations requises d'Horizon Cloud lors de l'attribution d'autorisations au niveau de l'abonnement

```
{
    “id”: “uuid”,
    “properties”: {
        “roleName”: “Horizon Cloud Custom Role - Titan”,
        “description”: “All permissions required for deployment and operation of a Horizon
Edge in Azure”,
        “assignableScopes”: [
              “/subscriptions/my_subscription_ID”
        ],
        “permissions”: [
            {
                “actions”: [
                    “Microsoft.Authorization/*/read”,
                    “Microsoft.Compute/*/read”,
                    “Microsoft.Compute/availabilitySets/*“,
                    “Microsoft.Compute/disks/*“,
                    “Microsoft.Compute/galleries/read”,
                    “Microsoft.Compute/galleries/write”,
                    “Microsoft.Compute/galleries/delete”,
                    “Microsoft.Compute/galleries/images/*”,
                    “Microsoft.Compute/galleries/images/versions/*”,
                    “Microsoft.Compute/images/*”,
                    “Microsoft.Compute/locations/*”,
                    “Microsoft.Compute/snapshots/*”,
                    “Microsoft.ContainerService/managedClusters/delete”,
                    “Microsoft.ContainerService/managedClusters/read”,
                    “Microsoft.ContainerService/managedClusters/write”,
                    “Microsoft.ContainerService/managedClusters/commandResults/read”,
                    “Microsoft.ContainerService/managedClusters/runcommand/action”,
                    “Microsoft.ContainerService/managedClusters/upgradeProfiles/read”,
                    “Microsoft.ManagedIdentity/userAssignedIdentities/*/assign/action”,
                    “Microsoft.ManagedIdentity/userAssignedIdentities/*/read”,
                    “Microsoft.Compute/virtualMachines/*”,
                    “Microsoft.Compute/virtualMachineScaleSets/*”,
                    “Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/
agreements/read”,
                    “Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/
agreements/write”,
                    “Microsoft.Network/loadBalancers/*”,
                    “Microsoft.Network/networkInterfaces/*”,
                    “Microsoft.Network/networkSecurityGroups/*”,
                    “Microsoft.Network/virtualNetworks/read”,
                    “Microsoft.Network/virtualNetworks/write”,
                    “Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read”,
                    “Microsoft.Network/virtualNetworks/subnets/*”,
                    “Microsoft.Network/virtualNetworks/virtualNetworkPeerings/read”,
                    “Microsoft.ResourceGraph/*”,
                    “Microsoft.Resources/deployments/*”,
                    “Microsoft.Resources/subscriptions/read”,
                    “Microsoft.Resources/subscriptions/resourceGroups/*”,
                    “Microsoft.ResourceHealth/availabilityStatuses/read”,
                    “Microsoft.Storage/*/read”,
                    “Microsoft.Storage/storageAccounts/*”,
                    “Microsoft.KeyVault/*/read”,
                    “Microsoft.KeyVault/vaults/*”,
                    “Microsoft.KeyVault/vaults/secrets/*”,
                    “Microsoft.Network/natGateways/join/action”,
                    “Microsoft.Network/natGateways/read”,
                    “Microsoft.Network/privateEndpoints/write”,
                    “Microsoft.Network/privateEndpoints/read”,
                    “Microsoft.Network/publicIPAddresses/*”,
                    “Microsoft.Network/routeTables/join/action",
```

Tableau 2-12. Exemple de JSON pour un rôle autorisant les opérations requises d'Horizon Cloud lors de l'attribution d'autorisations au niveau de l'abonnement

```
                    "Microsoft.Network/routeTables/read"
                ],
                “notActions”: [],
                “dataActions”: [],
                “notDataActions”: []
            }
        ]
    }
}
```

Planification des cas d'utilisation et des scénarios courants dans Plan de contrôle Horizon et Horizon Cloud Service - next-gen

3

Lorsque vous vous préparez à intégrer des utilisateurs à Plan de contrôle Horizon et à Horizon Cloud Service - next-gen, tenez compte de la taille dont vous aurez besoin pour prendre en charge vos cas d'utilisation et scénarios prévus.

Lisez les sections suivantes :

- Dimensionnement de votre déploiement d'Horizon Cloud Service - next-gen

Dimensionnement de votre déploiement d'Horizon Cloud Service - next-gen

Après l'intégration à Horizon Cloud Service - next-gen, vous pouvez utiliser l'outil en ligne Valeurs maximales de configuration pour dimensionner votre déploiement en fonction du nombre de VM, d'utilisateurs, de principaux de service, etc., pris en charge par fournisseur et Passerelle Horizon Edge.

Les informations de l'outil Valeurs maximales de configuration pour Horizon Cloud Service - next-gen transmettent la signification de chacune des limites répertoriées. Cependant, les informations générales suivantes vous aident à expliquer l'incidence que ces limites peuvent avoir sur les performances de votre déploiement.

Appliquez les informations suivantes aux limites appropriées de configuration d'Horizon Cloud Service - next-gen dans l'outil Valeurs maximales de configuration.

- Incidence du nombre de principaux de service sur la durée de provisionnement

  Pour provisionner un poste de travail pendant les workflows de gestion du cycle de vie des machines virtuelles, Horizon Cloud Service - next-gen émet plusieurs appels d'API Microsoft Azure. La limitation des API Microsoft Azure se base sur le principal de service. Par conséquent, l'augmentation du nombre de principaux de service permet d'émettre simultanément davantage d'API. Cela améliore les performances des workflows de gestion du cycle de vie des machines virtuelles. Les exemples de workflows incluent la création et la suppression de pools, les opérations d'alimentation en bloc sur des machines virtuelles, etc.
- Incidence des partages de fichiers de distribution des App Volumes sur les délais de chargement des applications

Les applications App Volumes sont fournies aux postes de travail en montant les fichiers VHD présents dans les partages de fichiers de distribution. Plus le nombre de montages simultanés dans un partage de fichiers est élevé, plus l'exécution du provisionnement des applications prend de temps dans une session ou un poste de travail. L'augmentation du nombre de partages de fichiers de distribution améliore le processus de provisionnement des applications, ce qui entraîne une disponibilité plus rapide de ces dernières.

Intégration pour les administrateurs Horizon Cloud Service - next-gen

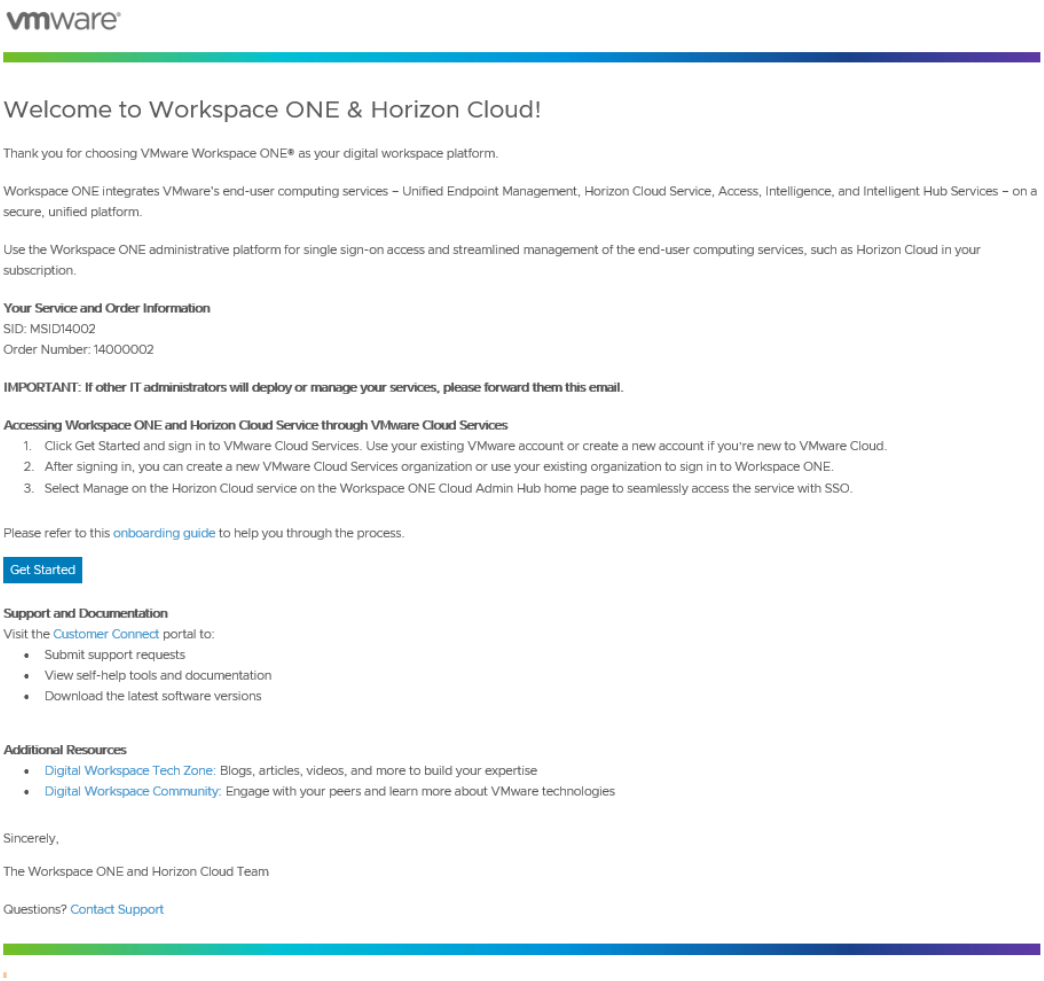
4

En tant qu'administrateur, examinez les informations suivantes pour commencer avec le processus d'intégration Horizon Cloud Service - next-gen et terminer celui-ci.

E-mail de bienvenue

VMware envoie un e-mail de bienvenue à votre compte d'administrateur pour confirmer l'évaluation ou l'achat de la licence du produit. L'e-mail confirme l'enregistrement et inclut un lien **Commencer** pour utiliser l'accès à Horizon Cloud Service - next-gen.

Note Les informations correspondantes sur la mise en route avec Workspace ONE peuvent être utiles à ce stade. Reportez-vous à la section Démarrage dans la documentation du produit Workspace ONE.



vmware

Welcome to Workspace ONE & Horizon Cloud!

Thank you for choosing VMware Workspace ONE® as your digital workspace platform.

Workspace ONE integrates VMware's end-user computing services – Unified Endpoint Management, Horizon Cloud Service, Access, Intelligence, and Intelligent Hub Services – on a secure, unified platform.

Use the Workspace ONE administrative platform for single sign-on access and streamlined management of the end-user computing services, such as Horizon Cloud in your subscription.

Your Service and Order Information
SID: MSID14002
Order Number: 14000002

IMPORTANT: If other IT administrators will deploy or manage your services, please forward them this email.

Accessing Workspace ONE and Horizon Cloud Service through VMware Cloud Services

1. Click Get Started and sign in to VMware Cloud Services. Use your existing VMware account or create a new account if you're new to VMware Cloud.
2. After signing in, you can create a new VMware Cloud Services organization or use your existing organization to sign in to Workspace ONE.
3. Select Manage on the Horizon Cloud service on the Workspace ONE Cloud Admin Hub home page to seamlessly access the service with SSO.

Please refer to this onboarding guide to help you through the process.

Get Started

Support and Documentation
Visit the Customer Connect portal to:

- Submit support requests
- View self-help tools and documentation
- Download the latest software versions

Additional Resources

- Digital Workspace Tech Zone: Blogs, articles, videos, and more to build your expertise
- Digital Workspace Community: Engage with your peers and learn more about VMware technologies

Sincerely,

The Workspace ONE and Horizon Cloud Team

Questions? Contact Support

Horizon Cloud Service - next-gen fait partie de la solution Anywhere Workspace globale.

Le service de licence Horizon Cloud dans Horizon Cloud Service - next-gen s'assure que les administrateurs informatiques peuvent accéder aux fonctionnalités par type de licence acheté et les exploiter.

Reportez-vous à la Matrice de comparaison des abonnements Horizon pour obtenir une comparaison des fonctionnalités de licence d'abonnement Horizon, qui classe globalement les licences sous la forme Durée et SaaS. Les fonctionnalités répertoriées ne s'appliquent pas toutes actuellement à Horizon Cloud Service - next-gen.

Note L'e-mail de bienvenue ne contient pas d'informations sur le type de licence acheté. Vous pouvez obtenir ces informations à partir de votre compte Customer Connect. Pour devenir un utilisateur de Customer Connect, reportez-vous à l'article 2007005 de la base de connaissances.

Une fois le processus d'intégration terminé, vous pouvez suivre vos licences Horizon à partir d'Horizon Universal Console. Reportez-vous à la section Utiliser Horizon Universal Console pour suivre vos licences Horizon.

Connectez-vous à Console Cloud Services

Note Pour plus d'informations sur la console Console Cloud Services, reportez-vous à la documentation du produit Cloud Services. Vous pouvez afficher d'autres noms pour VMware Cloud services, tels que *Cloud Services Platform (CSP)* et la *plate-forme d'engagement de Cloud Services*.

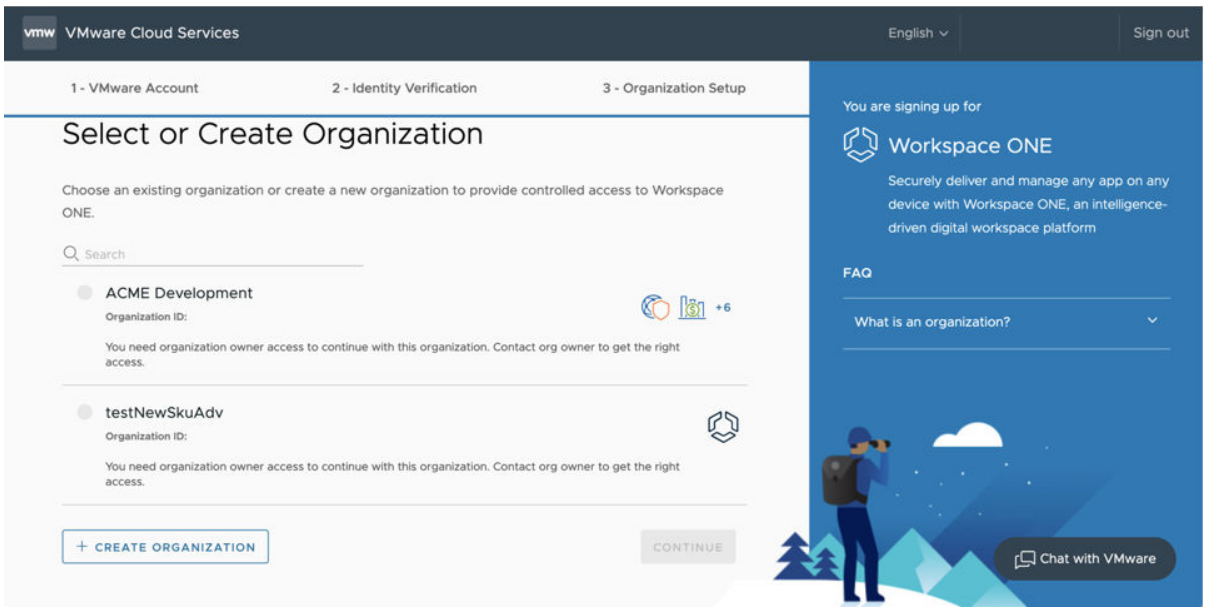
1 Créez un compte Console Cloud Services ou utilisez un compte existant.

Pour créer un compte, cliquez sur le lien dans l'e-mail de bienvenue, créez un compte VMware Cloud services et utilisez votre ID de VMware pour vous connecter à VMware Cloud services.

Note

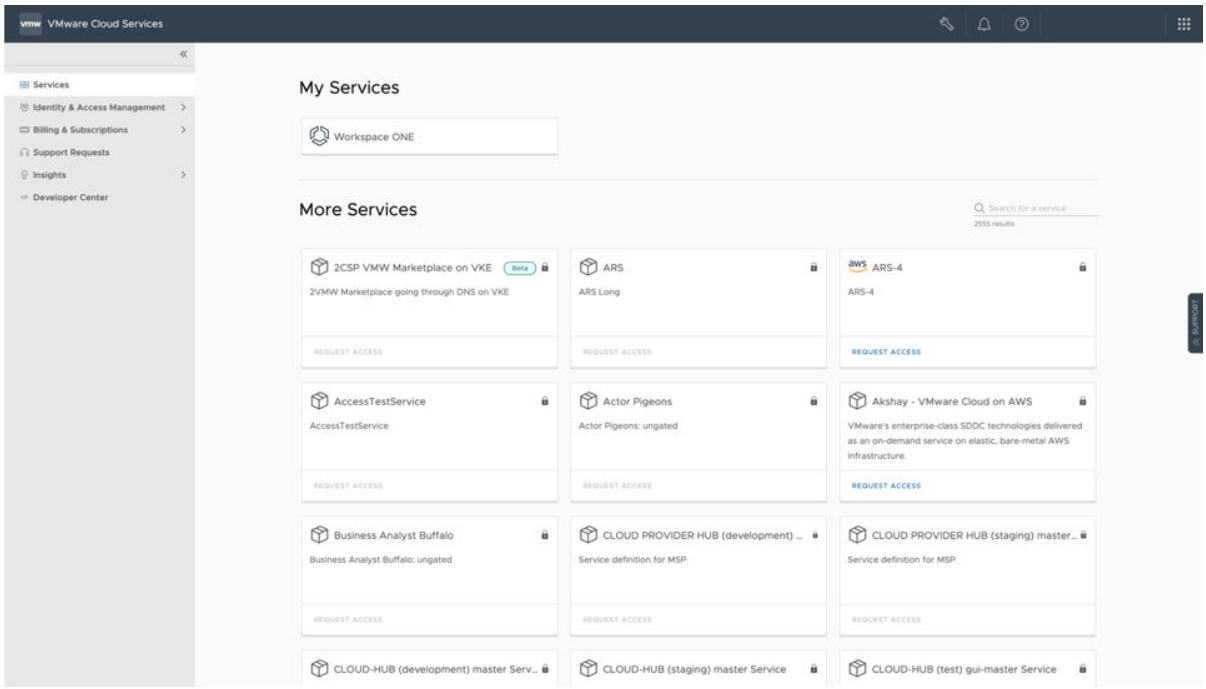
- Lorsque vous utilisez le lien de l'e-mail de bienvenue pour récupérer l'invitation, le rôle Administrateur vous est automatiquement attribué.
- Sélectionnez la même organisation CSP si vous l'utilisez également pour un autre produit fourni sur Cloud Services et que vous souhaitez que le même administrateur gère Horizon Cloud.
- Créez une organisation CSP si vous disposez d'une organisation CSP existante et que vous ne souhaitez pas que le même administrateur gère l'abonnement avec Horizon Cloud. Toutefois, si vous le faites, vous ne pourrez plus combiner ultérieurement les organisations CSP.
- Créez une organisation si vous disposez d'une organisation CSP existante dans laquelle vous gérez déjà Horizon Cloud et que vous ajoutez désormais un abonnement pour une nouvelle région géographique.

La console Console Cloud Services s'ouvre sur la page Configuration de l'organisation.



2 Entrez un nom d'organisation de votre choix et cliquez sur **Créer une organisation et terminer l'inscription**.

La page Console Cloud Services s'affiche en indiquant tous les services auxquels vous avez accès.



3 Cliquez sur votre nom dans le coin supérieur droit, puis sur **Afficher l'organisation**.

Revenez à la console Console Cloud Services dans laquelle vous pouvez désormais attribuer les rôles requis.

À propos de l'ajout d'autres utilisateurs et de l'attribution de rôles

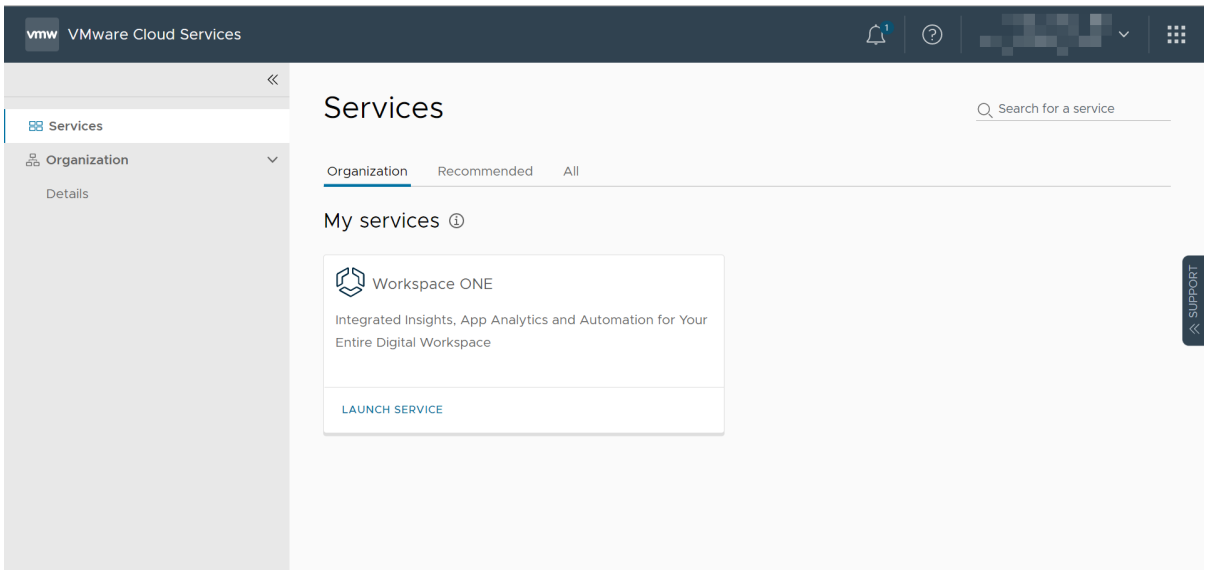
Lorsque vous utilisez le lien de l'e-mail de bienvenue pour récupérer l'invitation, le rôle Administrateur vous est automatiquement attribué. Le rôle Administrateur vous octroie des autorisations complètes pour l'interface utilisateur et les API d'Horizon Universal Console que vous devez intégrer. Vous pouvez fournir à d'autres utilisateurs administratifs des droits d'accès à Horizon Universal Console. Pour plus d'informations, reportez-vous à la section Attribution de rôles administratifs aux utilisateurs Horizon Universal Console.

Utiliser la console Console Cloud Services pour lancer Workspace ONE

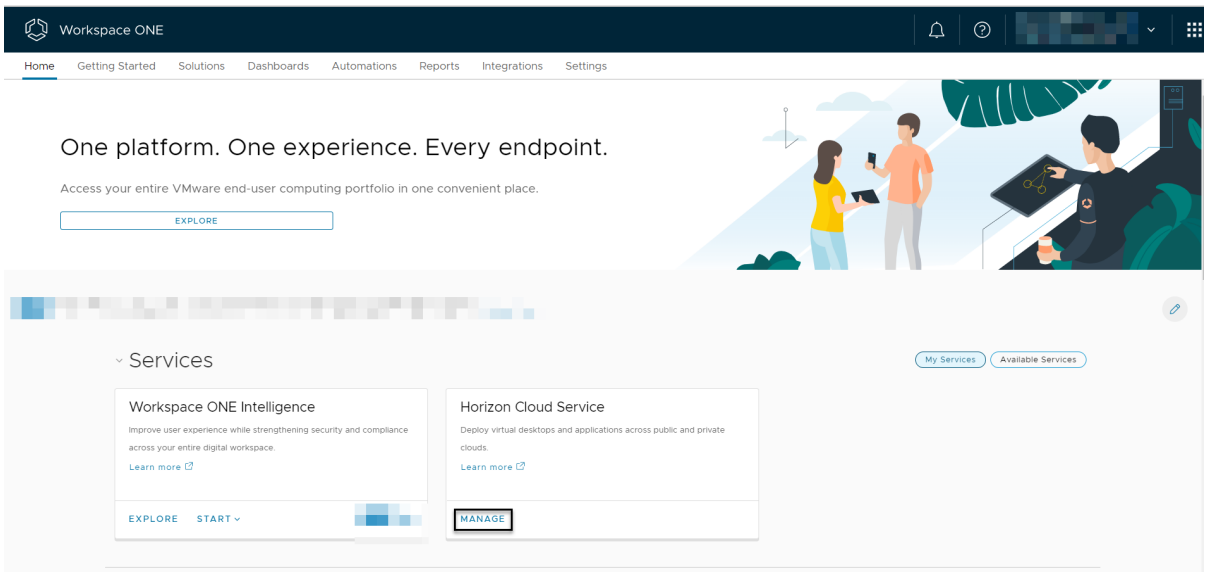
Pour lancer Horizon Cloud, procédez comme suit.

1 Dans le volet de gauche, cliquez sur **Services**.

2 Cliquez sur **Lancer le service** pour Workspace ONE.

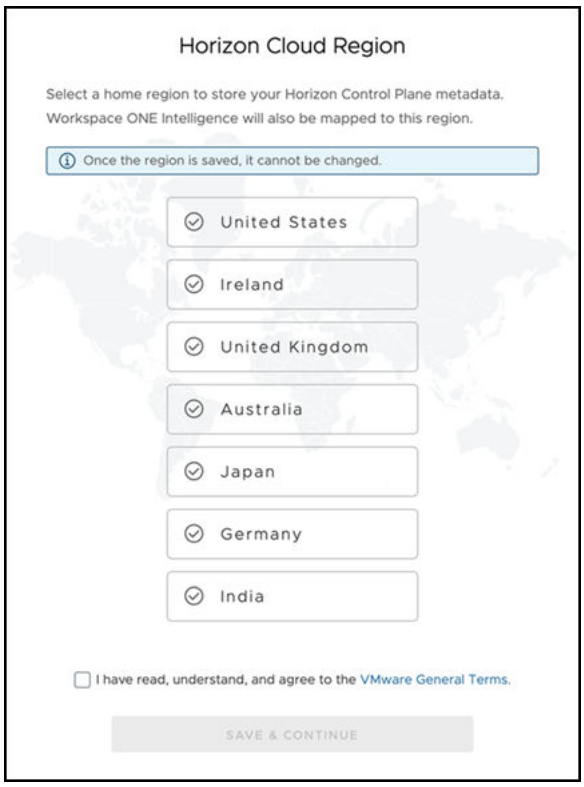


3 Cliquez sur **Gérer** sur la vignette **Horizon Cloud Service** pour lancer Horizon Universal Console.



Utiliser Horizon Universal Console pour sélectionner votre région Horizon Cloud

Après avoir lancé la console, vous êtes invité à sélectionner votre région. Pour respecter les principes d'intégrité des données, vous devez sélectionner la région dans laquelle résident vos ressources et leurs métadonnées. Une fois que vous avez sélectionné la région, vous ne pouvez plus la modifier.



1 Sélectionnez votre région Horizon Cloud.

2 Cochez la case pour accepter les conditions d'utilisation.

3 Cliquez sur **Enregistrer et continuer**.

Bienvenue à Horizon Universal Console pour Horizon Cloud Service - next-gen

Lorsque la console affiche l'écran d'accueil, suivez les instructions à l'écran et effectuez la sélection à l'écran pour le premier déploiement de votre locataire.

Note À ce stade, Horizon Universal Console peut afficher une bannière en haut de l'écran indiquant que la synchronisation de la licence est en cours. Dans ce cas, la console n'affiche pas toutes les fonctionnalités activées par votre licence spécifique tant que la synchronisation n'est pas terminée et que vous n'avez pas actualisé votre navigateur. Une fois la synchronisation terminée, Horizon Universal Console affiche les éléments appropriés à votre licence.

Pour obtenir la documentation qui prend en charge les instructions à l'écran en fonction de votre type de déploiement, reportez-vous aux éléments suivants.

- Démarrage et déploiement d'Horizon Plus.
- Déploiements de Microsoft Azure, Horizon Edge - Préparation au déploiement
- Déploiements d'Horizon 8, Horizon Edge - Préparation au déploiement
- Configuration des déploiements fédérés d'Horizon 8 avec Horizon Cloud Service - next-gen

Configuration et déploiement du Plan de contrôle Horizon et d'Horizon Cloud Service - next-gen

5

Utilisez les listes de vérification de configuration et configurez vos paramètres de réseau, de capacité et d'intégration lorsque vous vous préparez à créer et déployer des dispositifs Edge dans Plan de contrôle Horizon et Horizon Cloud Service - next-gen.

Lisez les sections suivantes :

- Configuration des informations du fournisseur d'identité et d'accès pour les déploiements de dispositifs Edge
- Déploiement d'Horizon Edge dans votre fournisseur de capacité de ressources
- Configuration des intégrations

Configuration des informations du fournisseur d'identité et d'accès pour les déploiements de dispositifs Edge

Dans Horizon Cloud Service - next-gen, configurez votre domaine Active Directory et votre fournisseur d'identité (IdP) dans le cadre du processus de configuration et de déploiement des dispositifs Edge.

En plus de remplir les listes de vérification des conditions requises Chapitre 2 Démarrage avec les déploiements du plan de contrôle Horizon, de Microsoft Azure et d'Horizon 8, configurez votre domaine Active Directory et votre fournisseur d'identité. Pour obtenir un complément d'informations, reportez-vous aux rubriques suivantes :

- Configuration de votre domaine Active Directory
- Configuration de votre fournisseur d'identité
- Connexion de votre fournisseur d'identité

Une fois que vous avez terminé ces configurations de domaine et de fournisseur d'identité qui s'appliquent à votre cas d'utilisation de déploiement prévu, déployez le dispositif Horizon Edge approprié en suivant les étapes décrites dans Déploiement d'Horizon Edge dans votre fournisseur de capacité de ressources.

Déploiement d'Horizon Edge dans votre fournisseur de capacité de ressources

Une fois que vous avez connecté votre fournisseur d'identité, vous pouvez déployer une infrastructure du Cloud légère de type thin-edge sur le fournisseur, le site et le réseau.

Déploiements des dispositifs Horizon 8 Edge

Pour intégrer Horizon Cloud Service - next-gen, vous devez configurer votre Horizon Edge avec Horizon Connection Server, comme décrit dans les sections suivantes et utiliser l'e-mail de bienvenue Horizon Cloud Service - next-gen envoyé au compte d'administrateur.

Pour plus d'informations sur l'utilisation de l'e-mail de bienvenue Horizon Cloud Service - next-gen, reportez-vous à la section Chapitre 4 Intégration pour les administrateurs Horizon Cloud Service - next-gen.

Pour configurer le domaine Active Directory et le fournisseur d'identité, reportez-vous à la section Configuration des informations du fournisseur d'identité et d'accès pour les déploiements de dispositifs Edge.

Déployer un dispositif Horizon Edge à utiliser avec les déploiements d'Horizon 8 et le plan de contrôle Horizon Cloud Service - next-gen

Cette page décrit les étapes de workflow **Ajouter un dispositif Horizon Edge** d'Horizon Universal Console pour le cas d'utilisation dans lequel vous créez un dispositif Horizon Edge qui utilise un espace Horizon 8 comme fournisseur de ressources et que cet espace se trouve dans un environnement vSphere (déploiement sur site ou intégré à SDDC). Vous pouvez également configurer différents types de capacités pour un déploiement fédéré sur la plate-forme de virtualisation souhaitée. Un seul espace Horizon Connection Server est pris en charge sur un dispositif Horizon Edge.

Le déploiement d'un dispositif Horizon Edge implique le déploiement d'un dispositif Passerelle Horizon Edge dans une infrastructure vSphere, le couplage de ce dispositif avec le Plan de contrôle Horizon et la configuration des détails de l'instance d'Horizon Connection Server de l'espace Horizon 8 pour votre dispositif Horizon Edge.

Important Lorsque vous déployez un dispositif Passerelle Horizon Edge dans une infrastructure vSphere, utilisez vSphere Client ou vSphere Web Client. Ne déployez pas le dispositif directement sur un hôte ESXi.

Ce processus de bout en bout comporte plusieurs étapes.

1 Démarrez ce processus à l'aide de la console Horizon Universal Console. Sur la page **Démarrage**, sélectionnez **Horizon 8** pour accéder à la page **Déployer et Configure**. Pour connecter Horizon 8 à Horizon Universal Console, déployez votre premier dispositif Horizon Edge et connectez votre fournisseur d'identité pour activer la fonctionnalité de fiche utilisateur, de recherche d'utilisateurs et de support technique d'Horizon 8. Si vous choisissez de ne pas connecter votre fournisseur d'identité, le champ **Rechercher un utilisateur** dans la console sera désactivé.

2 Déployez un dispositif OVA dans votre environnement vSphere. Vous devez utiliser les informations de code de couplage que le système crée dans la première partie du processus dans les champs de l'interface utilisateur Déployer le modèle OVF lorsque vous déployez le fichier OVA.

   Note Un déploiement d'OVA/OVF d'Passerelle Horizon Edge est uniquement disponible pour les fournisseurs Horizon 8 disposant d'une architecture intégrée à SDDC ou d'un type de capacité de centre de données privé. Pour les fournisseurs Horizon 8 disposant d'une architecture fédérée, reportez-vous à la procédure correspondant à votre type de capacité spécifique décrite dans la section Configuration des déploiements fédérés d'Horizon 8 avec Horizon Cloud Service - next-gen.

3 Revenez à Horizon Universal Console pour vérifier que l'état du couplage est réussi et effectuez les étapes restantes dans cette console pour ajouter les détails de l'espace Horizon 8.

Note Le terme *espace Horizon 8* fait référence à un espace exécutant une version du logiciel Horizon Connection Server qui est l'une des versions compatibles avec Horizon Cloud Service - next-gen. Par exemple, si la version 7.13 d'Horizon 7 est l'une des versions prises en charge, l'expression s'applique également à un espace exécutant cette version. Pour en savoir plus sur l'interopérabilité des versions d'Horizon et d'Horizon Cloud Service - next-gen, reportez-vous à la Matrice d'interopérabilité des produits VMware. Un seul dispositif Horizon 8 est pris en charge par Horizon Edge.

Le dispositif Horizon Edge est une infrastructure du Cloud légère de type thin-edge. Pour les déploiements d'Horizon 8, l'espace Horizon 8 est le fournisseur de capacités du dispositif Horizon Edge.

Une fois que votre environnement est configuré avec au moins un domaine Active Directory et un fournisseur d'identité, la console rend ce workflow **Ajouter un dispositif Horizon Edge** disponible.

Conditions préalables

- Examinez les conditions requises de la section Liste de vérification des conditions requises pour le déploiement d'un dispositif Horizon 8 Edge et respectez-les.

- Examinez les éléments préparatoires décrits sur les pages liées de la page Déploiements des dispositifs Horizon 8 Edge et effectuez-les.
- Déterminez le nom de domaine complet (FQDN) que vous utiliserez pour le dispositif Passerelle Horizon Edge déployé. L'assistant d'interface utilisateur vous demande d'entrer ce nom de domaine complet.
- Si l'instance d'Horizon Connection Server impliquée dans ce dispositif Horizon Edge dispose d'un certificat auto-signé, assurez-vous que vous connaissez l'empreinte digitale du certificat pour l'étape de vérification de l'assistant.
- Les connexions TLS sortantes de la Passerelle Horizon Edge à Horizon Cloud Service - next-gen peuvent échouer si le certificat par défaut rendu par Horizon Cloud Service - next-gen est remplacé par un certificat personnalisé à l'aide d'un proxy ou d'autres moyens. Le remplacement du certificat par défaut par un certificat personnalisé n'est pas pris en charge.
- **Note** Un déploiement d'OVA/OVF d'Passerelle Horizon Edge est uniquement disponible pour les fournisseurs Horizon 8 disposant d'une architecture intégrée à SDDC ou d'un type de capacité de centre de données privé. Pour les fournisseurs Horizon 8 disposant d'une architecture fédérée, reportez-vous à la procédure correspondant à votre type de capacité spécifique décrite dans la section Configuration des déploiements fédérés d'Horizon 8 avec Horizon Cloud Service - next-gen.
- Regardez les TechZone videos suivantes avant d'effectuer les étapes de cette procédure :
  - Déploiement du dispositif Passerelle Horizon Edge - Configuration DNS sur https://via.vmw.com/tchzmno5209
  - Déploiement du dispositif Passerelle Horizon Edge - Vérificateur d'URL sur https://via.vmw.com/tchzmno5210
  - Déploiement du dispositif Passerelle Horizon Edge - Configuration du fournisseur et du dispositif sur https://via.vmw.com/tchzmno5211
  - Déploiement d'Passerelle Horizon Edge à partir d'OVA sur https://via.vmw.com/tchzmno5212

Procédure

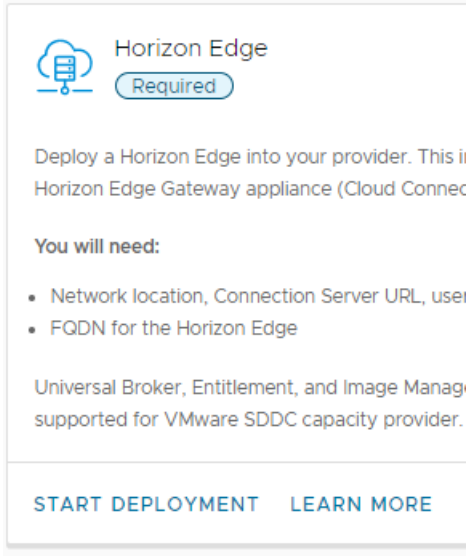
1 Démarrez l'assistant **Ajouter un dispositif Horizon Edge** de la console.

La console rend l'assistant **Ajouter un dispositif Horizon Edge** disponible à partir de différents points d'entrée. Votre point de départ dans la console pour cette étape varie généralement selon que votre environnement est vierge ou qu'il dispose de déploiements existants du dispositif Horizon Edge pour Horizon 8 ou pour Microsoft Azure.

Aucun dispositif Horizon Edge pour le moment : démarrez à partir de la carte Horizon Edge de la console

Si votre environnement ne dispose d'aucun dispositif Dispositifs Horizon Edge, vous pouvez démarrer généralement l'assistant en cliquant sur **DÉMARRER LE DÉPLOIEMENT**.

La capture d'écran suivante illustre cette carte **Horizon Edge**.



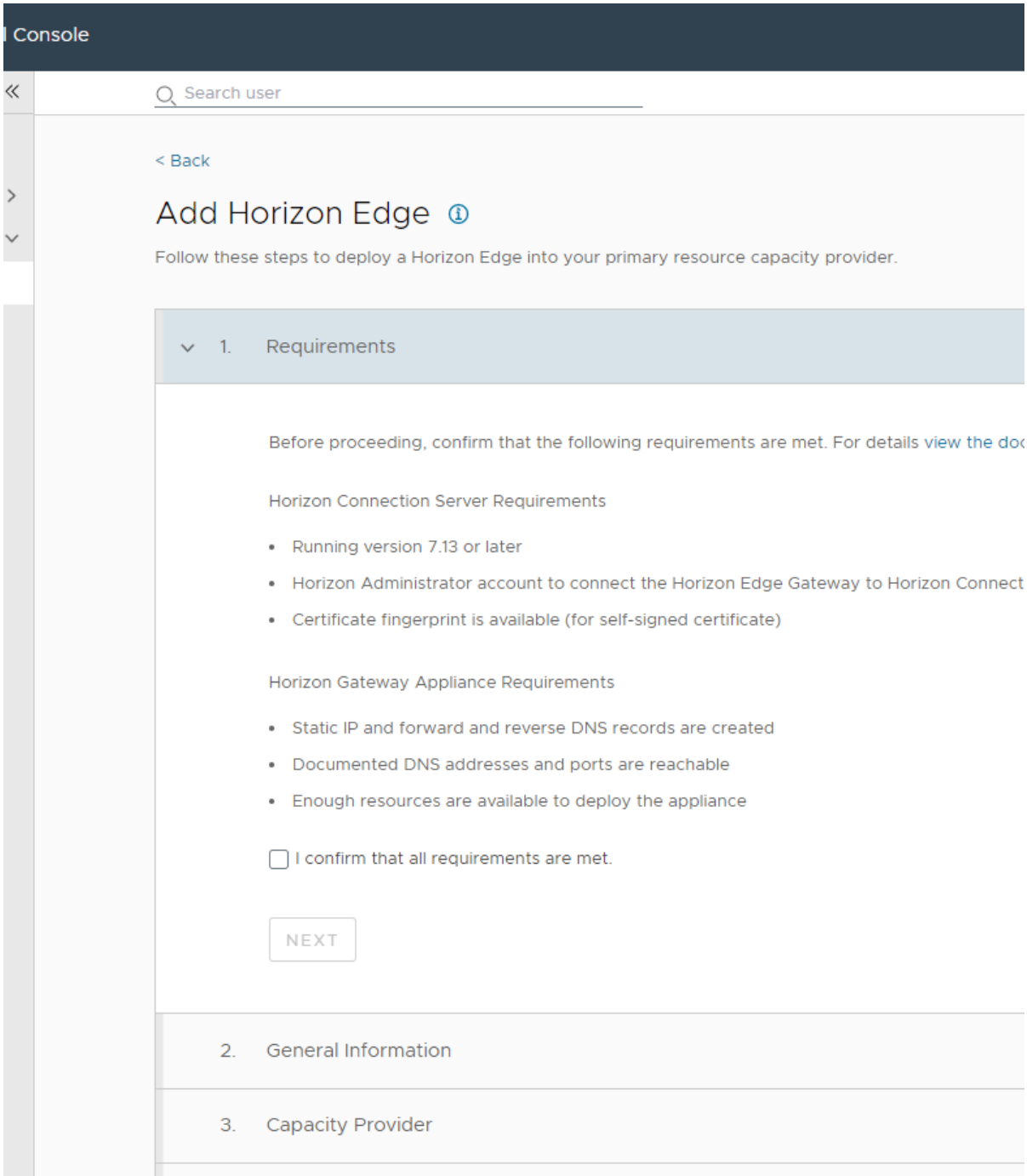
Aucun dispositif Horizon Edge : vous pouvez également démarrer à partir de la page Capacité de la console

Si aucun dispositif Dispositifs Horizon Edge n'est encore déployé dans l'environnement, la page **Capacité** contient du texte et un menu **Démarrer**. Dans ce scénario, vous pouvez démarrer l'assistant en accédant à **Ressources > Capacité** et en cliquant sur **Démarrer > Horizon 8**.

Au moins un dispositif Horizon Edge : démarrez à partir de la page Capacité de la console

Si au moins un dispositif Horizon Edge est déployé pour le moment dans l'environnement, la page **Capacité** contient une grille qui répertorie les dispositifs Dispositifs Horizon Edge existants. Dans ce scénario, vous pouvez démarrer l'assistant en accédant à **Ressources > Capacité** et en cliquant sur **Ajouter > Horizon 8**.

Après avoir utilisé l'une de ces trois méthodes pour démarrer l'assistant, la console affiche **Ajouter un dispositif Horizon Edge** à l'étape 1 de l'assistant.



Suivez les instructions à l'écran pour terminer chaque étape de l'assistant.

2 Ajoutez un **Nom du dispositif Horizon Edge** unique et une description facultative.

3 Dans la section **Fournisseur de capacités** de la page, sélectionnez le **Type de capacité** dans lequel votre passerelle Passerelle Horizon Edge sera déployée et entrez un emplacement pour ce dispositif Horizon Edge. Les types de capacités suivants sont disponibles :

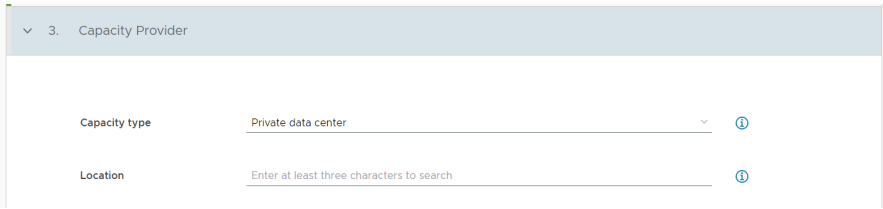
Remarque : à titre de référence, la valeur qui suit le symbole de tiret – ci-dessous représente la valeur utilisée dans Horizon Connection Server.

- Centre de données privé – Général
- Microsoft Azure – Solution Azure VMware (AVS)
- Amazon Web Services – VMware Cloud on AWS (VMC)
- Google Cloud – Google Cloud VMware Engine (GCVE)
- Oracle Cloud – Oracle Cloud VMware Solution (OCVS)
- Alibaba Cloud – Alibaba Cloud VMware Solution (ACVS)
- Cloud Dell EMC

Si le type de capacité sélectionné prend en charge la fédération, vous pouvez également être invité à spécifier un type d'architecture. En fonction du type de capacité que vous sélectionnez, l'une des trois options est par la suite disponible pour spécifier un type d'architecture.

- Le type de capacité est un centre de données privé.

  Si le type de capacité est un centre de données privé, aucun paramètre de type d'architecture ne s'affiche, comme indiqué dans la capture d'écran suivante.

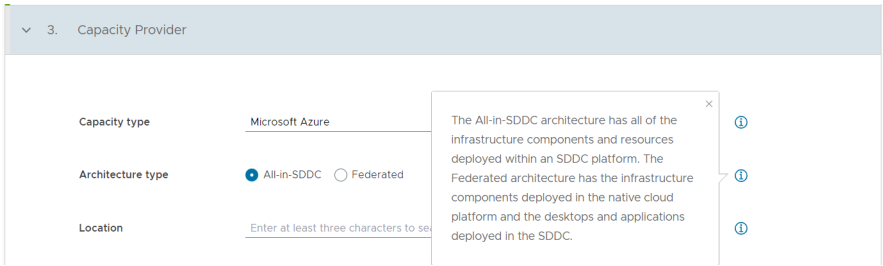


- Le type de capacité ne prend pas en charge l'architecture fédérée.

  Si le type de capacité ne prend pas en charge l'architecture fédérée, le paramètre de type d'architecture est affiché avec une valeur par défaut et non sélectionnable **Intégrée à SDDC**, comme indiqué dans la capture d'écran suivante.

- Le type de capacité prend en charge l'architecture fédérée.

Si le type de capacité prend en charge l'architecture fédérée, le paramètre type d'architecture s'affiche avec une option sélectionnable **Fédérée** ou **Intégrée à SDDC**, comme indiqué dans la capture d'écran suivante.



Sélectionnez ensuite le type de dispositif approprié. Les types de dispositifs disponibles affichés varient selon que vous sélectionnez l'option d'architecture **Fédérée** ou **Intégrée à SDDC**.

Si vous sélectionnez **Fédérée** comme type d'architecture, et en fonction du type de capacité que vous spécifiez, différents fichiers de dispositif Edge sont disponibles dans la section **Télécharger le dispositif de passerelle Horizon Edge** de la page.

Pour obtenir des informations connexes sur la spécification des dispositifs Dispositifs Horizon Edge pour la fédération, reportez-vous à la section Configuration des déploiements fédérés d'Horizon 8 avec Horizon Cloud Service - next-gen.

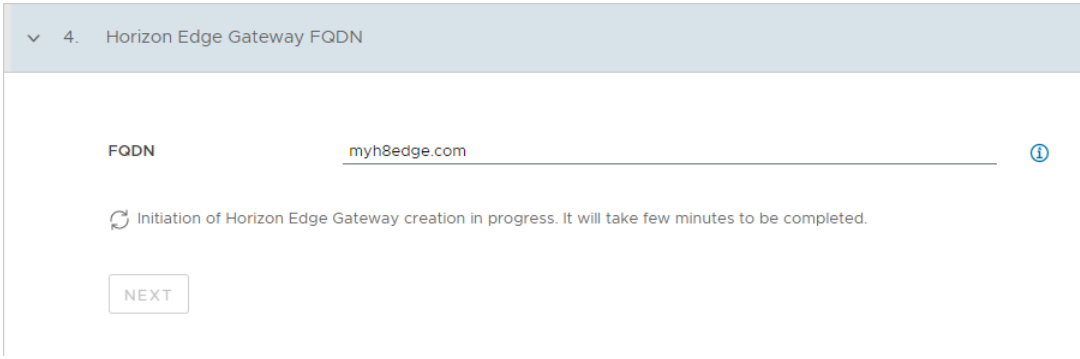
4 Spécifiez un emplacement pour ce déploiement à l'aide de l'option **Emplacement**, généralement l'emplacement géographique le plus proche de l'emplacement du fournisseur de capacités.

5 Dans la section **Nom de domaine complet de la passerelle Horizon Edge** de la page, pour la valeur **Nom de domaine complet de la passerelle Horizon Edge**, entrez le nom de domaine complet à utiliser pour le dispositif Passerelle Horizon Edge.

Important Dès que vous disposez de l'adresse IP du dispositif lorsqu'il est déployé dans votre environnement vSphere, vous devez inscrire un enregistrement DNS dans votre serveur DNS pour mapper l'adresse IP à ce **Nom de domaine complet de la passerelle Horizon Edge** que vous entrez ici. Pour obtenir une illustration de ce qu'il faut faire, consultez la Tech Zone video Déployer la passerelle Edge - Configuration DNS.

Pour les dispositifs Horizon 8 Edge configurés avec l'architecture fédérée, vous ne pouvez pas configurer par défaut les plages CIDR pour les clusters Kubernetes dans le dispositif Horizon 8 Edge. Pour reconfigurer et redémarrer le cluster k8s pour vos configurations CIDR souhaitées, contactez le support client.

Lorsque vous entrez le nom de domaine complet, le système commence à enregistrer les informations que vous avez entrées dans l'assistant jusqu'à ce stade. Le système inscrit un enregistrement Horizon Edge dans les enregistrements du système.



Important Même si un message à l'écran s'affiche et laisse supposer que le dispositif Horizon Edge est créé, il fait référence à la création de l'enregistrement système pour ce dispositif Horizon Edge. Le déploiement de bout en bout est toujours incomplet tant que vous n'avez pas téléchargé le fichier binaire du dispositif Passerelle Horizon Edge. Utilisez ce fichier binaire pour déployer le dispositif Passerelle Horizon Edge dans votre environnement vSphere, effectuez le couplage de ce dispositif avec le plan de contrôle du cloud et spécifiez les détails d'Horizon Connection Server.

6 Si vous disposez d'une licence universelle Horizon, vous pouvez utiliser l'option pour activer ou désactiver **Surveillance de l'agent**. Si vous choisissez de désactiver **Surveillance de l'agent**, cochez la case pour accepter les risques associés. Si vous disposez d'une licence Horizon Plus, vous ne pouvez pas désactiver **Surveillance de l'agent**. Cliquez sur **Suivant**.

Note Cela s'applique uniquement au type de dispositif Edge View et non à Azure. Cette action désactive également la surveillance de l'agent uniquement. Les données de surveillance de CS et toutes les autres données continueront d'être envoyées à WS1.

La surveillance de l'agent permet aux instances d'Horizon Agent d'envoyer des données, telles que des informations sur l'utilisation de VM et sur les erreurs à Workspace ONE Intelligent Hub. Il est recommandé de garder cette option activée pour votre dispositif Edge.

La désactivation des données de surveillance de l'agent aura une incidence sur les fonctionnalités et le fonctionnement de Horizon Cloud Service - next-gen et n'est donc pas recommandée.

7 Utilisez l'option **Télécharger** pour obtenir le fichier binaire du dispositif Passerelle Horizon Edge.

Enregistrez le fichier binaire téléchargé à un emplacement à partir duquel vous allez le déployer dans la plate-forme de virtualisation souhaitée. Pour plus d'informations sur le déploiement de vos dispositifs Edge fédérés, reportez-vous à la section Configuration des déploiements fédérés d'Horizon 8 avec Horizon Cloud Service - next-gen.

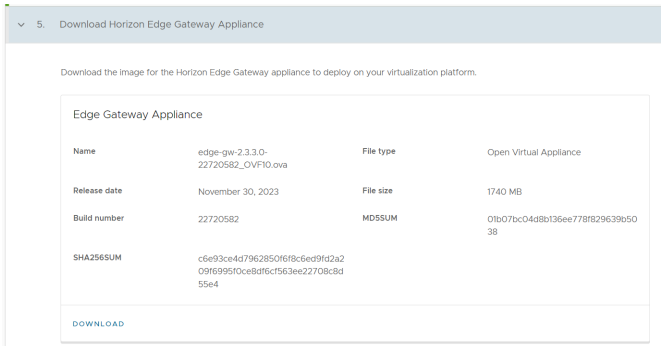
Note La taille binaire est d'environ 1,7 Go.

Comme indiqué dans la Tech Zone video, si vous déployez la Passerelle Horizon Edge dans vSphere, vous pouvez également cliquer avec le bouton droit sur le bouton, copier l'URL et utiliser cette dernière dans le champ **URL** de l'interface utilisateur **Déployer le modèle OVF de vCenter**. Pour plus d'informations sur l'utilisation de cette méthode d'URL, consultez la vidéo Déploiement du dispositif Horizon Edge à partir du fichier OVA.

Si vous déployez le dispositif Passerelle Horizon Edge en mode fédéré, reportez-vous à la section Configuration des déploiements fédérés d'Horizon 8 avec Horizon Cloud Service - next-gen relative à votre type de capacité spécifié.

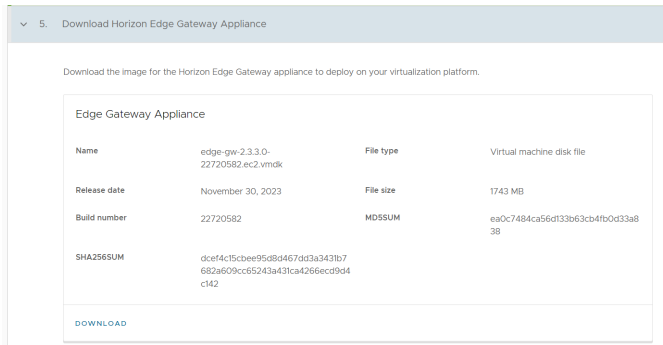
Des exemples d'images pour l'étape de téléchargement sont présentés ci-dessous, en fonction du type de capacité sélectionné et de l'architecture fédérée.

- Un exemple d'image pour l'architecture intégrée à SDDC avec n'importe quelle sélection de type de capacité est présenté ci-dessous :

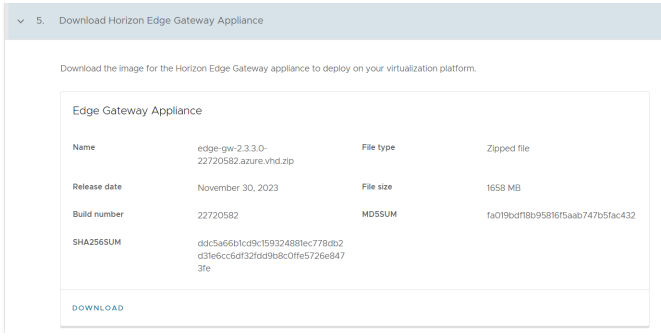


  La build est également la même pour le centre de données privé.

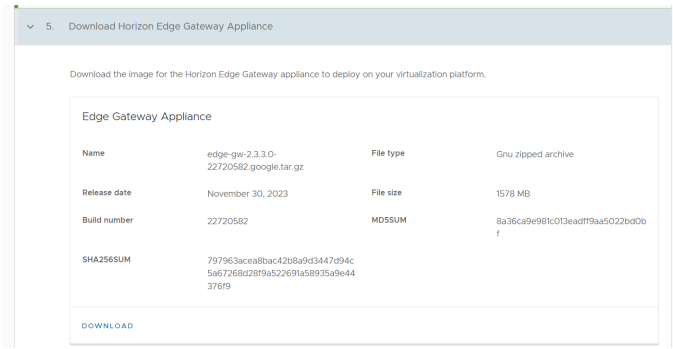
- Un exemple d'image pour le type de capacité d'AWS avec une architecture fédérée est présenté ci-dessous :



- Un exemple d'image pour le type de capacité de Microsoft Azure avec une architecture fédérée est présenté ci-dessous :



- Un exemple d'image pour le type de capacité de Google avec une architecture fédérée est présenté ci-dessous :



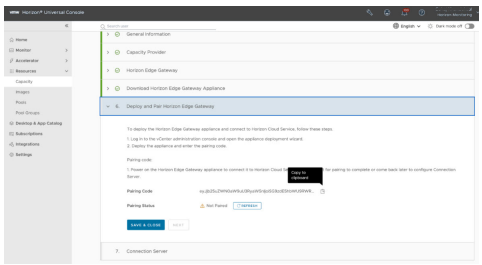
8 Une fois que vous avez obtenu le fichier binaire ou l'URL à utiliser dans l'interface utilisateur **Déployer le modèle OVF**, cliquez sur **Suivant**.

9 Si vous y êtes invité, copiez le code de couplage généré par le système et enregistrez-le dans un emplacement dans lequel vous pouvez le copier et le coller lorsque vous en aurez besoin lors du déploiement du dispositif avec l'interface utilisateur **Déployer le modèle OVF**.

Attention Le code de couplage est important pour la réussite du processus de bout en bout. Vous devez utiliser ce code de couplage dans l'interface utilisateur **Déployer le modèle OVF** lorsque vous déployez le dispositif. L'interface utilisateur **Déployer le modèle OVF** utilise une étiquette différente pour ce code (**Chaîne de connexion** dans l'interface utilisateur **Déployer le modèle OVF**).

Utilisez l'icône de copie fournie, car la console n'affiche pas la chaîne de code de couplage complète. La chaîne de code est plus longue que les éléments affichés par la console. Par conséquent, vous n'obtiendrez pas la chaîne de code complète en mettant uniquement le texte affiché en surbrillance et en le copiant.

L'image suivante montre comment copier le code de couplage à l'aide de l'interface utilisateur.



10 Cette étape s'applique uniquement si vous effectuez un déploiement dans un environnement vSphere, en fonction de votre sélection d'architecture intégrée à SDDC. Si vous utilisez plutôt une architecture fédérée pour le déploiement, reportez-vous à la section Configuration des déploiements fédérés d'Horizon 8 avec Horizon Cloud Service - next-gen relative à votre type de capacité spécifié, puis revenez à l'étape suivante de ce processus.

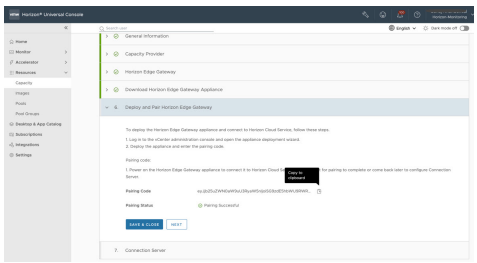
Lisez les instructions à l'écran sur le déploiement du dispositif dans votre environnement vSphere, puis suivez les étapes dans cet environnement pour déployer le dispositif à l'aide de l'interface utilisateur **Déployer le modèle OVF**. Laissez cet assistant **Ajouter un dispositif Horizon Edge** ouvert dans votre navigateur lors de l'exécution de ces étapes, car vous reviendrez à cet assistant pour vérifier si le couplage a réussi.

Pour obtenir l'illustration pas à pas du déploiement du dispositif Passerelle Horizon Edge en utilisant l'interface utilisateur **Déployer le modèle OVF**, reportez-vous à la Tech Zone video Déployer le dispositif Horizon Edge à partir d'OVA.

Attention Dans l'étape **Personnaliser le modèle** de l'interface utilisateur **Déployer le modèle OVF**, dans le champ **Code de couplage**, vous devez entrer la chaîne **Code de couplage** que vous avez copiée à l'étape précédente, à partir de l'assistant *Ajouter un dispositif Horizon Edge*.

La saisie du code de couplage correct dans le champ **Code de couplage** est requise pour réussir le déploiement du dispositif Passerelle Horizon Edge.

L'image suivante illustre l'emplacement du champ **Code de couplage** dans lequel vous voulez coller la chaîne **Code de couplage** que vous avez copiée à partir de l'assistant **Ajouter un dispositif Horizon Edge** d'Horizon Universal Console.



L'étape **Prêt à terminer** de l'interface utilisateur de l'outil OVF affiche les propriétés que vous avez entrées à l'étape **Personnaliser le modèle**.

Vérifiez que la chaîne complète de code de couplage que vous avez copiée à partir d'Horizon Universal Console est représentée dans cet ensemble de propriétés.

Note **Réseau d'espace** et **Réseau de service** sont des valeurs internes utilisées par le cluster Kubernetes interne du dispositif. Conservez ces valeurs par défaut.

11 Une fois le fichier OVF déployé, mettez le dispositif sous tension.

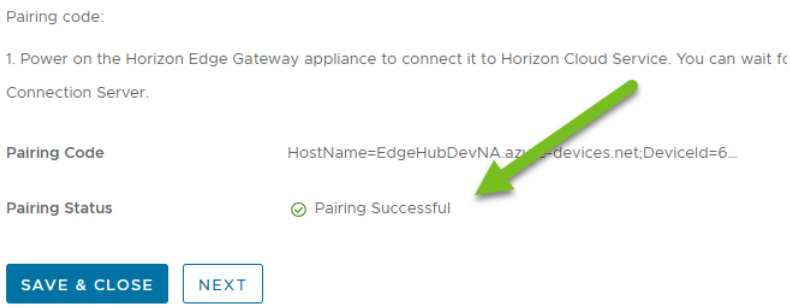
Lorsque le dispositif est sous tension et en cours d'exécution, revenez à l'assistant **Ajouter un dispositif Horizon Edge** dans Horizon Universal Console et cliquez sur **Actualiser** pour **État du couplage**.

Note Le système peut mettre quelques minutes à communiquer l'état du dispositif déployé au plan de contrôle du cloud.

Si vous avez entré le code de couplage copié correct dans l'interface utilisateur de déploiement du fichier OVA, mis sous tension le dispositif, rempli les conditions requises d'enregistrement DNS et toutes les conditions préalables indiquées en haut de cette page de documentation, le système doit représenter un couplage réussi. Lors de l'actualisation, l'**État du couplage** affiché passe à **Couplage réussi**.

Si le couplage du dispositif Edge échoue, reportez-vous à l'article de la base de connaissances Dépannage des problèmes de connectivité d'un dispositif Horizon 8 Edge pour plus d'informations sur l'exécution d'un outil de diagnostic et le dépannage des problèmes liés à l'absence du dispositif Edge dans un état **Couplage réussi**.

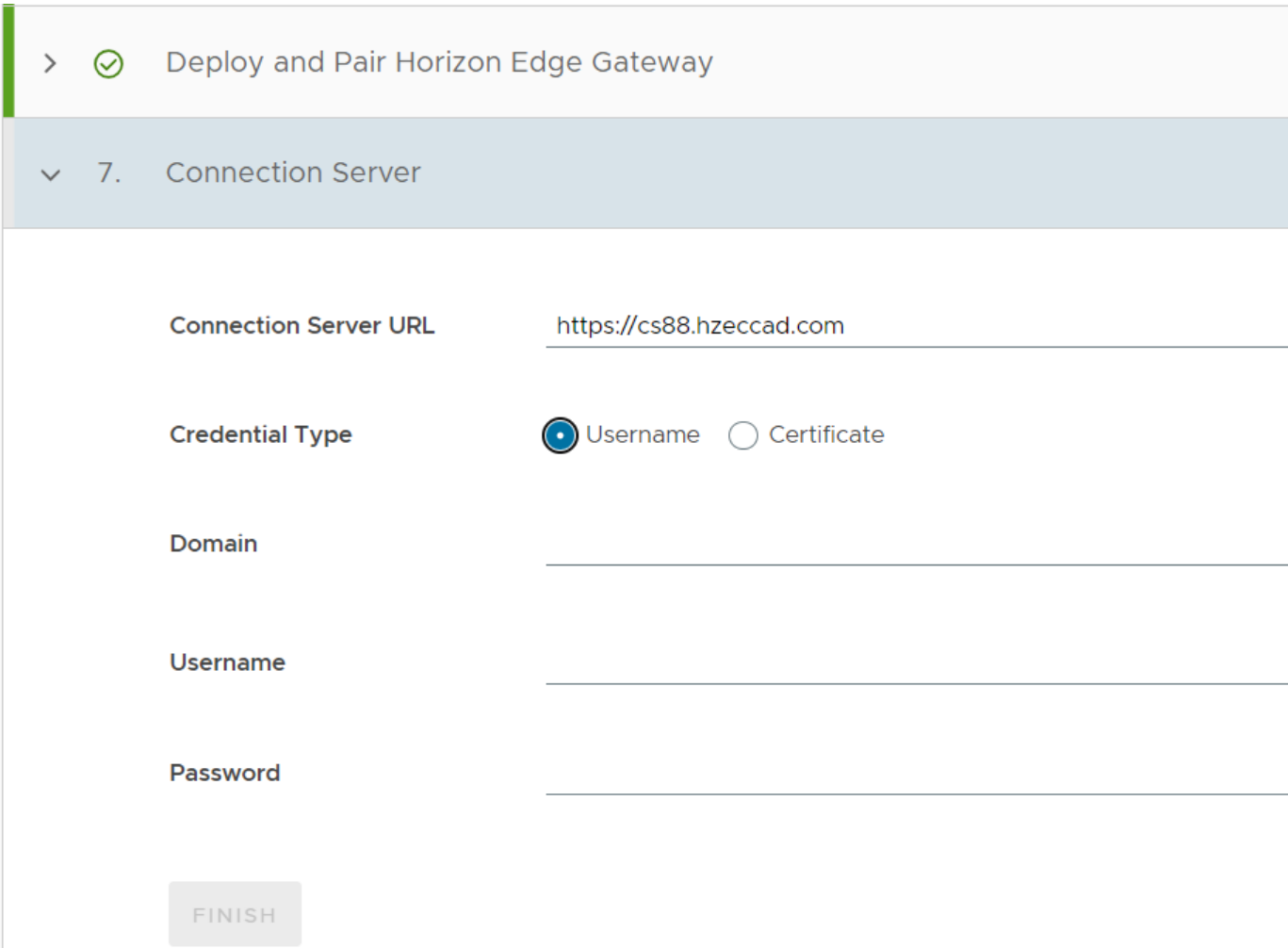
La capture d'écran suivante illustre un couplage réussi.



12 Cliquez sur **Suivant** pour passer à la saisie des informations d'Horizon Connection Server.

13 Remplissez les champs des informations d'Horizon Connection Server et cliquez sur **Terminer**.

La page vous invite à indiquer l'**URL du Serveur de connexion** et le **Type d'informations d'identification** pour l'authentification.



- Dans la valeur **Domaine** du dispositif Horizon 8 Edge , spécifiez le nom **Domaine** de DNS de l'emplacement du compte d'utilisateur. N'utilisez pas le nom NetBIOS.
- Si vous sélectionnez le type d'informations d'identification **Nom d'utilisateur**, entrez les champs **Domaine**, **Nom d'utilisateur** et **Mot de passe** du compte Horizon 8 à utiliser pour vous connecter à Horizon Connection Server.

  Note Le nom de domaine complet de l'équilibrage de charge n'est pas pris en charge pour l'URL du Serveur de connexion. Fournissez le nom de domaine complet d'un Serveur de connexion individuel uniquement. Le couplage d'un dispositif Passerelle Horizon Edge avec un nom de domaine complet d'équilibrage de charge n'est pas pris en charge.

  Le tableau ci-dessous décrit les rôles pris en charge pour ce compte et les capacités de cloud disponibles en fonction des rôles attribués au compte. Pour plus d'informations sur ces rôles, reportez-vous à la version de produit appropriée dans la rubrique Rôles d'administrateur prédéfinis de la documentation d'Horizon.

Rôles	Fonctionnalités d'Horizon Cloud
Administrateur	Autorise toutes les fonctionnalités d'Horizon Cloud Service.
Horizon Cloud Service	Permet l'application et la gestion des licences d'abonnement.

- Si vous sélectionnez le type d'informations d'identification **Certificat**, chargez le certificat au format PKCS12 ou PFX et entrez le mot de passe si le certificat est protégé par mot de passe.

  Note Pour utiliser cette méthode d'authentification, vous devez activer l'authentification par certificat sur Horizon Connection Server. Pour plus d'informations, reportez-vous à la section *Paramètres globaux liés à la sécurité pour Horizon Console* de la publication *Sécurité d'Horizon* dans la documentation du produit Horizon.

14 Cliquez sur **Terminer**.

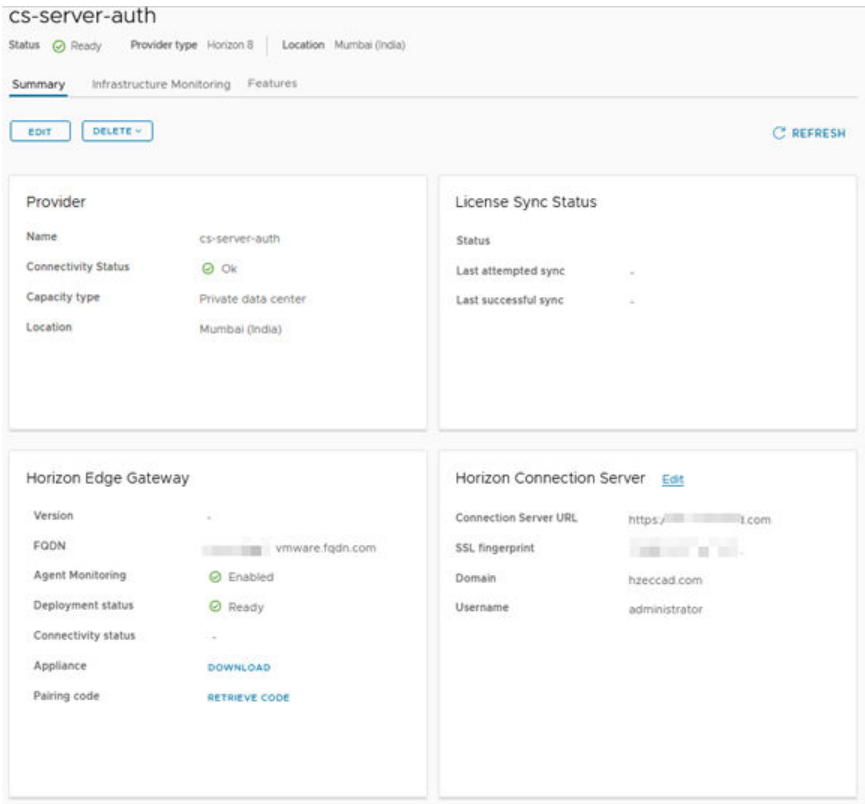
Si le système détecte qu'Horizon Connection Server dispose d'un certificat auto-signé, une zone s'affiche et vous demande de confirmer les détails du certificat. Si l'URL d'entrée d'Horizon Connection Server ne correspond à aucun des noms d'hôtes du certificat sur le Serveur de connexion, un message s'affiche pour le confirmer. Vérifiez-les et confirmez-les selon votre situation.

Résultats

En cas de réussite, la console ferme l'interface utilisateur de l'assistant et affiche la page de détails de ce dispositif Horizon Edge récemment ajouté.

Note En fonction du trafic réseau, le système peut prendre une minute pour terminer la mise à jour des indicateurs de l'état de la connectivité sur la page de détails.

L'image suivante illustre un exemple de page de détails avec un espace Horizon 8 connecté en tant que fournisseur de capacités.



Étape suivante

- Assurez-vous que vous avez inscrit un enregistrement DNS dans votre serveur DNS pour mapper l'adresse IP du dispositif déployé au **nom de domaine complet de la passerelle Horizon Edge** que vous entrez dans l'assistant. Pour obtenir une illustration de ce qu'il faut faire, consultez la Tech Zone video Déployer la passerelle Edge - Configuration DNS.

  Note L'utilisation d'alias DNS pour au moins deux instances d'Horizon Connection Server n'est pas prise en charge. Cela entraîne des problèmes d'authentification du dispositif Passerelle Horizon Edge.

- Pour éviter l'interruption de service en raison de l'expiration des informations d'identification du certificat d'Horizon Connection Server pour vos dispositifs Horizon 8 Edge, recherchez les notifications concernant l'expiration prochaine du certificat Horizon Connection Server pour les dispositifs Horizon 8 Edge et agissez sur celles-ci. Horizon Cloud Service - next-gen affiche ce type de notification dans Horizon Universal Console et, si vous êtes un administrateur enregistré auprès des VMware Cloud Services, également appelés VMware Cloud Services Platform (CSP), le système vous envoie également ces informations par e-mail.

  Lorsque vous recevez ces notifications, vous devez renouveler ou mettre à jour le certificat avant expiration. Si vous ne renouvelez pas le certificat avant l'expiration, vous rencontrerez des interruptions d'accès des utilisateurs finaux et d'opérations administratives.

Accès au plan de contrôle Horizon Cloud Service - next-gen

Le plan de contrôle Horizon Cloud Service - next-gen prend en charge les types de déploiements suivants.

- Microsoft Azure
- Horizon 8 déployé à l'aide du modèle intégré à SDDC pour utiliser le service de gestion des licences
- Déploiements d'Horizon Plus

Lorsque vous disposez d'Horizon Universal Subscription, vos cas d'utilisation impliquent uniquement des espaces Horizon 8 et que vous souhaitez que ces déploiements utilisent des services SaaS Horizon supplémentaires, tels que des attributions Horizon Image Management Service (IMS), Universal Broker et multicloud, remplissez le questionnaire Demande d'exception Horizon Cloud suivant et envoyez-le.

Configurer la tolérance aux pannes pour un dispositif Horizon 8 Edge

La procédure suivante décrit comment configurer la tolérance aux pannes pour un dispositif Horizon Edge qui utilise un espace Horizon 8 comme fournisseur de ressources, dans lequel cet espace se trouve dans un environnement VMware vSphere (déploiement sur site ou intégré à SDDC).

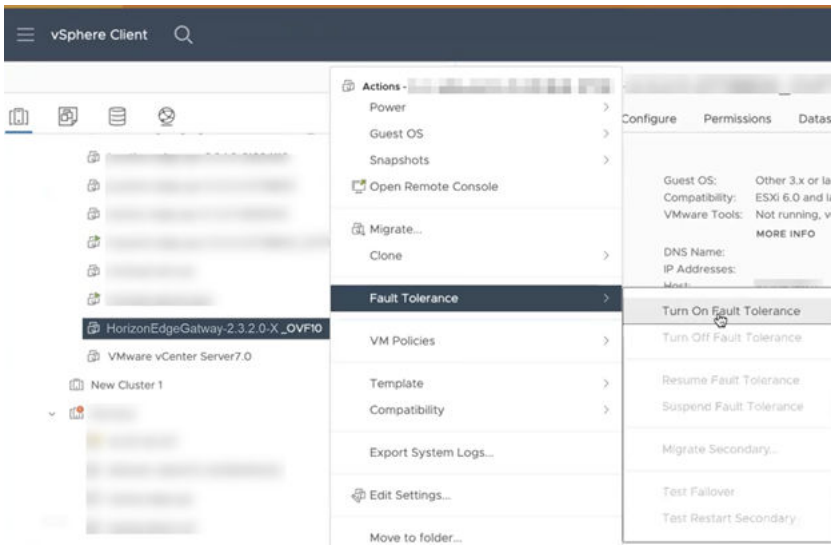
Cette procédure nécessite l'utilisation de vSphere Client pour configurer la tolérance aux pannes sur le dispositif Passerelle Horizon Edge dans l'infrastructure VMware vSphere.

Conditions préalables

- Utilisez un système 10 Gigabit Ethernet (10GbE) comme transport WAN.
- Déployez un dispositif Horizon Edge. Reportez-vous à la section Déployer un dispositif Horizon Edge à utiliser avec les déploiements d'Horizon 8 et le plan de contrôle Horizon Cloud Service - next-gen.

Procédure

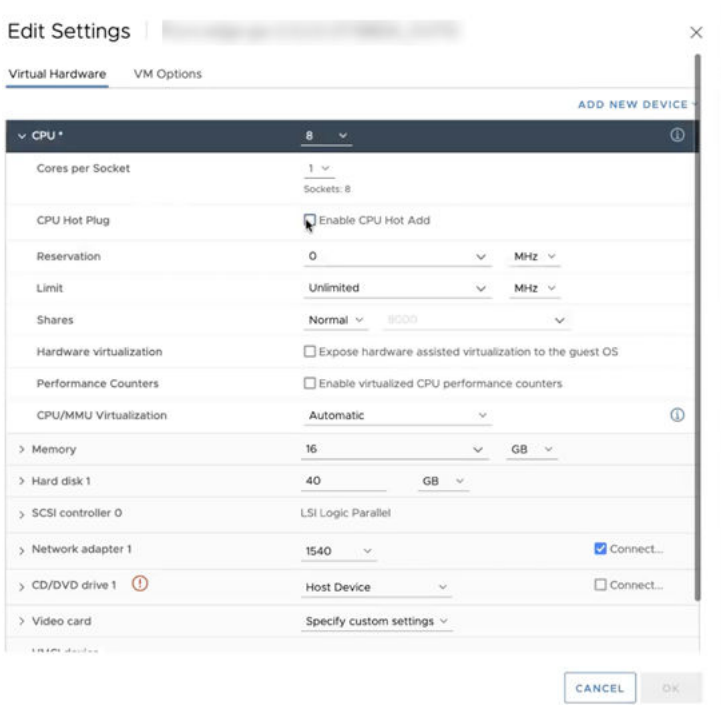
1 À l'aide de vSphere Client, accédez à la VM du dispositif Passerelle Horizon Edge et sélectionnez **Tolérance aux pannes > Activer la tolérance aux pannes**.



a Si une erreur s'affiche concernant l'enfichage à chaud du CPU non pris en charge pour la VM, désactivez cette dernière et, dans la boîte de dialogue Modifier les paramètres, sélectionnez l'onglet **Matériel virtuel** pour modifier la configuration de la VM comme suit.

1 Désactivez l'enfichage à chaud du CPU.

Développez le nœud CPU et, dans la section Enfichage à chaud du CPU, décochez la case **Activer l'ajout à chaud du CPU** pour le désactiver.



2 Désactivez l'enfichage à chaud de la mémoire.

Développez le nœud Mémoire et, dans la section Enfichage à chaud de la mémoire, décochez la case **Activer**.

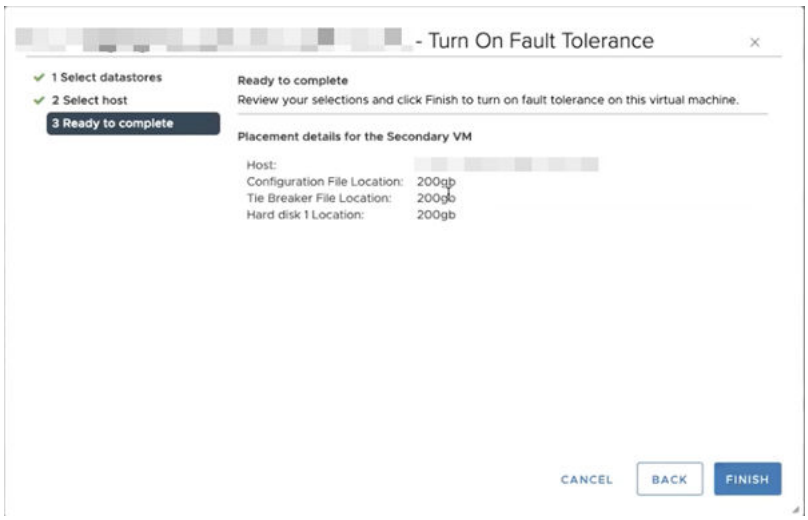
3 Sélectionnez le périphérique hôte pour le lecteur CD/DVD 1.

Dans la section Lecteur CD/DVD 1, sélectionnez **Périphérique hôte** dans le menu déroulant.

4 Cliquez sur **OK**.

2 Pour activer la tolérance aux pannes de la VM, sélectionnez la banque de données secondaire, cliquez sur **Suivant**, sélectionnez l'hôte secondaire, cliquez sur **Suivant**, vérifiez vos sélections, puis cliquez sur **Terminer**.

Attention Sélectionnez une banque de données différente de celle que vous avez sélectionnée lors du déploiement de la VM. La sélection de la même banque de données entraîne une erreur.



La tolérance aux pannes a été activée pour la VM Horizon Edge.

3 Utilisez vSphere Client pour vérifier que la tolérance aux pannes s'applique aux hôtes du cluster.

   a Dans le volet de gauche, sélectionnez l'hôte sur lequel vous avez déployé la VM principale et, dans le volet de droite avec l'option **Machines virtuelles** sélectionnée, vérifiez que la VM Edge Horizon 8 s'affiche comme VM principale.

   Le nom inclut « principal » entre parenthèses. Par exemple, le nom peut s'afficher sous la forme « Exemple-2.3.2.0-XXX_OVF10 (principal) ».

   b Dans le volet de gauche, sélectionnez l'hôte sur lequel vous avez déployé la VM secondaire et, dans le volet de droite avec l'option **Machines virtuelles** sélectionnée, vérifiez que la VM Edge Horizon 8 s'affiche comme VM secondaire.

   Le nom est le même que celui de la VM principale, sauf que le mot « secondaire » est entre parenthèses. Par exemple, « Exemple-2.3.2.0-XXX_OVF10 (secondaire) ».

4 Mettez sous tension la VM, activez-la via SSH et attendez que tous les espaces s'activent et que tous les services démarrent.

   Pour plus d'informations sur l'activation de SSH, reportez-vous à la section Activer l'accès SSH pour Horizon Edge .

Résultats

Avec la tolérance aux pannes correctement configurée, la VM secondaire prend le relais si l'hôte principal n'est plus disponible. Par conséquent, sans interruption de service, le basculement se produit et tous les services continuent de s'exécuter sans problème.

Si l'hôte qui contient la VM principale échoue naturellement ou si vous forcez l'échec dans un environnement de test, le comportement suivant s'applique.

- Lorsque vous sélectionnez l'hôte sur lequel vous avez déployé la VM principale, la VM Edge Horizon 8 s'affiche désormais comme VM secondaire. Le nom inclut « déconnecté » et « secondaire » entre parenthèses. Selon les exemples utilisés précédemment dans cette procédure, le nom s'affiche sous la forme « Exemple-2.3.2.0-XXX_OVF10 (déconnecté, secondaire) »
- Lorsque vous sélectionnez l'hôte sur lequel vous avez déployé la VM secondaire, la VM Edge Horizon 8 s'affiche désormais comme VM principale. Le nom inclut « principal » entre parenthèses. En fonction des exemples utilisés précédemment dans cette procédure, le nom s'affiche sous la forme « Exemple-2.3.2.0-XXX_OVF10 (principal) »

Activer l'accès SSH pour Horizon Edge

Vous pouvez activer SSH pour que l'utilisateur racine se connecte à un dispositif Horizon Edge.

Procédure

1 Une fois le dispositif Horizon Edge opérationnel, lancez la console Web vCenter pour la VM Edge.

2 Connectez-vous en tant qu'utilisateur racine et entrez le mot de passe.

3 Exécutez la commande **`/opt/vmware/bin/configure-adapter.py --sshEnable`** et attendez qu'elle se termine.

4 Saisissez **`vi /etc/ssh/sshd_config`**.

5 Remplacez la ligne **`PermitRootLogin <other-value>`** par **`PermitRootLogin yes`**.

6 Enregistrez les modifications dans l'éditeur vim.

7 Redémarrez le démon sshd en exécutant la commande **`systemctl restart sshd`**

8 Vous pouvez vous connecter via SSH au dispositif Edge à l'aide de **`ssh root@<edge-appliance-ip>`**

Configuration des déploiements fédérés d'Horizon 8 avec Horizon Cloud Service - next-gen

À l'aide d'Horizon Cloud Service - next-gen, vous pouvez télécharger et déployer la passerelle Passerelle Horizon Edge afin de configurer Dispositifs Horizon Edge pour le déploiement de cloud fédéré dans des environnements Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).

L'architecture de déploiement fédérée d'Horizon 8 est conçue pour fournir une solution évolutive lors de l'utilisation d'Horizon 8 dans des environnements de fournisseurs de cloud public. Reportez-vous aux trois rubriques suivantes pour obtenir plus d'informations sur la configuration des espaces Horizon 8 et de la passerelle Horizon Edge lors de l'utilisation de l'architecture de déploiement fédérée dans ces environnements cloud pris en charge.

Pour plus d'informations sur la spécification d'une architecture fédérée lors de l'ajout ou de la modification d'une valeur de type de capacité Horizon Edge, reportez-vous aux informations sur les paramètres de **Fournisseur de capacités** dans Déployer un dispositif Horizon Edge à utiliser avec les déploiements d'Horizon 8 et le plan de contrôle Horizon Cloud Service - next-gen.

Espaces Horizon 8 : architecture fédérée avec VMware Cloud on AWS : télécharger et déployer la passerelle Horizon Edge dans votre environnement d'Horizon Cloud Service - next-gen

Vous pouvez télécharger et déployer la passerelle Passerelle Horizon Edge dans votre déploiement fédéré d'Horizon 8 dans Amazon Web Services (AWS) à coupler avec Horizon Cloud Service - next-gen.

Conditions préalables

Suivez ces étapes pour télécharger et déployer le dispositif Passerelle Horizon Edge pour un déploiement de l'espace qui utilise l'architecture fédérée avec VMware Cloud on AWS. Dans l'architecture fédérée, vous devez déployer Passerelle Horizon Edge dans l'infrastructure Amazon Elastic Computer Cloud (EC2) native dans l'environnement de votre espace d'Horizon Cloud Service - next-gen.

- Vérifiez que vous avez respecté les conditions préalables liées à la Passerelle Horizon Edge décrites dans la section Déploiements des dispositifs Horizon 8 Edge.

- Vérifiez que vous avez respecté les conditions préalables répertoriées dans la section Rendre les URL de destination appropriées accessibles pour déployer une passerelle Passerelle Horizon Edge dans un environnement Horizon 8 pour utiliser la passerelle Passerelle Horizon Edge pour coupler un espace Horizon 8 avec Horizon Cloud Service.
- Le dispositif virtuel Passerelle Horizon Edge doit accéder à Internet pour communiquer avec le plan de contrôle Horizon Cloud. Si votre environnement nécessite l'utilisation d'une configuration de serveur proxy et de proxy pour que les dispositifs déployés accèdent à Internet, veillez à vérifier les informations liées au proxy, les limitations connues et les problèmes connus lors de l'utilisation des paramètres de proxy avec le dispositif Passerelle Horizon Edge.
- Si vous prévoyez d'utiliser un proxy lors de l'exécution d'un script pair-edge, vous devez d'abord exécuter la commande suivante, en indiquant *true* lorsque ProxySSL est activé et sinon en indiquant *false* :

  ```
  /opt/vmware/bin/pair-edge-with-proxy.sh -i 'IP_or FQDN_of Proxy' -o 'Proxy_Port' -u
  'Proxy_User_Name' -p 'Proxy_Password' -s 'true_or_false' -c 'Connection_String'
  ```

  Reportez-vous aux informations liées au proxy dans la Remarque suivante.

  Note **Mettre à jour la configuration du proxy dans Edge**

  ```
  /opt/vmware/bin/configure-edge-webproxy.py --proxyHost 127.0.0.1 --proxyPort 3128 --
  proxyUsername 'exampleUsername' --proxyPassword 'examplePassword'
  ```

  Pour explorer plus d'options, exécutez le script avec l'option `-h`, comme indiqué ci-dessous.

  ```
  /opt/vmware/bin/configure-edge-webproxy.py -h
  ```

- Vous devez utiliser la ligne de commande pour la plupart des étapes. Cependant, vous pouvez effectuer certaines étapes de déploiement à l'aide de la console de gestion AWS ou de l'interface de ligne de commande (CLI) AWS. Pour obtenir des informations détaillées sur l'utilisation d'un environnement Amazon EC2, reportez-vous à la documentation d'Amazon Elastic Compute Cloud à l'adresse https://docs.aws.amazon.com/ec2/index.html. Les étapes qui suivent suggèrent souvent le type spécifique de documentation d'Amazon Elastic Compute Cloud à référencer.

Procédure

1 Téléchargez l'image disque Passerelle Horizon Edge à l'aide de *Étape 7. Utilisez l'option Télécharger pour obtenir le fichier binaire du dispositif de passerelle Horizon Edge.Instruction* de la procédure à la page Déployer un dispositif Horizon Edge à utiliser avec les déploiements d'Horizon 8 et le plan de contrôle Horizon Cloud Service - next-gen. Répondez à toutes les invites à l'écran.

L'image disque Passerelle Horizon Edge est disponible sous la forme d'un fichier VMDK. Téléchargez le fichier VMDK sur votre système local.

Note Téléchargez la version 2.3.3.0 ou ultérieure de l'image disque Passerelle Horizon Edge, par exemple `edge-gw-2.3.3.0-22720582.ec2.vmdk`.

Enregistrez le fichier binaire téléchargé dans un emplacement à partir duquel vous le déploierez sur la plate-forme de virtualisation souhaitée, puis revenez à cette séquence d'étapes pour poursuivre le processus de couplage requis.

Avant de télécharger le fichier image de disque dans votre environnement Amazon EC2, vous devez d'abord créer un compartiment Amazon S3.

2 Créez un compartiment Amazon S3 dans votre environnement Amazon EC2. Pour obtenir des instructions détaillées, reportez-vous à la documentation d'Amazon Elastic Compute Cloud.

3 Chargez le fichier VMDK téléchargé dans votre compartiment Amazon S3. Vous pouvez effectuer cette étape à l'aide de la console de gestion AWS ou de l'interface de ligne de commande (CLI) d'AWS.

- (Console de gestion AWS) Connectez-vous à la console de gestion AWS pour votre environnement Amazon EC2. Accédez au service S3, sélectionnez le compartiment que vous avez créé précédemment et chargez le fichier VMDK dans ce compartiment.
- (CLI AWS) Accédez à l'interface de ligne de commande (CLI) et exécutez la commande suivante.

```
aws s3 cp <file-path-to-VMDK-file> <S3URI>
```

Pour plus d'informations sur l'exécution de la commande `cp`, reportez-vous à la documentation d'Amazon Elastic Compute Cloud.

Dans la console de gestion AWS, le fichier VMDK est répertorié dans l'onglet **Objets**.

4 Créez un rôle de service et une stratégie, puis associez la stratégie au rôle.

a Créez le premier des trois nouveaux fichiers JSON requis pour cette procédure.

L'objectif de ce fichier JSON particulier est de stocker les informations de rôle de service. Nommez le fichier comme vous le souhaitez. Dans cette procédure, l'exemple de nom pour ce fichier est `trust-policy.json`.

Le texte suivant est un exemple du contenu du fichier JSON.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"",
            "Effect":"Allow",
            "Principal":{
                "Service":"vmie.amazonaws.com"
            },
            "Action":"sts:AssumeRole",
            "Condition":{
                "StringEquals":{
                    "sts:ExternalId":"vmimport"
                }
            }
        }
    ]
}
```

b Créez un rôle de service avec un nom de votre choix et stockez les informations sur le rôle dans le nouveau fichier JSON.

Par exemple, à l'aide de l'interface de ligne de commande (CLI), exécutez la commande suivante.

Il s'agit d'un exemple générique.

```
aws iam create-role --role-name <role-name> --assume-role-policy-document <file-path>
```

L'exemple de commande suivant remplace l'espace réservé *<role-name>* par l'exemple `vmimport` spécifique et l'espace réservé *<file-path>* par l'exemple `trust-policy.json` spécifique.

```
aws iam create-role --role-name vmimport --assume-role-policy-document file://trust-
policy.json
```

Pour plus d'informations sur l'exécution de la commande `create-role`, reportez-vous à la documentation d'Amazon Elastic Compute Cloud.

c Créez le deuxième des trois nouveaux fichiers JSON requis pour cette procédure.

Indiquez le nom du compartiment dans lequel vous téléchargerez le fichier VMDK, tel que *<bucket-name>*, le nom utilisé dans l'exemple suivant.

L'objectif de ce fichier JSON particulier est d'associer une nouvelle stratégie au nouveau rôle. Nommez le fichier comme vous le souhaitez. Dans cette procédure, l'exemple de nom pour ce fichier est `role-policy.json`.

Le texte suivant est un exemple du contenu de l'exemple de fichier `role-policy.json`.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource":[
                "arn:aws:s3:::<bucket-name>"
            ]
        },
        {
            "Effect":"Allow",
            "Action":[
                "s3:GetObject"
            ],
            "Resource":[
                "arn:aws:s3:::<bucket-name>/*"
            ]
        },
        {
            "Effect":"Allow",
            "Action":[
                "ec2:ModifySnapshotAttribute",
                "ec2:CopySnapshot",
                "ec2:RegisterImage",
                "ec2:Describe*"
            ],
            "Resource":"*"
        }
    ]
}
```

d Créez une stratégie, associez-la au nouveau rôle et stockez-la dans le fichier JSON récemment créé.

Par exemple, à l'aide de l'interface de ligne de commande (CLI), exécutez la commande suivante.

Il s'agit d'un exemple générique.

```
aws iam put-role-policy --role-name <role-name> --policy-name <policy-name> --policy-
document <file-path>
```

L'exemple spécifique suivant remplace l'espace réservé *<role-name>* par un exemple spécifique d'une stratégie nommée `vmimport`, l'espace réservé *<policy-name>* par l'exemple spécifique du rôle nommé précédemment, également appelé `vmimport` et l'espace réservé *<file-path>* par l'exemple spécifique du fichier JSON précédemment nommé, `role-policy.json`.

```
aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-document
file://role-policy.json
```

Pour plus d'informations sur l'exécution de la commande `put-role-policy`, reportez-vous à la documentation d'Amazon Elastic Compute Cloud.

5 Importez un snapshot à partir du fichier VMDK importé.

a Créez le troisième des trois nouveaux fichiers JSON requis pour cette procédure.

Incluez les informations suivantes dans le fichier.

- Le nom du compartiment, tel que *<bucket-name>*, qui est utilisé dans l'exemple suivant.
- Nom du fichier VMDK que vous avez chargé dans votre compartiment Amazon S3, tel que *<vmdk-file-name-uploaded-to-S3>*, qui est utilisé dans l'exemple suivant.

L'objectif de ce fichier JSON particulier est de stocker le snapshot du fichier VMDK importé. Nommez le fichier comme vous le souhaitez. Dans cette procédure, l'exemple de nom pour ce fichier est `container.json`.

Le texte suivant est un exemple du contenu du fichier `container.json`.

```
{
    "Description": "Adapter-VM",
    "Format": "vmdk",
    "UserBucket": {
        "S3Bucket": "<bucket-name>",
        "S3Key": "<vmdk-file-name-uploaded-to-S3>"
    }
}
```

b Exécutez la commande pour importer le snapshot à partir du fichier VMDK importé dans le fichier JSON récemment créé.

À l'aide de l'interface de ligne de commande (CLI), exécutez le type de commande suivant.

```
aws ec2 import-snapshot --role-name <role-name> --description <description> --disk-
container <file-path>
```

Pour plus d'informations sur l'exécution de la commande `import-snapshot`, reportez-vous à la documentation d'Amazon Elastic Compute Cloud.

La commande suivante est un exemple spécifique de la commande `import-snapshot`, dans laquelle le paramètre `role-name` est facultatif et n'est pas utilisé, la description est `"Adapter-VM"` et le nom de fichier du conteneur est `container.json`.

```
aws ec2 import-snapshot --description "Adapter-VM" --disk-container file://
container.json
```

L'exécution de la commande `import-snapshot` peut prendre plusieurs minutes. Cependant, une fois que vous avez exécuté la commande, celle-ci crée une sortie qui inclut une ligne `ImportTaskId` que vous pouvez utiliser pour suivre la progression de la tâche. La sortie suivante est un exemple.

```
{
    "ImportTaskId": "import-snap-05b4c84af4xxxxxxx",
    "Description": "Adapter-VM",
    "SnapshotTaskDetail": {
        "StatusMessage": "pending",
        "UserBucket": {
              "S3Bucket": "awsbucket",
             "S3Key": "edge-gw-2.3.3.0-22720582.ec2.vmdk"
         },
       "Progress": "0",
       "Status": "active",
        "Description": "Adapter-VM",
        "DiskImageSize": 0.0
    }

}
```

c Notez la valeur `ImportTaskId` dans la sortie de la commande `import-snapshot`.

6 Pour suivre la progression de la tâche `import-snapshot` et obtenir l'ID de snapshot, exécutez la commande suivante.

```
aws ec2 describe-import-snapshot-tasks --import-task-ids <import-task-id>
```

Remplacez l'espace réservé *<import-task-id>* par la valeur répertoriée dans la sortie de la commande `import-snapshot`. L'exemple de valeur répertorié dans l'exemple de sortie précédent est `import-snap-05b4c84af4xxxxxxx`. Pour plus d'informations sur l'exécution de la commande `describe-import-snapshot-tasks`, reportez-vous à la documentation d'Amazon Elastic Compute Cloud.

La commande `describe-import-snapshot-tasks` fournit une sortie qui indique la progression de la tâche `import-snapshot` et, lorsque celle-ci est terminée, fournit l'ID de snapshot qui est nécessaire à l'enregistrement de l'image. Par exemple :

- `"Progress": "43"`. Une telle ligne dans la sortie indique le pourcentage de progression de la tâche `import-snapshot`. Dans cet exemple, la tâche est effectuée à 43 %.
- `"Status": "completed"`. Une telle ligne dans la sortie indique la fin de la tâche `import-snapshot`.
- `"SnapshotId": "snap-06d42e043bxxxxxxx"`. Une telle ligne dans la sortie est incluse à la fin de la tâche. Dans cet exemple, l'ID de snapshot est `snap-06d42e043bxxxxxxx`.

7 Notez l'ID de snapshot de la sortie de la commande `describe-import-snapshot-tasks`.

8 Pour enregistrer l'image de snapshot, exécutez la commande `register-image`.

```
aws ec2 register-image --region us-west-2 --name <image-name> --architecture x86_64 --root-device-name '/dev/sda1' --virtualization-type hvm --ena-support --block-device-mappings DeviceName=/dev/sda1,Ebs={SnapshotId=<SnapshotId>}
```

Vous devez fournir ici des réponses spécifiques à votre déploiement pour chaque option, telles que `--region`, `--architecture`, etc. Pour plus d'informations sur l'exécution de la commande `register-image`, reportez-vous à la documentation d'Amazon Elastic Compute Cloud.

Les informations suivantes sont spécifiques à l'option `--name` et au paramètre `SnapshotId`.

- `--name` : fournissez un nom pour l'image en fonction des contraintes de la chaîne.
- `SnapshotId` : fournissez l'ID de snapshot de la sortie de la commande `describe-import-snapshot-tasks`.

La commande `register-image` fournit une sortie qui inclut l'ID de l'image de machine Amazon (AMI, Amazon Machine Image). Voici un exemple de sortie `register-image` standard.

```
{
        "ImageId": "ami-0721ee000321c4685"
    }
```

L'AMI indiquée dans la sortie de la commande `register-image` s'affiche également dans la console de gestion AWS dans la liste des AMI.

9 Pour prendre en charge la création et la configuration de l'instance d'AMI d'Passerelle Horizon Edge, préparez un script de démarrage semblable à l'exemple suivant.

```
#! /bin/bash
/usr/bin/python3 /opt/vmware/bin/configure-adapter.py --sshEnable
sudo useradd ccadmin
echo -e 'password\npassword' | passwd ccadmin
echo 'cs_ip cs_fqdn' >> /etc/hosts
```

Dans l'exemple, le script prend en charge les configurations suivantes :

- Activation de l'accès SSH au dispositif Passerelle Horizon Edge.
- Création d'un compte d'utilisateur `ccadmin` sur le dispositif avec le mot de passe défini (<*Mypassword*>\n<*Mypassword*>). Veillez à définir un mot de passe fort. Les mots de passe forts contiennent au moins 8 caractères et doivent inclure un ou plusieurs chiffres, des lettres majuscules et minuscules et des caractères spéciaux.
- Résolution du nom d'hôte (*cs_fqdn*) du Serveur de connexion sur l'adresse IP (*cs_ip*) du Serveur de connexion.

Vous devez ajouter ce script aux données utilisateur à l'étape suivante à laquelle vous lancez l'instance d'AMI d'Passerelle Horizon Edge.

10 Lancez l'instance d'AMI pour Passerelle Horizon Edge.

Note Pour vous assurer que cette instance fournit des capacités suffisantes, utilisez au moins le modèle c5.2xlarge.

Vous pouvez lancer une instance à l'aide de la console de gestion AWS ou de l'interface de ligne de commande (CLI). Dans les deux cas, utilisez l'ID de l'image de la machine Amazon (AMI, Amazon Machine Image) fournie dans la sortie de la commande `register-image` et ajoutez le script de démarrage que vous aviez préparé à l'étape précédente aux données utilisateur.

Note Vous devez ajouter le script de démarrage à ce stade, car les données utilisateur ne sont exécutées qu'à la première séquence de démarrage de l'instance d'AMI.

Pour utiliser l'interface de ligne de commande (CLI), reportez-vous à la documentation d'Amazon Elastic Compute Cloud pour en savoir plus sur l'exécution de la commande `run-instances`.

Pour utiliser la console de gestion AWS, reportez-vous à la documentation d'Amazon Elastic Compute Cloud, par exemple pour lancer une instance à l'aide de l'assistant de lancement d'instance.

Si vous choisissez de lancer l'instance à l'aide de la console de gestion AWS, localisez la nouvelle AMI en fonction de l'ID d'image, sélectionnez l'AMI, puis cliquez sur **Lancer**. Vous pouvez ensuite poursuivre l'assistant en fournissant les informations de votre déploiement.

11 Après le démarrage de l'AMI d'Passerelle Horizon Edge, modifiez la configuration de l'instance d'AMI et supprimez le script de démarrage.

12 Connectez-vous via SSH à l'instance d'AWS de la VM Passerelle Horizon Edge.

Pour utiliser l'interface de ligne de commande ou la console de gestion AWS, reportez-vous à la documentation d'Amazon Elastic Compute Cloud pour plus d'informations sur la connexion à votre instance. Nous recommandons SSH pour autoriser le copier-coller de la clé de couplage.

Pour des informations complémentaires, consultez Activer l'accès SSH pour Horizon Edge .

Pour obtenir des informations connexes, reportez-vous également aux sections Connexion à votre instance de Linux et Connexion à votre instance de Linux avec EC2 Instance Connect dans la documentation du produit AWS.

13 Exécutez un script pair-edge à l'aide du format de commande suivant, où *pairing_code* est le code de couplage que vous avez copié à partir de la capture d'écran de l'étape 9 décrite dans Déployer un dispositif Horizon Edge à utiliser avec les déploiements d'Horizon 8 et le plan de contrôle Horizon Cloud Service - next-gen :

```
sudo /opt/vmware/sbin/pair-edge.sh 'pairing_code'
```

14 Pour améliorer la sécurité, pensez à désactiver SSH une fois ces étapes terminées.

15 Revenez à Horizon Universal Console pour terminer la configuration du détail d'Horizon Connection Server. Reportez-vous à la section Déployer un dispositif Horizon Edge à utiliser avec les déploiements d'Horizon 8 et le plan de contrôle Horizon Cloud Service - next-gen.

Espaces Horizon 8 : architecture fédérée avec la Solution Azure VMware : télécharger et déployer la passerelle Horizon Edge dans votre environnement d'Horizon Cloud Service - next-gen

Vous pouvez télécharger et déployer la passerelle Passerelle Horizon Edge dans votre déploiement fédéré d'Horizon 8 dans la Solution Azure VMware à coupler avec Horizon Cloud Service - next-gen.

Téléchargez et déployez le dispositif Passerelle Horizon Edge pour un déploiement d'espace qui utilise l'architecture fédérée pour VMware Cloud on Microsoft Azure. Dans l'architecture fédérée, vous devez déployer Passerelle Horizon Edge dans l'infrastructure Microsoft Azure native de l'environnement de votre espace.

Voici une présentation générale des étapes requises pour déployer Passerelle Horizon Edge dans l'infrastructure Azure native de l'environnement de votre espace

- Téléchargez le fichier VHD d'Passerelle Horizon Edge.
- Créez un conteneur de stockage Azure et téléchargez le fichier VHD du dispositif vers ce conteneur de stockage.
- Créez une image de machine virtuelle (VM) à partir du VHD téléchargé.
- Créez la VM Passerelle Horizon Edge à partir de l'image de cette dernière.

Conditions préalables

Suivez ces étapes pour télécharger et déployer le dispositif Passerelle Horizon Edge pour un déploiement de l'espace qui utilise l'architecture fédérée avec Azure VMware Solution (AVS). Dans l'architecture fédérée, vous devez déployer Passerelle Horizon Edge dans l'infrastructure Microsoft Azure native de l'environnement de votre espace.

Vous devez respecter les conditions préalables suivantes avant de poursuivre.

- Vérifiez que vous avez respecté les conditions préalables liées à la Passerelle Horizon Edge décrites dans la section Déploiements des dispositifs Horizon 8 Edge.
- Vérifiez que vous avez respecté les conditions préalables répertoriées dans la section Rendre les URL de destination appropriées accessibles pour déployer une passerelle Passerelle Horizon Edge dans un environnement Horizon 8 pour utiliser la passerelle Passerelle Horizon Edge pour coupler un espace Horizon 8 avec Horizon Cloud Service.
- Le dispositif virtuel Passerelle Horizon Edge doit accéder à Internet pour communiquer avec le plan de contrôle Horizon Cloud. Si votre environnement nécessite l'utilisation d'une

configuration de serveur proxy et de proxy pour que les dispositifs déployés accèdent à Internet, veillez à vérifier les informations liées au proxy, les limitations connues et les problèmes connus lors de l'utilisation des paramètres de proxy avec le dispositif Passerelle Horizon Edge.

Note **Mettre à jour la configuration du proxy dans Edge**

```
/opt/vmware/bin/configure-edge-webproxy.py --proxyHost 127.0.0.1 --proxyPort 3128 --
proxyUsername 'exampleUsername' --proxyPassword 'examplePassword'
```

Pour explorer plus d'options, exécutez le script avec l'option `-h`, comme indiqué ci-dessous :

```
/opt/vmware/bin/configure-edge-webproxy.py -h
```

- Pour utiliser un proxy lors de l'exécution d'un script pair-edge, vous devez d'abord exécuter la commande suivante, en indiquant *true* lorsque ProxySSL est activé et sinon en indiquant *false* :

```
/opt/vmware/bin/pair-edge-with-proxy.sh -i 'IP_or FQDN_of Proxy' -o 'Proxy_Port' -u
'Proxy_User_Name' -p 'Proxy_Password' -s 'true_or_false' -c 'Connection_String'
```

Procédure

1 Téléchargez l'image disque Passerelle Horizon Edge à l'aide de *Étape 7. Utilisez l'option Télécharger pour obtenir le fichier binaire du dispositif de passerelle Horizon Edge.Instruction* de la procédure à la page Déployer un dispositif Horizon Edge à utiliser avec les déploiements d'Horizon 8 et le plan de contrôle Horizon Cloud Service - next-gen. Répondez à toutes les invites à l'écran.

L'image disque Passerelle Horizon Edge est disponible sous la forme d'un fichier VHD. Téléchargez le fichier VHD sur votre système local comme spécifié.

Note Téléchargez la version 2.3.3.0 ou ultérieure de l'image disque Passerelle Horizon Edge, par exemple `edge-gw-2.3.3.0-22720582.azure.vhd.zip`.

Enregistrez le fichier binaire téléchargé dans un emplacement à partir duquel vous le déploierez sur la plate-forme de virtualisation souhaitée, puis revenez à cette séquence d'étapes pour poursuivre le processus de couplage requis.

Note Les fonctionnalités et les services suivants ne sont pas pris en charge pour les espaces Horizon dans AVS en cas de couplage avec Passerelle Horizon Edge :

- Attribution de licence
- Surveillance

Avant de télécharger le fichier image de disque dans votre environnement AVS, vous devez d'abord créer un conteneur de stockage Azure et le partager à l'aide d'une signature d'accès partagé.

2 Dans le portail Azure, accédez à votre compte de stockage et créez un conteneur de stockage pour le fichier VHD. Pour plus d'informations, reportez-vous à la section https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview.

Lors de la création de la signature d'accès partagé, un jeton SAS est généré. Vous devez construire une URL de compte de stockage pour le fichier image de disque en ajoutant le jeton SAS à l'URL du conteneur de stockage.

a Pour ouvrir le conteneur de stockage, accédez à **Compte de stockage > Propriétés > URL**. Notez l'URL du conteneur de stockage pour les étapes suivantes.

b Créez une signature d'accès partagé. Accédez à **Compte de stockage > Signature d'accès partagé > Sélectionner les types de ressources et générer SAS et une chaîne de connexion**. Notez le jeton SAS généré pour les étapes suivantes.

c Construisez l'URL du compte de stockage à l'aide du format suivant :

<*StorageContainerPath*>/EdgeDiskImageName.vhd<*SAS-Token*>

Vous trouverez ci-après un exemple d'URL de compte de stockage :

```
https://azurestorage1.blob.core.windows.net/vmware/edge-
gw-2.3.3.0-22720582.azure.vhd.zip?
sv=2020-01-01&ss=bfqt&srt=sco&sp=rwdlapx&se=2020-01-01T12:00:00Z&st=2020-01-01T06:00:00
Z&spr=https&sig=dUPul74l4K0ah%2FdoCpaTTjY4t2Js8kBY%3D
```

3 Téléchargez le fichier image de disque vers l'URL du compte de stockage que vous avez créée.

a Téléchargez et installez l'utilitaire AzCopy sur le système local où vous avez extrait le fichier VHD contenant l'image de disque Passerelle Horizon Edge.

Pour plus d'informations sur l'utilitaire AzCopy, reportez-vous à la section https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10.

b Pour télécharger le fichier VHD, exécutez la commande suivante dans l'utilitaire AzCopy :

azcopy cp <*Path to extracted VHD file*> "<*StorageAccountURL*>" --blob-type PageBlob

L'exemple suivant montre un exemple de commande de chargement émise par un ordinateur Windows local :

```
azcopy cp c:\edge-gw-2.3.3.0-22720582.azure.vhd.zip "https://
azurestorage1.blob.core.windows.net/vmware/edge-gw-2.3.3.0-22720582.azure.vhd?
sv=2020-01-01&ss=bfqt&srt=sco&sp=rwdlapx&se=2020-01-01T12:00:00Z&st=2020-01-01T06:00:00
Z&spr=https&sig=dUPul74l4K0ah%2FdoCpaTTjY4t2Js8kBY%3D" --blob-type PageBlob
```

4 Créez une image de machine virtuelle (VM) à partir du fichier VHD téléchargé.

   a Dans le portail Azure, accédez à **Images** et créez une image de VM. Entrez un nom pour l'image et spécifiez l'emplacement cible et le groupe de ressources.

   b Spécifiez les options suivantes :

      - Définissez l'option **Type de système d'exploitation** sur **Linux**.
      - Définissez l'option **Génération de la VM** sur **Gen1**.

   c Pour l'objet blob de stockage, accédez au compte de stockage et au conteneur que vous avez créés, puis sélectionnez le fichier VHD que vous avez téléchargé.

   d Cliquez sur **Créer** pour créer l'image de VM à partir du fichier VHD.

5 Pour déployer le dispositif Passerelle Horizon Edge, créez la VM du dispositif à partir de l'image de la VM.

   a Dans le portail Azure, ouvrez l'image de la VM que vous avez créée à l'étape précédente. Cliquez sur **Créer une VM**.

   b Spécifiez les paramètres suivants :

      - Entrez un nom pour la nouvelle VM. Il s'agit du nom d'hôte du dispositif Passerelle Horizon Edge.
      - Pour **Dimensionnement de la VM**, reportez-vous à la section Rendre les URL de destination appropriées accessibles pour déployer une passerelle Passerelle Horizon Edge dans un environnement Horizon 8.

   c Pour le compte d'administrateur, spécifiez **`ccadmin`** comme nom d'utilisateur. Vous devez créer ce compte d'utilisateur **`ccadmin`** afin d'autoriser l'accès SSH au dispositif.

   d Pour l'accès SSH, spécifiez la méthode d'authentification par **Clé publique SSH**.

   Note Les méthodes d'authentification par clé publique SSH et par mot de passe sont prises en charge. Toutefois, la clé publique SSH fournit une sécurité renforcée et constitue la méthode préférée.

   e Pour les paramètres de pare-feu, configurez les ports suivants :

      - Port 443 pour HTTPS
      - Port 22 pour SSH

      Si vous prévoyez de configurer un pare-feu et un serveur proxy pour le dispositif, vous devez également configurer le dispositif pour autoriser certaines URL publiques. Pour plus d'informations, Rendre les URL de destination appropriées accessibles pour déployer une passerelle Passerelle Horizon Edge dans un environnement Microsoft Azure.

f Pour les paramètres réseau, spécifiez une allocation d'adresse IP publique si vous devez autoriser l'accès au dispositif sur un réseau public. Spécifiez également les ports entrants publics pour HTTPS et SSH.

g Accédez à **Propriétés de la VM** et notez l'adresse IP et le nom de domaine complet de la VM du dispositif. Vous aurez besoin de ces informations ultérieurement pour accéder au portail de configuration Passerelle Horizon Edge basé sur le navigateur.

6 Si votre environnement nécessite l'utilisation d'un serveur proxy HTTP pour que vos dispositifs virtuels accèdent à Internet, configurez les paramètres liés au proxy du dispositif, comme décrit dans la section Conditions préalables de cette rubrique.

7 Autorisez l'accès SSH à la passerelle Passerelle Horizon Edge à l'aide d'une interface de ligne de commande. Pour des informations complémentaires, consultez Activer l'accès SSH pour Horizon Edge .

8 Si vous voulez utiliser un nom de domaine complet (FQDN) pour le dispositif Passerelle Horizon Edge et résoudre le nom d'hôte, créez un enregistrement de recherche directe et inversée dans votre serveur DNS qui mappe ce nom de domaine complet à l'adresse IP statique du dispositif virtuel Passerelle Horizon Edge.

9 Connectez-vous via SSH à l'instance de Microsoft Azure de la VM Passerelle Horizon Edge.

Pour des informations complémentaires, consultez Activer l'accès SSH pour Horizon Edge .

Pour plus d'informations sur la connexion à votre instance, reportez-vous à la documentation de Microsoft Azure. Nous recommandons SSH pour autoriser le copier-coller de la clé de couplage.

10 Exécutez un script pair-edge à l'aide du format de commande suivant, où *pairing_code* est le code de couplage que vous avez copié à partir de la page de l'interface utilisateur **6. Déployer et coupler la passerelle Horizon Edge** décrite dans Déployer un dispositif Horizon Edge à utiliser avec les déploiements d'Horizon 8 et le plan de contrôle Horizon Cloud Service - next-gen :

```
/opt/vmware/sbin/pair-edge.sh 'pairing_code'
```

11 Pour améliorer la sécurité, pensez à désactiver SSH une fois ces étapes terminées.

12 Revenez à Horizon Universal Console pour terminer la configuration du détail d'Horizon Connection Server. Reportez-vous à la section Déployer un dispositif Horizon Edge à utiliser avec les déploiements d'Horizon 8 et le plan de contrôle Horizon Cloud Service - next-gen.

Espaces Horizon 8 : architecture fédérée avec Google Cloud VMware Engine : télécharger et déployer la passerelle Horizon Edge dans votre environnement d'Horizon Cloud Service - next-gen

Vous pouvez télécharger et déployer la passerelle Passerelle Horizon Edge dans votre déploiement fédéré d'Horizon 8 dans Google Cloud Platform (GCP) à coupler avec Horizon Cloud Service - next-gen.

Téléchargez et déployez le dispositif Passerelle Horizon Edge pour un déploiement d'espace qui utilise l'architecture fédérée pour VMware Cloud on Google Cloud Platform. Dans l'architecture fédérée, vous devez déployer Passerelle Horizon Edge dans l'infrastructure Google Cloud Platform (GCP) native de l'environnement de votre espace.

Voici une présentation générale des étapes requises pour déployer Passerelle Horizon Edge dans l'infrastructure GCP native de l'environnement de votre espace

- Téléchargez le fichier TAR d'Passerelle Horizon Edge.
- Créez un compartiment de stockage Google Cloud et chargez le fichier TAR du dispositif dans ce compartiment.
- Créez une image personnalisée à partir du fichier TAR téléchargé.
- Créez l'instance de machine virtuelle (VM) Passerelle Horizon Edge à partir de l'image personnalisée.

Conditions préalables

Vous devez respecter les conditions préalables suivantes avant de poursuivre.

- Vérifiez que vous avez respecté les conditions préalables liées à la Passerelle Horizon Edge décrites dans la section Déploiements des dispositifs Horizon 8 Edge.
- Vérifiez que vous avez respecté les conditions préalables répertoriées dans la section Rendre les URL de destination appropriées accessibles pour déployer une passerelle Passerelle Horizon Edge dans un environnement Horizon 8 pour utiliser la passerelle Passerelle Horizon Edge pour coupler un espace Horizon 8 avec Horizon Cloud Service.
- Le dispositif virtuel Passerelle Horizon Edge doit accéder à Internet pour communiquer avec le plan de contrôle Horizon Cloud. Si votre environnement nécessite l'utilisation d'une configuration de serveur proxy et de proxy pour que les dispositifs déployés accèdent à Internet, veillez à vérifier les informations liées au proxy, les limitations connues et les problèmes connus lors de l'utilisation des paramètres de proxy avec le dispositif Passerelle Horizon Edge.

Note **Mettre à jour la configuration du proxy dans Edge**

```
/opt/vmware/bin/configure-edge-webproxy.py --proxyHost 127.0.0.1 --proxyPort 3128 --
proxyUsername 'exampleUsername' --proxyPassword 'examplePassword'
```

Pour explorer plus d'options, exécutez le script avec l'option `-h`, comme indiqué ci-dessous :

```
/opt/vmware/bin/configure-edge-webproxy.py -h
```

- Pour utiliser un proxy lors de l'exécution d'un script pair-edge, vous devez d'abord exécuter la commande suivante, en indiquant *true* lorsque ProxySSL est activé et sinon en indiquant *false* :

  ```
  /opt/vmware/bin/pair-edge-with-proxy.sh -i 'IP_or FQDN_of Proxy' -o 'Proxy_Port' -u
  'Proxy_User_Name' -p 'Proxy_Password' -s 'true_or_false' -c 'Connection_String'
  ```

- Vous pouvez effectuer certaines étapes de déploiement à l'aide de l'interface utilisateur graphique (GUI) de Google Cloud ou de l'interface de ligne de commande (CLI) de Google Cloud. Pour utiliser l'interface de ligne de commande (CLI), vous devez d'abord installer les composants requis sur votre système local :
  - Outil `gsutil`. Pour obtenir des instructions, reportez-vous à la documentation de Google Cloud Storage.
  - SDK Google Cloud. Pour obtenir des instructions, reportez-vous à la documentation du SDK Google Cloud.

Procédure

1. Téléchargez l'image disque Passerelle Horizon Edge à l'aide de *Étape 7. Utilisez l'option Télécharger pour obtenir le fichier binaire du dispositif de passerelle Horizon Edge.Instruction* de la procédure à la page Déployer un dispositif Horizon Edge à utiliser avec les déploiements d'Horizon 8 et le plan de contrôle Horizon Cloud Service - next-gen. Répondez à toutes les invites à l'écran.

   L'image disque Passerelle Horizon Edge est disponible sous la forme d'un fichier TAR. Téléchargez le fichier TAR sur votre système local comme spécifié.

   Enregistrez le fichier binaire téléchargé dans un emplacement à partir duquel vous le déploierez sur la plate-forme de virtualisation souhaitée, puis revenez à cette séquence d'étapes pour poursuivre le processus de couplage requis.

   Note Pour déployer le dispositif dans un environnement GCVE, téléchargez la version 2.3.3.0 ou ultérieure de l'image disque Passerelle Horizon Edge, par exemple `edge-gw-2.3.3.0-22720582.google.tar.gz`.

   Avant de charger le fichier d'image de disque dans votre environnement GCVE, vous devez d'abord créer un compartiment Google Cloud Storage.

2. Créez un compartiment Google Cloud Storage dans votre environnement GCVE. Pour obtenir des instructions détaillées, reportez-vous à la documentation de Google Cloud.

3. Chargez le fichier TAR téléchargé dans votre compartiment Google Cloud Storage. Vous pouvez effectuer cette étape à l'aide de l'interface utilisateur graphique (GUI) de Google Cloud ou de l'interface de ligne de commande (CLI) de Google Cloud.
   - (GUI) Connectez-vous à Google Cloud Platform pour votre environnement GCVE. Accédez à la page **Cloud Storage**, sélectionnez le compartiment que vous avez créé précédemment et chargez le fichier TAR dans ce compartiment.

- (CLI) Ouvrez la console `gsutil` et exécutez la commande suivante.

  ```
  gsutil cp <file-path-to-TAR-file> gs://<bucket-name>
  ```

4 Créez une image personnalisée à partir du fichier TAR téléchargé.

- (GUI) Dans Google Cloud Platform, accédez à la page **Compute Engine > Images**. Sélectionnez l'option pour créer une image. Sur la page de création d'image, spécifiez **Cloud Storage** en tant que source et accédez au fichier TAR chargé dans votre compartiment. Spécifiez d'autres propriétés de l'image, le cas échéant, puis procédez à la création de l'image.

  Vérifiez que la nouvelle image apparaît dans la liste **Images**.

- (CLI) Dans la console `gsutil`, exécutez la commande de création d'image, semblable à l'exemple suivant.

  ```
  gcloud compute --project <project-name> images create <image-name> --description
  <image-description> --source-uri <TAR-file-uri>
  ```

  Note Vous pouvez personnaliser la commande avec les paramètres appropriés si nécessaire. Pour obtenir des informations détaillées, reportez-vous à la documentation de référence du SDK Google Cloud.

5 Pour prendre en charge la création et la configuration de l'instance de machine virtuelle Passerelle Horizon Edge, préparez un script de démarrage semblable à l'exemple suivant.

```
#! /bin/bash
/usr/bin/python3 /opt/vmware/bin/configure-adapter.py --sshEnable
sudo useradd ccadmin
echo -e 'password\npassword' | passwd ccadmin
echo 'cs_ip cs_fqdn' >> /etc/hosts
```

Dans l'exemple, le script prend en charge les configurations suivantes :

- Activation de l'accès SSH au dispositif Passerelle Horizon Edge.
- Création d'un compte d'utilisateur `ccadmin` sur le dispositif avec le mot de passe défini (*password*).
- Résolution du nom d'hôte (*cs_fqdn*) du Serveur de connexion sur l'adresse IP (*cs_ip*) du Serveur de connexion.

6 Créez l'instance de VM Passerelle Horizon Edge à partir de l'image personnalisée. Assurez-vous de configurer au minimum **n2-standard-8** pour le dimensionnement de machine virtuelle ou le type de machine.

- (GUI) Dans Google Cloud Platform, accédez à la page **Images**, sélectionnez l'image personnalisée que vous avez créée précédemment, puis sélectionnez l'option de création d'une instance de machine virtuelle. Spécifiez au minimum **n2-standard-8** pour

le dimensionnement de machine virtuelle ou le type de machine, désignez l'image personnalisée comme disque de démarrage et ajoutez le script de démarrage que vous avez préparé précédemment. Spécifiez les autres propriétés de la machine virtuelle de la manière appropriée, puis procédez à la création de l'instance de machine virtuelle.

Vérifiez que la machine virtuelle Passerelle Horizon Edge figure dans la liste des instances de machine virtuelle.

- (CLI) Dans la console `gsutil`, exécutez la commande de création d'instance, semblable à l'exemple suivant.

```
gcloud compute --project <project-name> instances create <instance-name>
--zone <zone> --machine-type <n2-standard-8-minimum> --network <network>
--subnet <subnet> --maintenance-policy <maintenance-policy> --scopes <scope>
--image <custom-TAR-image> --metadata startup-script=<startup-script>
```

Note Vous pouvez personnaliser la commande avec les paramètres appropriés si nécessaire. Pour obtenir des informations détaillées, reportez-vous à la documentation de référence du SDK Google Cloud.

7 Une fois la machine virtuelle Passerelle Horizon Edge démarrée, modifiez la configuration de l'instance de machine virtuelle et supprimez le script de démarrage.

Important Vous devez supprimer le script de démarrage de l'instance pour empêcher le script de s'exécuter à chaque redémarrage d'Passerelle Horizon Edge.

8 Connectez-vous via SSH à l'instance de GCP de la VM Passerelle Horizon Edge.

Pour des informations complémentaires, consultez Activer l'accès SSH pour Horizon Edge .

Pour plus d'informations sur la connexion à votre instance, reportez-vous à la documentation de Google Cloud. Nous recommandons SSH pour autoriser le copier-coller de la clé de couplage.

9 Exécutez un script pair-edge à l'aide du format de commande suivant, où *pairing_code* est le code de couplage que vous avez copié à partir de la page de l'interface utilisateur **6. Déployer et coupler la passerelle Horizon Edge** décrite dans Déployer un dispositif Horizon Edge à utiliser avec les déploiements d'Horizon 8 et le plan de contrôle Horizon Cloud Service - next-gen :

```
/opt/vmware/sbin/pair-edge.sh 'pairing_code'
```

10 Pour améliorer la sécurité, pensez à désactiver SSH une fois ces étapes terminées.

11 Revenez à Horizon Universal Console pour terminer la configuration du détail d'Horizon Connection Server. Reportez-vous à la section Déployer un dispositif Horizon Edge à utiliser avec les déploiements d'Horizon 8 et le plan de contrôle Horizon Cloud Service - next-gen.

Déploiements de Microsoft Azure Edge

Pour déployer des dispositifs Edge à partir d'Horizon Cloud Service - next-gen dans Microsoft Azure, vous devez configurer votre environnement Horizon Cloud, comme décrit dans les sections suivantes et utiliser l'e-mail de bienvenue Horizon Cloud Service - next-gen envoyé au compte d'administrateur.

Pour plus d'informations sur l'utilisation de l'e-mail de bienvenue Horizon Cloud Service - next-gen, reportez-vous à la section Chapitre 4 Intégration pour les administrateurs Horizon Cloud Service - next-gen.

Pour configurer le domaine Active Directory et le fournisseur d'identité, reportez-vous à la section Configuration des informations du fournisseur d'identité et d'accès pour les déploiements de dispositifs Edge.

Configuration réseau pour les déploiements de Microsoft Azure Edge

Dans Horizon Cloud Service - next-gen, configurez les paramètres réseau tels que les paramètres du serveur DNS et les règles de réseau et de groupe de sécurité.

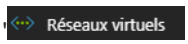
Configurer les paramètres du serveur DNS sur le réseau virtuel Microsoft Azure pour votre déploiement d'Horizon Edge

Les réseaux virtuels dans lesquels votre dispositif Horizon Edge est déployé doivent avoir la possibilité de résoudre les noms des machines internes et externes. La possibilité de résoudre les noms des machines virtuelles internes est nécessaire pour les opérations de jonction de domaine Active Directory du service avec les VM déployées dans votre environnement Microsoft Azure.

Conditions préalables

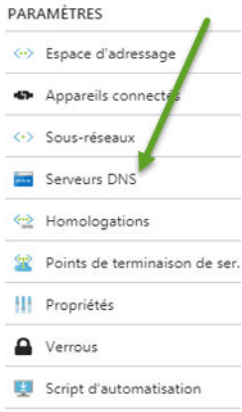
- Assurez-vous que votre région Microsoft Azure dispose de la topologie de réseau virtuel que vous prévoyez d'indiquer lorsque vous déployez une instance d'Horizon Edge.
- Assurez-vous que les paramètres du serveur DNS que vous ou votre équipe de mise en réseau allez configurer pour cette topologie de réseau virtuel peuvent atteindre et résoudre Active Directory et les adresses répertoriées dans Rendre les URL de destination appropriées accessibles pour déployer une passerelle Passerelle Horizon Edge dans un environnement Microsoft Azure.

Procédure

1. Dans la barre de navigation de gauche du portail Microsoft Azure, cliquez sur l' 

(**Réseaux virtuels**), puis cliquez sur le réseau virtuel que vous allez utiliser pour votre déploiement d'Horizon Edge.

2 Affichez les paramètres de serveur DNS du réseau virtuel en cliquant sur **Serveurs DNS**.



3 Utilisez l'option **Personnaliser**, ajoutez l'adresse du serveur DNS que vous souhaitez utiliser pour la résolution de nom et cliquez sur **Enregistrer**.

Configurer les paramètres réseau pour les régions Microsoft Azure

Pour Horizon Cloud Service - next-gen, votre déploiement requiert la prise en charge du sous-réseau dans la région Microsoft Azure, ce qui nécessite l'existence d'un réseau virtuel Microsoft Azure dans cette région.

Créez un réseau virtuel dans une région Microsoft Azure avec un espace d'adresses applicable pour les sous-réseaux requis.

Pour Horizon Cloud Service - next-gen, vous devez créer des sous-réseaux à l'avance.

Créez trois plages d'adresses de sous-réseau qui ne se chevauchent pas au format CIDR (routage interdomaine sans classe) dans le réseau virtuel. Les conditions requises suivantes pour le sous-réseau sont minimales. Pour des environnements plus grands, des sous-réseaux de taille plus grande peuvent être nécessaires.

Procédure

1 Créer le sous-réseau de gestion - /26 minimum

Si vous déployez une passerelle Edge (AKS) et que vous utilisez une passerelle NAT comme type de connectivité sortante, configurez une passerelle NAT. Assurez-vous également que le sous-réseau de gestion n'est pas en conflit avec les plages d'adresses IP suivantes.

- 169.254.0.0/16
- 172.30.0.0/16
- 172.31.0.0/16
- 192.0.2.0/24

2 Créez le sous-réseau de poste de travail (locataire).

Pour le sous-réseau principal de poste de travail (locataire), créez des sous-réseaux minimaux /27, mais d'une taille appropriée en fonction du nombre de postes de travail et de serveurs RDS. Vous pouvez ajouter d'autres sous-réseaux si nécessaire.

Note Si vous utilisez un équilibrage de charge interne, assurez-vous que tous les sous-réseaux de VM pour vos VM de poste de travail se trouvent dans les plages d'adresses IP décrites dans RFC1918.

3 Créez le sous-réseau de zone DMZ.

Créez des sous-réseaux minimaux /27 pour le cluster d'Unified Access Gateway.

Note Le déploiement d'une instance d'Unified Access Gateway nécessite trois sous-réseaux. Chaque VM Unified Access Gateway dispose de trois cartes réseau, une de chaque sous-réseau. Le pool principal d'équilibrage de charge externe est attaché aux cartes réseau du sous-réseau de zone DMZ. Le pool principal d'équilibrage de charge interne est attaché aux cartes réseau du sous-réseau de poste de travail. Vérifiez qu'il n'y a pas de règles de NSG (Groupes de sécurité réseau) ou de pare-feu qui bloquent l'entrée au réseau DMZ depuis Internet. Les seuls NSG que VMware déploie sont ceux qui sont attachés aux cartes réseau (pas au sous-réseau) et autorisent par défaut l'entrée. Toutes les règles de pare-feu ou de NSG qui bloquent le trafic entrant d'Internet vers les cartes réseau de zone DMZ entraînent des problèmes lors de la tentative de connexion aux instances d'Unified Access Gateway via l'équilibrage de charge externe.

Pour obtenir des informations complémentaires sur les NSG, reportez-vous à la section Présentation des règles de groupe de sécurité réseau par défaut pour les dispositifs Horizon Edge et Unified Access Gateway déployés dans Microsoft Azure.

Présentation des règles de groupe de sécurité réseau par défaut pour les dispositifs Horizon Edge et Unified Access Gateway déployés dans Microsoft Azure

L'utilisation de Horizon Cloud Service - next-gen pour créer des dispositifs Horizon Edge et Unified Access Gateway dans votre abonnement Microsoft Azure crée plusieurs groupes de sécurité réseau par défaut. Ces groupes de sécurité s'affichent lorsque vous vous connectez au portail Microsoft Azure et doivent rester tels que fournis.

Dans le cadre du déploiement des dispositifs Horizon Edge et Unified Access Gateway dans Microsoft Azure, le processus de déploiement automatique crée un ensemble de groupes de sécurité réseau (NSG) et associe chacun d'entre eux aux interfaces réseau (cartes réseau) individuelles qui se trouvent sur chaque dispositif Horizon Edge contrôlé par VMware et les machines virtuelles (VM) Unified Access Gateway. Ces VM liées aux dispositifs Edge et UAG sont les VM de la passerelle Edge et les VM déployées lorsque le dispositif Edge est configuré avec Unified Access Gateway.

Présentation globale

Dans Horizon Cloud Service - next-gen, le système de déploiement du dispositif Edge associe le NSG créé par le système de déploiement approprié à la carte réseau adéquate, en fonction de la conception et de l'architecture du dispositif Edge. Ces NSG sont utilisés au niveau de la carte réseau pour vérifier que chaque carte réseau sur un dispositif spécifique géré peut recevoir le trafic que le dispositif géré est censé recevoir pour les opérations de service et de dispositif Edge standard sur le sous-réseau associé à la carte réseau et pour bloquer tout le trafic que ce dispositif n'est pas censé recevoir. Chaque NSG contient un ensemble de règles de sécurité qui définissent le trafic autorisé vers et depuis chaque carte réseau.

Les NSG créés par le système de déploiement décrits ici sont distincts de ceux utilisés pour les VM, les batteries de serveurs et les postes de travail VDI de base qui sont provisionnés par le dispositif Edge lorsque vous les créez à l'aide de la console Horizon Universal Console.

Note Les règles de NSG créées par le système de déploiement décrites ici sont les exigences de configuration du service. Ne supprimez pas ni ne modifiez les NSG Horizon Cloud Service - next-gen qui sont automatiquement créés et associés aux cartes réseau des VM du dispositif Edge.

Les NSG créés par Horizon Cloud Service - next-gen et les règles à l'intérieur de ceux-ci sont propres aux cartes réseau et aux machines virtuelles spécifiques auxquelles ils sont attachés. Ils s'appliquent expressément dans le cadre de ces cartes réseau et de ces machines virtuelles. Toute modification apportée à ces NSG ou à ces règles, ou toute tentative de les utiliser à d'autres fins, même sur les mêmes sous-réseaux auxquels ces cartes réseau sont attachées, entraînera probablement une interruption du trafic réseau requis vers et depuis les cartes réseau auxquelles ils sont attachés. Cette interruption peut entraîner à son tour l'interruption de toutes les opérations du dispositif Edge. Le cycle de vie de ces NSG est géré par Horizon Cloud Service - next-gen. Il existe des raisons spécifiques pour chacun d'entre eux.

Étant donné que ces NSG créés par le système de déploiement sont des exigences de configuration du service, si vous tentez de les modifier ou de les déplacer, cela est considéré comme une utilisation non prise en charge d'Horizon Cloud Service - next-gen et une utilisation abusive des offres de service.

Toutefois, vous pouvez créer vos propres NSG contenant les règles de votre organisation dans des groupes de ressources en dehors de ceux du dispositif Edge qui sont créés automatiquement et gérés par Horizon Cloud Service - next-gen pour les VM du dispositif Edge. Les règles de vos propres NSG ne doivent pas entrer en conflit avec les conditions préalables d'Horizon Cloud Service - next-gen pour la gestion et les opérations des VM du dispositif Edge. Ces NSG doivent être attachés aux sous-réseaux de gestion, de locataire et de zone DMZ utilisés par le dispositif Edge. La création de vos propres NSG dans les groupes de ressources gérés par Horizon Cloud Service - next-gen entraîne un échec lors des actions de suppression sur les groupes de ressources gérés par Horizon Cloud Service - next-gen si vos NSG de ces groupes de ressources sont associés à une ressource qui se trouve dans un autre groupe de ressources.

Comme décrit dans la documentation de Microsoft Azure, l'objectif d'un groupe de sécurité réseau (NSG) est de filtrer le trafic réseau vers et depuis les ressources dans votre environnement Microsoft Azure à l'aide de règles de sécurité. Chaque règle dispose d'un ensemble de propriétés, telles que la source, la destination, le port, le protocole, etc. qui déterminent le trafic autorisé pour les ressources auxquelles le NSG est associé. Les NSG qu'Horizon Cloud Service - next-gen crée automatiquement et qu'il associe aux cartes réseau des VM de dispositif Edge contrôlées contiennent des règles spécifiques qu'Horizon Cloud Service - next-gen a jugées nécessaires pour la gestion du dispositif Edge du service, pour l'exécution appropriée des opérations du dispositif Edge en cours et pour la gestion du cycle de vie du dispositif Edge. Généralement, chaque règle définie dans ces NSG est destinée à fournir le trafic de port des opérations du dispositif Edge qui fait partie intégrante de l'exécution des objectifs commerciaux standard du service d'un abonnement à Horizon Cloud Service - next-gen, par exemple les cas d'utilisation VDI de la remise de postes de travail virtuels aux utilisateurs finaux. Pour des informations complémentaires, consultez Configuration requise des ports et des protocoles pour le déploiement d'Horizon 8 Edge.

Les sections ci-dessous répertorient les règles de NSG qu'Horizon Cloud Service - next-gen définit dans ces NSG créés par le système de déploiement.

Informations générales sur les NSG créés par le système de déploiement

Cette liste s'applique à tous les NSG créés par le système de déploiement que celui-ci associe à des cartes réseau spécifiques sur les VM associées au dispositif Edge.

- Ces NSG créés automatiquement sont destinés à la sécurité des dispositifs logiciels contrôlés. Lorsque de nouveaux logiciels sont ajoutés à votre abonnement et que des règles supplémentaires sont requises, ces nouvelles règles sont ajoutées à ces NSG.
- Pour Unified Access Gateway dans le portail Microsoft Azure, les NSG ont des noms qui contiennent le modèle `vmw-hcs-`*`UUID`*, où *UUID* est l'identifiant du dispositif Edge, à l'exception des NSG qui sont destinés à une configuration de passerelle externe déployée dans son propre réseau virtuel. Dans ce cas, les NSG appropriés de la passerelle ont des noms qui contiennent le modèle `vmw-hcs-`*`ID`*, où *ID* est l'ID de déploiement de cette passerelle externe.

  Note Pour le scénario dans lequel la configuration de la passerelle externe est déployée dans un abonnement distinct à l'aide de l'option de déploiement dans un groupe de ressources existant que vous avez créé dans cet abonnement, le NSG sur la carte réseau de gestion de la VM du connecteur de passerelle est nommé selon un modèle utilisant le nom du groupe de ressources au lieu du modèle `vmw-hcs-`*`UUID`*. Par exemple, si vous avez nommé ce groupe de ressources `hcsgateways`, Horizon Cloud Service - next-gen crée un NSG nommé `hcsgateways-mgmt-nsg` à l'intérieur et l'associe à la carte réseau de gestion de la VM du connecteur de passerelle.

  Pour la passerelle Horizon Edge, le NSG dispose du modèle d'attribution de nom `aks-agentpool-ID-nsg`, où `ID` est un numéro aléatoire ajouté par Microsoft Azure et le NSG fait partie du groupe de ressources avec le mode d'attribution de nom `vmw-hcs-UUID-edge-aks-node`, où `UUID` est l'identifiant du dispositif Edge.

Pour rechercher ces identifiants, vous pouvez accéder aux détails du dispositif Edge sur la page Capacité de la console d'administration.

Note Lorsque vous choisissez de faire en sorte que l'instance externe d'Unified Access Gateway du dispositif Edge utilise un groupe de ressources personnalisées, le nom du NSG créé par le système de déploiement de la VM du connecteur de passerelle contient le nom de ce groupe de ressources personnalisées au lieu du modèle `vmw-hcs-ID`. Par exemple, si vous spécifiez l'utilisation d'un groupe de ressources personnalisées nommé `ourhcspodgateway` pour la passerelle externe de votre dispositif Edge, le NSG que le système de déploiement crée et associe à la carte réseau de la machine virtuelle de la passerelle est nommé `ourhcspodgateway-mgmt-nsg`.

- Les NSG sont situés dans le même groupe de ressources que les VM et les cartes réseau auxquelles ils sont associés. Par exemple, les NSG associés aux cartes réseau des VM Unified Access Gateway externes sont situés dans le groupe de ressources nommé `vmw-hcs-UUID-uag` lors du déploiement de la passerelle externe dans le réseau virtuel du dispositif Edge et utilisant un groupe de ressources créé par le système de déploiement.
- Horizon Cloud peut ajouter des règles ou modifier ces règles selon les besoins afin de garantir la facilité de maintenance du service.
- Les NSG et règles sont conservés lors d'une mise à jour du dispositif Edge. Ils ne seront pas supprimés.
- Les règles Horizon Cloud Service - next-gen commencent à la priorité 1000 et les priorités augmentent généralement par incréments de 100. Les règles Horizon Cloud Service - next-gen se terminent par une règle à la priorité 3000.
- Les règles `AllowAzureInBound` relatives à l'adresse IP source 168.63.129.16 permettent aux NSG d'accepter les communications entrantes de la plate-forme Microsoft Azure, comme décrit dans la rubrique Qu'est-ce que l'adresse IP 168.63.129.16 ? de la documentation de Microsoft Azure. Toutes les VM associées au dispositif Edge se trouvent dans Microsoft Azure. Comme décrit dans la rubrique de la documentation de Microsoft Azure, leur adresse IP 168.63.129.16 facilite les différentes tâches de gestion de VM que la plate-forme de cloud Microsoft Azure effectue pour toutes les VM de leur cloud. Par exemple, cette adresse IP facilite l'utilisation de l'agent sur la VM pour communiquer avec la plate-forme Microsoft Azure afin d'indiquer que l'état de la VM est Prêt.
- Microsoft Azure crée automatiquement des règles par défaut dans chaque NSG au moment de sa création. Dans chaque NSG créé, Microsoft Azure crée des règles de trafic entrant et sortant à la priorité 65000 et suivantes. Ces règles Microsoft Azure par défaut ne sont pas décrites dans cette rubrique de la documentation, car elles sont créées automatiquement par Microsoft Azure. Pour plus d'informations sur ces règles par défaut, reportez-vous à la rubrique Règles de sécurité par défaut dans la documentation de Microsoft Azure.
- Chaque règle définie dans ces NSG est destinée à fournir le trafic de port des opérations du dispositif Edge qui fait partie intégrante de l'exécution des objectifs commerciaux

standard du service d'un abonnement Horizon Cloud Service - next-gen, par exemple les cas d'utilisation VDI de la remise de postes de travail virtuels aux utilisateurs finaux. Pour des informations complémentaires, consultez Configuration requise des ports et des protocoles pour le déploiement d'Horizon 8 Edge.

- Lorsque vous modifiez votre dispositif Edge pour spécifier des sous-réseaux de locataires supplémentaires à utiliser avec des batteries de serveurs et des attributions de poste de travail VDI, les règles dans les NSG liés au sous-réseau de locataire sur les VM de la passerelle Edge et les cartes réseau des VM Unified Access Gateway sont mises à jour afin d'inclure ces sous-réseaux de locataires supplémentaires.

NSG créés par le système de déploiement AKS de la passerelle Edge

L'AKS de la passerelle Edge dispose d'un groupe identique de machines virtuelles (VM) dans lequel une carte réseau est connectée au sous-réseau de gestion pour chaque instance de machine virtuelle. Microsoft Azure crée automatiquement un NSG spécifique et l'associe à toutes les cartes réseau associées aux instances du groupe identique de VM.

Pour le type de VM de la passerelle Edge, nous ne créons actuellement aucun NSG.

Dans votre environnement Microsoft Azure, le NSG AKS Edge réside dans le groupe de ressources du nœud AKS du dispositif Edge, qui est nommé selon le modèle `vmw-hcs-UUID-edge-aks-node`.

Le NSG est nommé selon le modèle `aks-agentpool-`*`ID`*`-nsg`, où `ID` est un numéro aléatoire attribué par Microsoft Azure.

Comme indiqué précédemment, Microsoft Azure crée les règles affichées par défaut dans les tableaux suivants, comme décrit dans la rubrique de la documentation de Microsoft Azure Règles de sécurité par défaut.

Tableau 5-1. Règles de NSG créées par le système de déploiement sur la carte réseau de gestion de l'instance du groupe de VM identique AKS de la passerelle Edge - Règles de sécurité entrantes

Priorité	Nom	Port	Protocole	Source	Destination	Action
65 000	AllowVnetInBound	Toutes	Toutes	VirtualNetwork	VirtualNetwork	Autoriser
65 001	AllowAzureLoadBalancerInBound	Toutes	Toutes	AzureLoadBalancer	Toutes	Autoriser
65 500	DenyAllInbound	Toutes	Toutes	Toutes	Toutes	Refuser

Tableau 5-2. Règles de NSG créées par le système de déploiement sur la carte réseau de gestion de l'instance du groupe de VM identique AKS de la passerelle Edge - Règles de sécurité sortantes

Priorité	Nom	Port	Protocole	Source	Destination	Action
65 000	AllowVnetOutBound	Toutes	Toutes	VirtualNetwork	VirtualNetwork	Autoriser
65 001	AllowInternetOutBound	Toutes	Toutes	Toutes	Internet	Autoriser
65 500	DenyAllOutbound	Toutes	Toutes	Toutes	Toutes	Refuser

NSG créés par le système de déploiement des VM Unified Access Gateway externes

Chacune des VM pour la configuration externe d'Unified Access Gateway dispose de trois (3) cartes réseau : une connectée au sous-réseau de gestion, une connectée au sous-réseau de locataire et une autre connectée au sous-réseau de zone DMZ. Le système de déploiement crée un NSG spécifique pour chacune de ces trois cartes réseau et associe chaque NSG à sa carte réseau appropriée.

- La carte réseau de gestion dispose d'un NSG nommé dans le modèle `vmw-hcs-`*`ID`*`-uag-management-nsg`.
- La carte réseau de locataire dispose d'un NSG nommé dans le modèle `vmw-hcs-`*`ID`*`-uag-tenant-nsg`.
- La carte réseau de la zone DMZ dispose d'un NSG nommé dans le modèle `vmw-hcs-`*`ID`*`-uag-dmz-nsg`.

Dans votre environnement Microsoft Azure, ces NSG sont nommés selon le modèle `vmw-hcs-`*`ID`*`-uag` où *ID* est l'ID du dispositif Edge tel qu'il est affiché sur la page de détails du dispositif Edge dans la console, sauf si la passerelle externe est déployée dans son propre réseau virtuel distinct de celui du dispositif Edge. Dans le cas d'une passerelle externe déployée dans son propre réseau virtuel, l'*ID* est la valeur de l'**ID de déploiement** affichée sur la page de détails du dispositif Edge.

Tableau 5-3. Règles de NSG créées par le système de déploiement sur la carte réseau de gestion des VM Unified Access Gateway externes

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Entrant	1000	AllowHttpsInBound	9443	TCP	Sous-réseau de gestion	Toutes	Autoriser	Pour que le service configure les paramètres d'administration de la passerelle à l'aide de son interface de gestion. Comme décrit dans la documentation du produit Unified Access Gateway, son interface de gestion se trouve sur le port 9443/TCP.
Entrant	1100	AllowAzureInBound	Toutes	Toutes	168.63.129.16	Toutes	Autoriser	Pour que la VM accepte les communications entrantes de la plate-forme Microsoft Azure, comme décrit dans la section Informations

Tableau 5-3. Règles de NSG créées par le système de déploiement sur la carte réseau de gestion des VM Unified Access Gateway externes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
								générales précédente et dans la rubrique de la documentation de Microsoft Azure Qu'est-ce que l'adresse IP 168.63.129.16.
Entrant	1200	AllowSshInBound	22	Toutes	Sous-réseau de gestion	Toutes	Autoriser	Pour que VMware effectue un accès d'urgence à la VM si nécessaire à des fins de dépannage. L'autorisation vous est demandée avant tout accès d'urgence.

Tableau 5-3. Règles de NSG créées par le système de déploiement sur la carte réseau de gestion des VM Unified Access Gateway externes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Entrant	3000	DenyAllInBound	Toutes	Toutes	Toutes	Toutes	Refuser	Ajouté par le système de déploiement pour limiter le trafic entrant de cette carte réseau aux éléments des lignes précédentes.
Sortant	3000	DenyAllOutBound	Toutes	Toutes	Toutes	Toutes	Refuser	Ajouté par le système de déploiement pour refuser le trafic sortant de cette carte réseau.

Tableau 5-4. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway externes

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Entrant	1000	AllowAzureInBound	Toutes	Toutes	168.63.129.16	Toutes	Autoriser	Pour que la VM accepte les communications entrantes de la plate-forme Microsoft Azure, comme décrit dans la section Informations générales précédente et dans la rubrique de la documentation de Microsoft Azure Qu'est-ce que l'adresse IP 168.63.129.16.
Entrant	1400	AllowPcoipUdpInBound	Toutes	UDP	Sous-réseau de locataire	Toutes	Autoriser	Cette règle prend en charge la configuration standard utilisée pour Unified Access Gateway utilisant Horizon Agent. Les agents Horizon

Tableau 5-4. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway externes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
								Agent sur les VM de poste de travail et de batterie de serveurs renvoient les données PCoIP aux instances d'Unified Access Gateway à l'aide d'UDP.
Entrant	3000	DenyAllInBound	Toutes	Toutes	Toutes	Toutes	Refuser	Ajouté par le système de déploiement pour limiter le trafic entrant de cette carte réseau aux éléments des lignes précédentes.

Tableau 5-4. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway externes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Sortant	1000	AllowHttpsOutBound	443 8443	TCP	Toutes	Sous-réseau de locataire	Autoriser	Cette règle prend en charge les instances d'Unified Access Gateway communiquant avec les VM de la passerelle Edge pour l'envoi de nouvelles demandes de connexion client aux passerelles Edge.
Sortant	1100	AllowBlastOutBound	22443	Toutes	Toutes	Sous-réseau de locataire	Autoriser	Cette règle prend en charge le cas d'utilisation d'une session Horizon Client Blast Extreme dans Horizon Agent sur une VM de poste de travail ou de batterie de serveurs.

Tableau 5-4. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway externes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Sortant	1200	AllowPcoipOutBound	4172	Toutes	Toutes	Sous-réseau de locataire	Autoriser	Cette règle prend en charge le cas d'utilisation d'une session Horizon Client PCoIP dans Horizon Agent sur une VM de poste de travail.

Tableau 5-4. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway externes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Sortant	1300	AllowUsbOutBound	32111	TCP	Toutes	Sous-réseau de locataire	Autoriser	Cette règle prend en charge le cas d'utilisation du trafic de redirection USB. La redirection USB est une option d'agent sur les VM de poste de travail ou de batterie de serveurs. Ce trafic utilise le port 32 111 pour une session client de l'utilisateur final dans Horizon Agent sur une VM de poste de travail ou de batterie de serveurs.

Tableau 5-4. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway externes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Sortant	1400	AllowMmrOutBound	9427	TCP	Toutes	Sous-réseau de locataire	Autoriser	Cette règle prend en charge les cas d'utilisation du trafic de redirection multimédia (MMR) et de redirection de pilote client (CDR). Ces redirections sont des options d'agent sur les VM de poste de travail ou de batterie de serveurs. Ce trafic utilise le port 9427, pour une session cliente d'utilisateur final dans Horizon Agent sur une VM de poste de travail ou de batterie de serveurs.

Tableau 5-4. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway externes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Sortant	1500	AllowAllOutBound	Toutes	Toutes	Toutes	Sous-réseau de locataire	Autoriser	Lors de l'exécution sur une machine virtuelle prenant en charge plusieurs sessions utilisateur, Horizon Agent choisit des ports différents à utiliser pour le trafic PCoIP des sessions. Étant donné que ces ports ne peuvent pas être déterminés à l'avance, vous ne pouvez pas définir à l'avance une règle de NSG nommant des ports spécifiques pour autoriser le trafic. Par conséquent, comme pour la règle à la priorité 1200, cette règle prend en

Tableau 5-4. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway externes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
								charge le cas d'utilisation de plusieurs sessions PCoIP d'Horizon Client avec ces VM.
Sortant	3000	DenyAllOutBound	Toutes	Toutes	Toutes	Toutes	Refuser	Ajouté par le système de déploiement pour limiter le trafic sortant de cette carte réseau aux éléments des lignes précédentes.

Tableau 5-5. Règles de NSG créées par le système de déploiement sur la carte réseau de zone DMZ des VM Unified Access Gateway externes

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Entrant	1000	AllowHttpsInBound	80 443	TCP	Internet	Toutes	Autoriser	Cette règle fournit le trafic entrant des utilisateurs finaux externes à partir des clients Horizon Client et du client Web Horizon pour demander l'authentification de connexion à la passerelle Edge. Par défaut, Horizon Client et le client Web Horizon utilisent le port 443 pour cette demande. Pour prendre en charge la redirection facile à titre de référence pour un utilisateur qui peut entrer HTTP dans son client au lieu de HTTPS, ce trafic

Tableau 5-5. Règles de NSG créées par le système de déploiement sur la carte réseau de zone DMZ des VM Unified Access Gateway externes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
								arrive sur le port 80 et est automatiquement redirigé vers le port 443.
Entrant	1100	AllowBlastInBound	443 8443	Toutes	Internet	Toutes	Autoriser	Cette règle prend en charge les instances d'Unified Access Gateway qui reçoivent le trafic Blast des clients Horizon Client d'utilisateurs finaux externes.
Entrant	1200	AllowPcoipInBound	4172	Toutes	Internet	Toutes	Autoriser	Cette règle prend en charge les instances d'Unified Access Gateway qui reçoivent le trafic PCoIP des clients Horizon Client d'utilisateurs finaux externes.

Tableau 5-5. Règles de NSG créées par le système de déploiement sur la carte réseau de zone DMZ des VM Unified Access Gateway externes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Entrant	1300	AllowAzureInBound	Toutes	Toutes	168.63.129.16	Toutes	Autoriser	Pour que la VM accepte les communications entrantes de la plate-forme Microsoft Azure, comme décrit dans la section Informations générales précédente et dans la rubrique de la documentation de Microsoft Azure Qu'est-ce que l'adresse IP 168.63.129.16.
Entrant	3000	DenyAllInBound	Toutes	Toutes	Toutes	Toutes	Refuser	Ajouté par le système de déploiement pour limiter le trafic entrant de cette carte réseau aux éléments des lignes précédentes.

NSG créés par le système de déploiement des VM Unified Access Gateway internes

Chacune des VM de la configuration interne d'Unified Access Gateway dispose de deux (2) cartes réseau : une connectée au sous-réseau de gestion et une autre connectée au sous-réseau de locataire. Le système de déploiement crée un NSG spécifique pour chacune de ces deux cartes réseau et associe chaque NSG à sa carte réseau appropriée.

- La carte réseau de gestion dispose d'un NSG nommé dans le modèle `vmw-hcs-`*`podUUID`*`-uag-management-nsg`.
- La carte réseau de locataire dispose d'un NSG nommé dans le modèle `vmw-hcs-`*`podUUID`*`-uag-tenant-nsg`.

Dans votre environnement Microsoft Azure, ces NSG se trouvent dans le groupe de ressources du dispositif Edge nommé selon le modèle `vmw-hcs-`*`podUUID`*`-uag-internal`.

Tableau 5-6. Règles de NSG créées par le système de déploiement sur la carte réseau de gestion des VM Unified Access Gateway internes

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Entrant	1000	AllowHttpsInBound	9443	TCP	Sous-réseau de gestion	Toutes	Autoriser	Pour que le service configure les paramètres d'administration de la passerelle à l'aide de son interface de gestion. Comme décrit dans la documentation du produit Unified Access Gateway, son interface de gestion se trouve sur le port 9443/TCP.
Entrant	1100	AllowAzureInBound	Toutes	Toutes	168.63.129.16	Toutes	Autoriser	Pour que la VM accepte les communications entrantes de la plate-forme Microsoft Azure, comme décrit dans la section Informations

Tableau 5-6. Règles de NSG créées par le système de déploiement sur la carte réseau de gestion des VM Unified Access Gateway internes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
								générales précédente et dans la rubrique de la documentation de Microsoft Azure Qu'est-ce que l'adresse IP 168.63.129.16.
Entrant	1200	AllowSshInBound	22	Toutes	Sous-réseau de gestion	Toutes	Toutes	Pour que VMware effectue un accès d'urgence à la VM si nécessaire à des fins de dépannage. L'autorisation vous est demandée avant tout accès d'urgence.

Tableau 5-6. Règles de NSG créées par le système de déploiement sur la carte réseau de gestion des VM Unified Access Gateway internes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Entrant	3000	DenyAllInBound	Toutes	Toutes	Toutes	Toutes	Refuser	Ajouté par le système de déploiement pour limiter le trafic entrant de cette carte réseau aux éléments des lignes précédentes.
Sortant	3000	DenyAllOutBound	Toutes	Toutes	Toutes	Toutes	Refuser	Ajouté par le système de déploiement pour refuser le trafic sortant de cette carte réseau.

Tableau 5-7. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway internes

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Entrant	1000	AllowAzureInBound	Toutes	Toutes	168.63.129.16	Toutes	Autoriser	Pour que la VM accepte les communications entrantes de la plate-forme Microsoft Azure, comme décrit dans la section Informations générales précédente et dans la rubrique de la documentation de Microsoft Azure Qu'est-ce que l'adresse IP 168.63.129.16.
Entrant	1100	AllowHttpsInBound	80 443	TCP	VirtualNetwork	Toutes	Autoriser	Cette règle fournit le trafic entrant des utilisateurs finaux internes à partir des clients Horizon Client et du client Web Horizon pour

Tableau 5-7. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway internes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
								demander l'authentification de connexion à la passerelle Edge. Par défaut, Horizon Client et le client Web Horizon utilisent le port 443 pour cette demande. Pour prendre en charge la redirection facile à titre de référence pour un utilisateur qui peut entrer HTTP dans son client au lieu de HTTPS, ce trafic arrive sur le port 80 et est automatiquement redirigé vers le port 443.

Tableau 5-7. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway internes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Entrant	1200	AllowBlastInBound	443 8443	Toutes	VirtualNetwork	Toutes	Autoriser	Cette règle prend en charge les instances d'Unified Access Gateway qui reçoivent le trafic Blast des clients Horizon Client d'utilisateurs finaux internes.
Entrant	1300	AllowPcoipInBound	4172	Toutes	VirtualNetwork	Toutes	Autoriser	Cette règle prend en charge les instances d'Unified Access Gateway qui reçoivent le trafic PCoIP des clients Horizon Client d'utilisateurs finaux internes.

Tableau 5-7. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway internes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Entrant	1400	AllowPcoipUdpInBound	Toutes	UDP	Sous-réseau de locataire	Toutes	Autoriser	Cette règle prend en charge la configuration standard utilisée pour Unified Access Gateway utilisant Horizon Agent. Les agents Horizon Agent sur les VM de poste de travail et de batterie de serveurs renvoient les données PCoIP aux instances d'Unified Access Gateway à l'aide d'UDP.

Tableau 5-7. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway internes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Entrant	3000	DenyAllInBound	Toutes	Toutes	Toutes	Toutes	Refuser	Ajouté par le système de déploiement pour limiter le trafic entrant de cette carte réseau aux éléments des lignes précédentes.
Sortant	1000	AllowHttpsOutBound	443 8443	TCP	Toutes	Sous-réseau de locataire	Autoriser	Cette règle prend en charge les instances d'Unified Access Gateway communiquant avec les VM de la passerelle Edge pour l'envoi de nouvelles demandes de connexion client au dispositif Edge.

Tableau 5-7. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway internes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Sortant	1100	AllowBlastOutBound	22443	Toutes	Toutes	Sous-réseau de locataire	Autoriser	Cette règle prend en charge le cas d'utilisation d'une session Horizon Client Blast Extreme dans Horizon Agent sur une VM de poste de travail ou de batterie de serveurs.
Sortant	1200	AllowPcoipOutBound	4172	Toutes	Toutes	Sous-réseau de locataire	Autoriser	Cette règle prend en charge le cas d'utilisation d'une session Horizon Client PCoIP dans Horizon Agent sur une VM de poste de travail.

Tableau 5-7. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway internes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Sortant	1300	AllowUsbOutBound	32111	TCP	Toutes	Sous-réseau de locataire	Autoriser	Cette règle prend en charge le cas d'utilisation du trafic de redirection USB. La redirection USB est une option d'agent sur les VM de poste de travail ou de batterie de serveurs. Ce trafic utilise le port 32 111 pour une session client de l'utilisateur final dans Horizon Agent sur une VM de poste de travail ou de batterie de serveurs.

Tableau 5-7. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway internes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Sortant	1400	AllowMmrOutBound	9427	TCP	Toutes	Sous-réseau de locataire	Autoriser	Cette règle prend en charge les cas d'utilisation du trafic de redirection multimédia (MMR) et de redirection de pilote client (CDR). Ces redirections sont des options d'agent sur les VM de poste de travail ou de batterie de serveurs. Ce trafic utilise le port 9427, pour une session cliente d'utilisateur final dans Horizon Agent sur une VM de poste de travail ou de batterie de serveurs.

Tableau 5-7. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway internes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
Sortant	1500	AllowAllOutBound	Toutes	Toutes	Toutes	Sous-réseau de locataire	Autoriser	Lors de l'exécution sur une machine virtuelle prenant en charge plusieurs sessions utilisateur, Horizon Agent choisit des ports différents à utiliser pour le trafic PCoIP des sessions. Étant donné que ces ports ne peuvent pas être déterminés à l'avance, vous ne pouvez pas définir à l'avance une règle de NSG nommant des ports spécifiques pour autoriser le trafic. Par conséquent, comme pour la règle à la priorité 1200, cette règle prend en

Tableau 5-7. Règles de NSG créées par le système de déploiement sur la carte réseau de locataire des VM Unified Access Gateway internes (suite)

Sens	Priorité	Nom	Ports	Protocole	Source	Destination	Action	Objectif
								charge le cas d'utilisation de plusieurs sessions PCoIP d'Horizon Client avec ces VM.
Sortant	3000	DenyAllOutBound	Toutes	Toutes	Toutes	Toutes	Refuser	Ajouté par le système de déploiement pour limiter le trafic sortant de cette carte réseau aux éléments des lignes précédentes.

Déploiement d'un dispositif Microsoft Azure Edge

Cette page de documentation décrit le flux de l'interface utilisateur Ajouter un dispositif Horizon Edge d'Horizon Universal Console que vous utilisez pour déployer un dispositif Horizon Edge dans votre abonnement Microsoft Azure.

Introduction

Horizon Edge est une infrastructure du Cloud légère de type thin-edge. Pour les déploiements Microsoft Azure, un abonnement Azure correspond au fournisseur.

Une fois que votre environnement est configuré avec au moins un domaine Active Directory et un fournisseur d'identité, la console rend ce flux d'interface utilisateur **Ajouter un dispositif Horizon Edge** disponible.

Types de déploiements

Un dispositif Horizon Edge déployé dans Microsoft Azure utilise le format de passerelle Edge (VM) ou de passerelle Edge (AKS).

Vous décidez du type à utiliser en fonction des qualités requises.

Type de déploiement	Qualités clés	Détails
AKS	■ Prend en charge plus de 5 000 sessions ■ Azure Kubernetes Service présente des conditions requises liées à Microsoft qui doivent être remplies ■ L'expérience de connexion SSO et la collecte de données de surveillance sont gérées via des services répliqués qui prennent en charge la distribution de ces fonctions avec une capacité de basculement complète en cas de panne.	AKS est une norme Microsoft Azure pour les applications cloud natives d'entreprise dans les centres de données Microsoft Azure. Le type AKS fournit une passerelle Edge d'une architecture en cluster, qui fournit des services répliqués prenant en charge l'expérience de connexion SSO et les collectes de données de surveillance.

VM	■ Prend en charge jusqu'à 5 000 sessions
	■ Moins de conditions préalables impliquées dans l'abonnement Microsoft Azure que pour le type AKS
	■ Si, ultérieurement, la VM déployée n'est pas disponible, le comportement qui en résulte est le suivant :
	  ■ Les utilisateurs finaux devront se connecter sans Single Sign-On (SSO)
	  ■ Les données de surveillance des postes de travail ne sont pas enregistrées pendant la période d'indisponibilité de la VM.
		Même si le type de VM est plus simple à déployer en raison de conditions préalables inférieures à celles du type AKS, si la VM déployée devient indisponible :
		■ Les utilisateurs finaux verront le flux de connexion sans expérience de connexion SSO. Par exemple, ils devront se connecter à l'aide de leurs informations d'identification Active Directory.
		■ Les données de surveillance des postes de travail qui sont envoyées à la VM de la passerelle Edge ne sont pas enregistrées pendant la période d'indisponibilité de la VM.

Conditions préalables

Avant d'effectuer ces étapes dans la console, vous devez vérifier que vous ou votre équipe informatique avez terminé les éléments répertoriés suivants.

Important Lorsque vous sélectionnez des éléments dans l'interface utilisateur de la console, le système tente de confirmer que des éléments spécifiques sont en place. Si ces conditions remplies ne sont pas remplies, vous ne pourrez alors pas effectuer les étapes de l'interface utilisateur.

Par exemple, lors du déploiement du type AKS, si la passerelle NAT sélectionnée dans **Type de cluster sortant** n'est pas connectée au **Sous-réseau de gestion** sélectionné, l'interface utilisateur affiche un message et empêche toute progression lorsque vous cliquez sur **Déployer**. À ce stade, vous devrez quitter l'assistant, remplir la condition requise de connexion de la passerelle NAT au sous-réseau de gestion et redémarrer l'assistant depuis le début.

- Examinez la Liste de vérification des conditions requises pour le déploiement d'un dispositif Microsoft Edge et assurez-vous que ces conditions requises sont remplies.
- Examinez les éléments préparatoires décrits sur les pages en lien hypertexte de la page Déploiements de Microsoft Azure, Horizon Edge - Préparation au déploiement et vérifiez que ces éléments sont terminés.
- Vérifiez que vous disposez des informations d'abonnement Azure, des informations réseau, des noms de domaine complets et de ces éléments afin de pouvoir les spécifier dans les champs et les listes de l'assistant.
- Vérifiez que les ports sortants nécessaires sont autorisés. Reportez-vous à la section Rendre les URL de destination appropriées accessibles pour déployer une passerelle Passerelle Horizon Edge dans un environnement Microsoft Azure.
- Si vous prévoyez d'utiliser un serveur proxy pour le trafic de routage, il doit être accessible via le sous-réseau de gestion Edge.
- Décidez si vous souhaitez que le fournisseur principal de ce dispositif Horizon Edge soit dédié à la passerelle Horizon Edge et aux instances d'Unified Access Gateway, ou si vous souhaitez que le fournisseur principal fournisse également les applications et les postes de travail des utilisateurs finaux.

  Note Pour que le fournisseur principal soit dédié aux dispositifs de passerelle de ce dispositif Horizon Edge, vous aurez besoin des informations d'abonnement Azure pour l'étape de l'assistant de spécification d'un fournisseur secondaire pour les postes de travail et les applications.

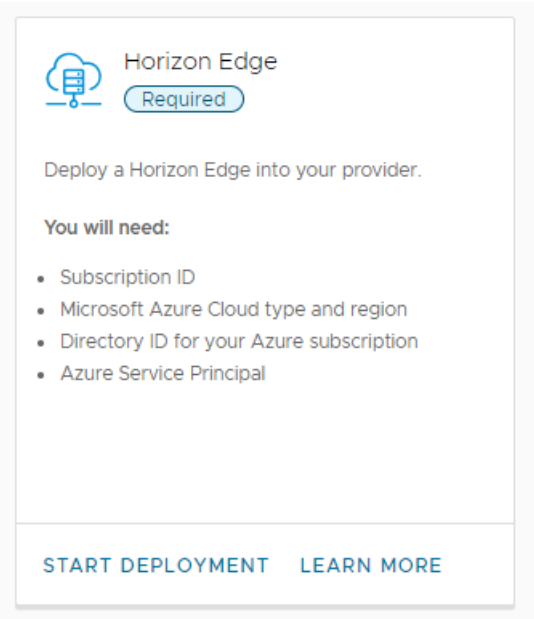
Démarrage de l'assistant de déploiement

La console rend l'assistant **Ajouter un dispositif Horizon Edge** disponible à partir de différents points d'entrée. Votre point de départ dans la console pour cette étape varie généralement selon que votre environnement est vierge ou qu'il dispose de déploiements existants d'Horizon Edge pour Horizon 8 ou pour Microsoft Azure.

Aucun dispositif Horizon Edge pour le moment : démarrez à partir de la carte Horizon Edge de la console

Si votre environnement ne dispose d'aucun dispositif Horizon Edge, vous pouvez démarrer généralement l'assistant en cliquant sur **DÉMARRER LE DÉPLOIEMENT**.

La capture d'écran suivante illustre cette carte **Horizon Edge**.



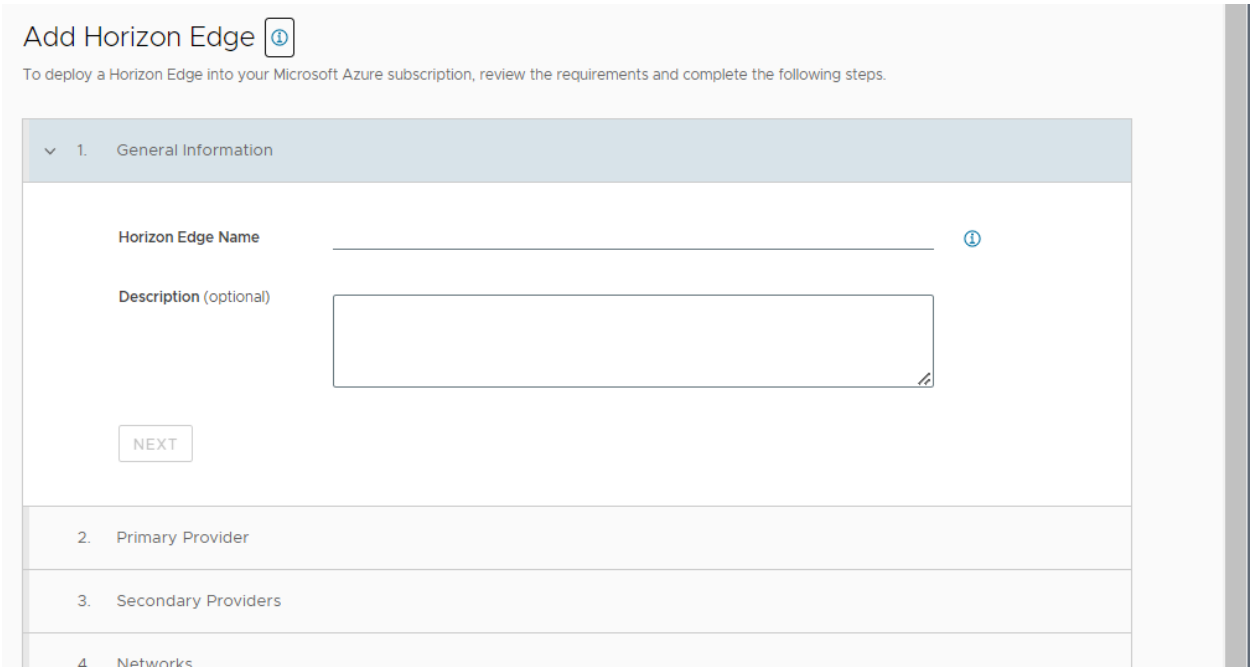
Aucun dispositif Horizon Edge : vous pouvez également démarrer à partir de la page Capacité de la console

Si aucun dispositif Horizon Edge n'est encore déployé dans l'environnement, la page Capacité contient du texte et un menu **Démarrer**. Dans ce scénario, vous pouvez démarrer l'assistant en accédant à **Ressources > Capacité** et en cliquant sur **Démarrer > Microsoft Azure**.

Au moins un dispositif Horizon Edge : démarrez à partir de la page Capacité de la console

Si au moins un dispositif Horizon Edge est déployé pour le moment dans l'environnement, la page Capacité contient une grille qui répertorie les dispositifs Horizon Edge existants. Dans ce scénario, vous pouvez démarrer l'assistant en accédant à **Ressources > Capacité** et en cliquant sur **Ajouter > Microsoft Azure**.

Après avoir utilisé l'une de ces trois méthodes pour démarrer l'assistant, la console affiche **Ajouter un dispositif Horizon Edge** à l'étape 1 de l'assistant.



Informations générales

Ajoutez un **Nom du dispositif Horizon Edge** qui distingue ce dispositif Horizon Edge des autres dispositifs qui s'affichent dans la console. Vous pouvez ajouter une description facultative.

Fournisseur principal

Remplissez cette section. Une fois cette étape terminée, passez à l'étape suivante.

1 Dans **Abonnement Azure**, sélectionnez l'un des fournisseurs existants de votre environnement ou utilisez **Ajouter un nouveau** pour fournir des informations d'abonnement sur le nouveau fournisseur.

   Lors de l'ajout d'informations d'abonnement sur le nouveau fournisseur, spécifiez les éléments suivants :

   - Nom unique de ce fournisseur qui le distingue des autres qui s'affichent dans la console.
   - Votre ID d'abonnement Microsoft Azure à partir du portail Microsoft Azure.
   - Sélectionnez le type de cloud Azure, la région Azure et l'ID d'annuaire applicables pour cet ID d'abonnement Microsoft Azure.
   - Spécifiez les informations du principal de service (l'**ID d'application** et la **Clé d'application**) que vous avez créées dans le portail Microsoft Azure à cette fin.

2 Pour dédier ce fournisseur à la passerelle Horizon Edge et aux instances d'Unified Access Gateway, et utiliser un fournisseur distinct pour transmettre des ressources autorisées d'utilisateurs finaux, cochez la case affichée.

   Si cette case n'est pas cochée, ce fournisseur transmet également les ressources autorisées des utilisateurs finaux.

3 Vous pouvez éventuellement spécifier des balises de ressources Azure à utiliser pour ce déploiement d'Horizon Edge en développant l'interface utilisateur pour afficher cette section.

4 Dans cette étape de l'interface utilisateur, vous pouvez éventuellement ajouter jusqu'à quatre principaux de service supplémentaires (paires **ID d'application** et **Clé d'application**).

Fournisseurs secondaires

L'ajout de fournisseurs secondaires à un dispositif Horizon Edge est facultatif.

Le fournisseur secondaire doit se trouver dans la même région Azure que le fournisseur principal.

Pour chaque fournisseur secondaire, vous pouvez ajouter jusqu'à cinq principaux de service uniques, pour une capacité Horizon Edge totale maximale de 20 000 VM.

Réseaux

Dans la section **Réseaux**, sélectionnez les sous-réseaux de locataires (poste de travail) à utiliser pour les fournisseurs principaux et secondaires.

Vous pouvez sélectionner les sous-réseaux ultérieurement. Toutefois, le système empêche le déploiement de ressources dans un fournisseur tant qu'Horizon Edge n'est pas associé à au moins un sous-réseau de locataire associé.

Site

Dans la section **Site**, sélectionnez un site existant dans votre environnement ou **Ajouter un nouveau** pour ajouter des informations sur le nouveau site. Pour un nouveau site, spécifiez un nom unique et une description facultative.

Connectivité

Remplissez la section **Connectivité**. Une fois cette étape terminée, passez à l'étape suivante.

1 Sélectionnez le type de connexion réseau à utiliser pour ce dispositif Horizon Edge **Azure Private Link** ou **Internet**.

   Pour plus d'informations sur cette condition requise, reportez-vous à la section Conditions requises pour les abonnements Microsoft Azure.

2 Dans la section **Stockage de l'application App Volumes**, sélectionnez le sous-réseau du point de terminaison privé Azure.

Note Après la configuration du point de terminaison privé, il est recommandé que les utilisateurs finaux se déconnectent de leurs machines virtuelles, puis se reconnectent à celles-ci.

Option	Description
Utiliser le sous-réseau de gestion de la passerelle Edge	Sous-réseau de gestion de la passerelle Edge dans lequel une ressource de point de terminaison privé est créée. Il est recommandé d'utiliser cette option par défaut.
Configurer le sous-réseau personnalisé	Vérifiez que vous avez configuré les conditions préalables. Pour plus d'informations sur ces configurations préalables, reportez-vous à la section Point de terminaison privé Azure pour un compte de stockage d'applications App Volumes. 1 Cochez les cases de confirmation. 2 Sélectionnez un réseau virtuel dans la liste déroulante **vNet de point de terminaison privé**. 3 Sélectionnez le sous-réseau correspondant dans le menu déroulant **Sous-réseau**.

Une fois le dispositif Horizon Edge déployé et le point de terminaison privé créé, l'état du point de terminaison privé est `Configured`. Si l'état est `Not Configured`, le point de terminaison privé peut être configuré à nouveau à l'aide de l'option **Configurer le point de terminaison privé** dans la section **Stockage de l'application App Volumes** du dispositif Horizon Edge. Pour plus d'informations sur l'utilisation de cette option, reportez-vous à la section *Configurer le point de terminaison privé pour un compte de stockage de l'application App Volumes* de la page Détails d'Horizon Edge.

S'il existe des problèmes de connectivité entre l'un des pools de postes de travail existants et les partages de fichiers affectant la distribution d'applications et que vous souhaitez revenir à l'accès au réseau public pour le compte de stockage tant que vous n'avez pas résolu ces problèmes, vous pouvez utiliser l'option **Supprimer le point de terminaison privé**. Cette option supprime le point de terminaison privé configuré et active automatiquement l'accès au réseau public pour le compte de stockage dans le portail Azure. Une fois ces problèmes résolus, vous pouvez configurer le point de terminaison privé à l'aide de l'option **Configurer le point de terminaison privé**.

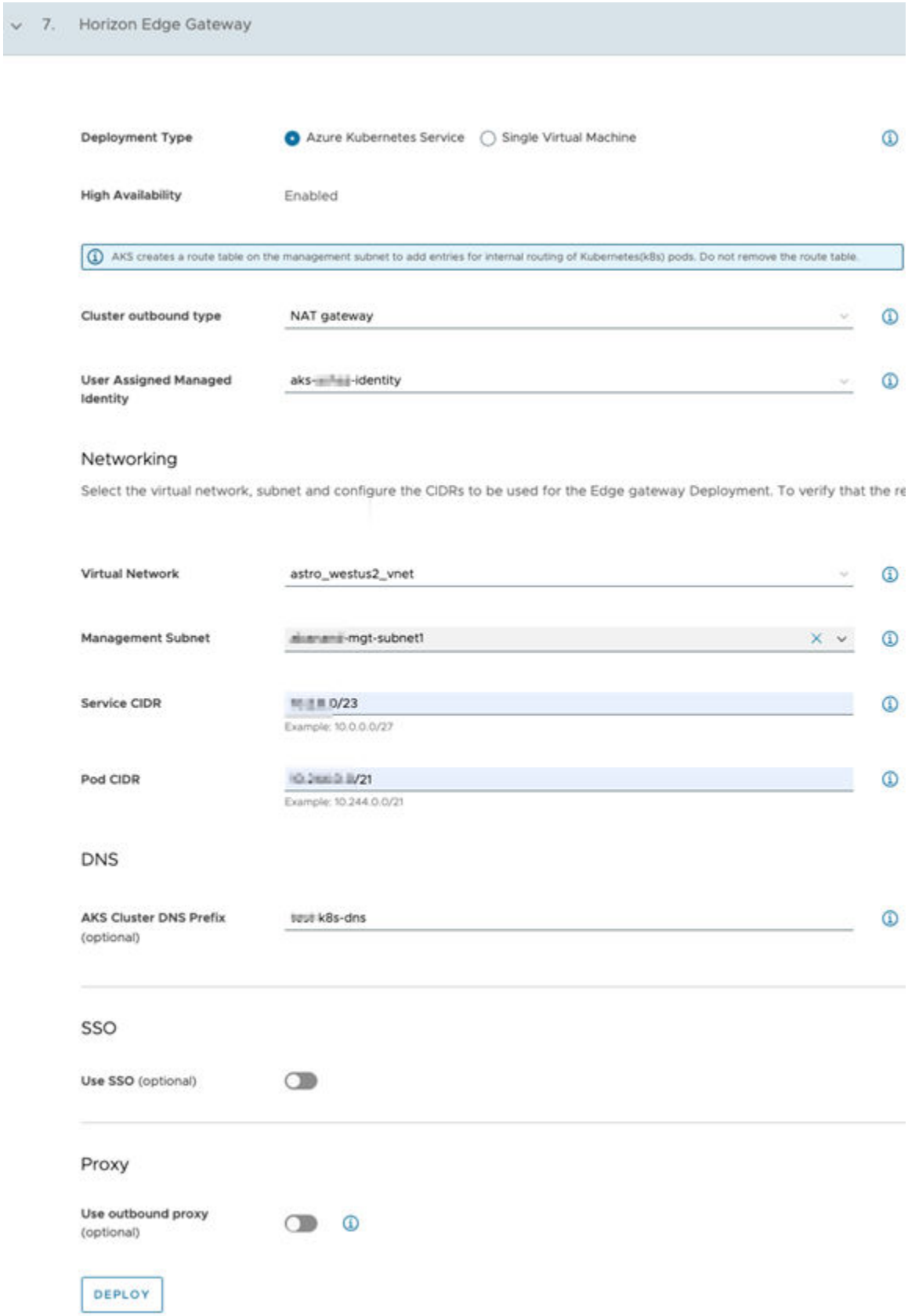
Passerelle Horizon Edge

Dans la section **Passerelle Horizon Edge**, sélectionnez un type de déploiement (**Azure Kubernetes Service** ou **Machine virtuelle unique**).

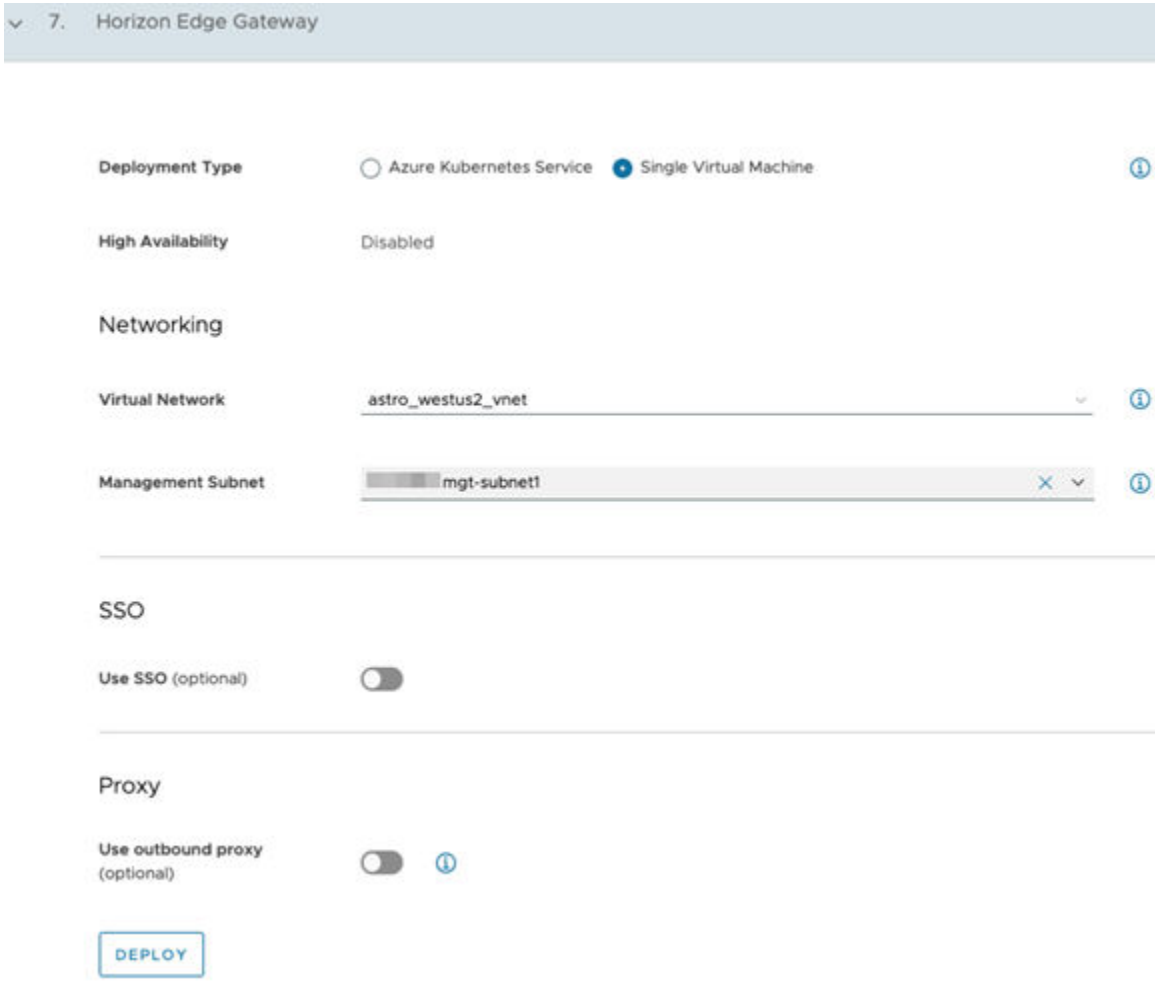
Une fois le type de déploiement sélectionné, configurez les paramètres de la passerelle Passerelle Horizon Edge à l'aide des instructions de ce type de déploiement spécifique, comme suit.

Une fois que vous avez rempli les champs de l'interface utilisateur tels qu'affichés pour le type de déploiement que vous avez choisi, suivez les invites à l'écran.

- **Azure Kubernetes Service** : cette option s'applique à la passerelle Edge (AKS). La capture d'écran suivante montre le type d'information affiché et demandé lorsque vous sélectionnez le type de déploiement **Azure Kubernetes Service**.



- **Machine virtuelle unique** : cette option s'applique à la passerelle Edge (VM). La capture d'écran suivante montre le type d'information affiché et demandé lorsque vous sélectionnez le type de déploiement **Machine virtuelle unique**.



Note L'interface utilisateur affiche une étiquette sur `Haute disponibilité`, en fonction du type de déploiement sélectionné. Vous ne pouvez pas la modifier ultérieurement. Pour le type de déploiement Machine virtuelle unique, la chaîne affichée indique que si la VM n'est pas disponible, les utilisateurs finaux observent le flux de connexion sans expérience de connexion SSO et les données de surveillance des postes de travail ne sont pas enregistrées pendant la période d'indisponibilité de la VM. Pour le type de déploiement Azure Kubernetes Service, la chaîne affichée indique que l'expérience de connexion SSO et la collecte de données de surveillance sont gérées via des services répliqués qui permettent un basculement complet de ces fonctions.

Type de déploiement	Étapes
Azure Kubernetes Service (AKS)	Pour l'option **Azure Kubernetes Service**, 1 Sélectionnez **Type de cluster sortant** dans **Passerelle NAT** et **Routes définies par l'utilisateur**. La sélection par défaut est **Passerelle NAT**. Si vous sélectionnez **Passerelle NAT**, une **Passerelle NAT** doit être associée au sous-réseau de gestion. Si vous sélectionnez **Routes définies par l'utilisateur**, une table de routage doit être associée au sous-réseau de gestion avec la route par défaut configurée avec un type de tronçon suivant du dispositif virtuel. Pour plus d'informations, reportez-vous à la section Conditions requises pour le réseau. En outre, les ports et les URL requis doivent être accessibles. Sinon, le déploiement de dispositifs Edge AKS risque d'échouer. Pour plus d'informations, reportez-vous à la section Rendre les URL de destination appropriées accessibles pour déployer une passerelle Passerelle Horizon Edge dans un environnement Microsoft Azure. AKS ajoute des entrées à la table de routage sur le sous-réseau de gestion pour le routage interne des espaces Kubernetes. Ne supprimez pas les entrées. Vous ne pouvez pas modifier le **Type de cluster sortant** après la création d'un dispositif Horizon Edge. 2 Sélectionnez **Identité gérée attribuée à l'utilisateur** qui dispose des rôles requis. Pour plus d'informations sur **Identité gérée attribuée à l'utilisateur**, reportez-vous à la section Liste de vérification des conditions requises pour le déploiement d'un dispositif Microsoft Azure Edge. 3 Dans la sous-section **Réseau virtuel**, sélectionnez un réseau virtuel pour votre site. Les réseaux virtuels disponibles sont déterminés par la région Microsoft Azure précédemment sélectionnée. Pour créer un réseau virtuel, accédez au portail Microsoft Azure. 4 Sélectionnez le **Sous-réseau de gestion** à utiliser pour les instances de la passerelle Passerelle Horizon Edge et d'Unified Access Gateway. Assurez-vous que le sous-réseau de gestion sélectionné est configuré avec une passerelle NAT, car un dispositif Horizon Edge utilisant un cluster AKS a besoin d'une passerelle NAT pour la connectivité sortante. **Attention** Assurez-vous que le sous-réseau de gestion sélectionné n'est pas utilisé par un autre cluster AKS. Reportez-vous à la section Conditions requises pour le réseau. 5 Dans la zone de texte **CIDR de service**, entrez la plage d'adresses IP pour ce CIDR. Fournissez une plage minimale de /27. Assurez-vous que cette plage CIDR n'est utilisée par aucun élément réseau activé ni connectée au réseau virtuel du sous-réseau de gestion. Assurez-vous que cette plage CIDR n'est pas en conflit avec d'autres adresses IP importantes, telles que l'adresse IP du serveur DNS, l'adresse IP du serveur AD ou les adresses IP d'Unified Access Gateway. 6 Dans la zone de texte **CIDR d'espace**, entrez la plage d'adresses IP pour ce CIDR. Fournissez une plage minimale de /21. Assurez-vous que cette plage CIDR n'est utilisée par aucun élément réseau activé ni connectée au réseau virtuel du sous-réseau de gestion. Assurez-vous que cette plage CIDR n'est pas en conflit avec d'autres adresses IP importantes, telles que l'adresse IP du serveur DNS, l'adresse IP du serveur AD ou les adresses IP d'Unified Access Gateway. 7 Vous pouvez éventuellement ajuster le **Préfixe DNS du cluster AKS** par défaut. 8 Pour activer Single Sign-On pour les ressources qui font partie de ce dispositif Horizon Edge, basculez **Utiliser SSO** et sélectionnez la configuration appropriée dans le menu déroulant **Configurations SSO**.

Type de déploiement	Étapes
	9 Pour acheminer les demandes sortantes via un serveur proxy, activez **Utiliser le proxy sortant**. a Entrez le nom et l'adresse IP du serveur proxy. b Entrez le numéro de port sur lequel le proxy HTTP/TCP écoute le trafic HTTP/HTTPS. c Pour ajouter un certificat pour la communication sécurisée SSL/TLS, sélectionnez **Activer SSL**. Horizon Cloud Service prend uniquement en charge l'authentification SSL. L'authentification par nom d'utilisateur et mot de passe n'est pas prise en charge. d Chargez un certificat de proxy. Horizon Cloud Service prend uniquement en charge les certificats au format PEM. Le certificat doit prendre en charge les noms alternatifs du sujet (SAN, Subject Alternative Name) au lieu des noms communs obsolètes. 10 Cliquez sur **Déployer** pour activer le processus de création d'Horizon Edge.
Machine virtuelle unique	Pour l'option **Machine virtuelle unique**, 1 Dans la sous-section **Réseau virtuel**, sélectionnez un réseau virtuel pour votre site. Les réseaux virtuels disponibles sont déterminés par la région Microsoft Azure précédemment sélectionnée. Pour créer un réseau virtuel, accédez au portail Microsoft Azure. 2 Sélectionnez le **Sous-réseau de gestion** à utiliser pour les instances de la passerelle Passerelle Horizon Edge et d'Unified Access Gateway. 3 Pour activer Single Sign-On pour les ressources qui font partie de ce dispositif Horizon Edge, basculez **Utiliser SSO** et sélectionnez la configuration appropriée dans le menu déroulant **Configurations SSO**. 4 Pour acheminer les demandes sortantes via un serveur proxy, activez **Utiliser le proxy sortant**. a Sélectionnez éventuellement **Paramètres de proxy** d'un autre dispositif Horizon Edge. b Entrez le nom et l'adresse IP du serveur proxy. c Entrez le numéro de port sur lequel le proxy HTTP/TCP écoute le trafic HTTP/HTTPS. d Si le serveur proxy exigeait des informations d'identification, entrez éventuellement **Nom d'utilisateur** et **Mot de passe**. e Pour ajouter un certificat pour la communication sécurisée SSL/TLS, sélectionnez **Activer SSL**. 5 Cliquez sur **Déployer** pour activer le processus de création d'Horizon Edge.

Unified Access Gateway

Dans la section **Unified Access Gateway**, remplissez les champs requis pour votre déploiement.

Une fois que vous avez rempli les champs de l'interface utilisateur, passez à l'étape suivante.

1 Sélectionnez le **Type d'accès**.

Trois options sont disponibles :

- **Accès interne sur un réseau d'entreprise** : si vous souhaitez accéder à vos VM via intranet (réseau d'entreprise interne) uniquement. Un équilibrage de charge de couche 4 sera déployé avec un serveur frontal dans le réseau de poste de travail.

- **Accès externe sur Internet** : si vous souhaitez accéder à vos VM via Internet. Un équilibrage de charge de couche 4 sera déployé avec une adresse IP publique.
- **Accès interne et externe** autorisez l'accès interne et externe.

Note Pour les trois options, l'accès Internet sortant à `*.horizon.vmware.com` est toujours requis. Reportez-vous à la section Conditions requises pour Unified Access Gateway. Lors de l'utilisation de l'option **Accès interne sur un réseau d'entreprise**, vous pouvez appliquer le routage défini par l'utilisateur ou la passerelle NAT au **Sous-réseau de gestion** pour autoriser le trafic sortant. Vous devez configurer l'accès externe sur `*.horizon.vmware.com` sur le réseau DMZ lorsqu'il est défini en externe sur ce dernier.

2 Activez l'option **Adresse IP publique automatique** pour UAG ou désactivez-la si vous préférez utiliser une adresse IP publique manuelle.

Cette option est activée par défaut. Si une adresse IP personnalisée manuelle est sélectionnée, une instance externe d'UAG est déployée avec une adresse IP frontale privée sur le réseau DMZ. Vous devez ensuite gérer le routage à partir de cette adresse IP privée vers l'adresse publique fournie par le client.

Spécifiez le nom de domaine complet pour le déploiement d'Unified Access Gateway.

3 Dans le champ **Type de certificat**, faites votre choix entre **PEM** et **PFX** dans le menu déroulant.

4 Dans le champ **Certificat**, chargez le certificat qui permet aux clients d'approuver les connexions à Unified Access Gateway dans Microsoft Azure.

5 Sélectionnez **Modèle de VM** dans les modèles de VM disponibles dans le menu déroulant.

6 Ajoutez une valeur dans le champ **VM UAG**.

7 Cliquez sur **Enregistrer**.

Étape suivante

Une fois cette procédure terminée, vous devez créer des enregistrements DNS qui correspondent au nom de domaine complet que vous avez entré pour les instances d'Unified Access Gateway. Reportez-vous à la section Configurer les enregistrements DNS requis après le déploiement de la passerelle Passerelle Horizon Edge et d'Unified Access Gateway.

Note Une fois que vous avez terminé le déploiement d'Horizon Cloud et autorisé l'accès des utilisateurs finaux aux postes de travail ou aux applications, notez comment le comportement d'Unified Access Gateway suivant affecte et apporte des avantages aux utilisateurs finaux qui utilisent Horizon HTML Access (client Web).

Pour Unified Access Gateway 2203.1 ou version ultérieure, si une instance d'Unified Access Gateway passe en mode de maintenance ou à un état défectueux et devient inaccessible, les sessions en cours des utilisateurs finaux utilisant Horizon HTML Access se reconnectent à une instance d'Unified Access Gateway saine. La période de reconnexion peut prendre quelques minutes.

Sachez que l'actualisation du certificat SSL pour le dispositif Unified Access Gateway met fin aux sessions des utilisateurs finaux.

Modifier Horizon Edge et Unified Access Gateway

Après avoir déployé Horizon Edge et Unified Access Gateway à l'aide d'Horizon Cloud Service - next-gen, vous pouvez modifier certains champs.

Lors de la modification du dispositif Edge, vous pouvez choisir d'acheminer les demandes sortantes vers Internet via un serveur proxy. Si les détails du proxy sont modifiés, le dispositif Edge peut être redéployé. Cela peut avoir une incidence sur un ou plusieurs des services suivants jusqu'à la fin du redéploiement.

- Single Sign-On pour la connectivité aux postes de travail.

  Vous pouvez toujours vous connecter à vos postes de travail avec votre nom d'utilisateur et votre mot de passe.
- Mise à jour du certificat pour Unified Access Gateway.
- Surveillance de la perte de données pour Workspace ONE Intelligence.
- Collecte de journaux DCT (Data Collection Tool) de l'agent.
- Ajout et réplication d'applications App Volumes sur des partages de fichiers.
- Les tests configurés de type Lancement de ressource simulé dans Surveillance de la disponibilité échouent lors du processus de redéploiement.

Procédure

1. Connectez-vous à Horizon Universal Console.
2. Cliquez sur **Dispositifs Horizon Edge** sur la vignette **Dispositifs Horizon Edge**.

3 Sur la page **Capacité**, sélectionnez le dispositif **Horizon Edge** à modifier et cliquez sur **Modifier**.

4 Vous pouvez **modifier** le **Nom** et la **Description** du dispositif Horizon Edge dans la section **Informations générales**. Cliquez sur **Suivant**.

5 Cochez la **case** pour dédier le fournisseur principal au déploiement de dispositifs de passerelle Horizon : Passerelle Horizon Edge et Unified Access Gateway.

Si la case n'est pas cochée, le fournisseur distribue également des postes de travail et des applications.

6 Vous pouvez éventuellement ajouter une paire nom et valeur pour 10 **Balises de ressources Azure** au maximum.

7 Vous pouvez également ajouter jusqu'à quatre **Principaux de service supplémentaires**.

8 Vous pouvez également ajouter des **fournisseurs secondaires** à ce dispositif Horizon Edge comportant jusqu'à cinq principaux de service uniques par fournisseur, pour une capacité maximale totale de 20 000 VM pour Horizon Edge. Cliquez sur **Suivant**.

9 Dans la section **Réseaux**, **sélectionnez** ou **modifiez** les sous-réseaux de locataire (poste de travail) pour le **Fournisseur principal** et les **Fournisseurs secondaires**. Cliquez sur **Suivant**.

Vous pouvez sélectionner les sous-réseaux ultérieurement. Toutefois, vous ne pourrez pas déployer de ressources dans un fournisseur tant que vous n'aurez pas sélectionné au moins un sous-réseau.

10 Sélectionnez **Site** ou **Ajouter un nouveau site**.

11 Si vous ajoutez un nouveau site, entrez **Nom du site**. Ajoutez éventuellement **Description**. Cliquez sur **Suivant**.

12 Cliquez sur **Suivant** pour la section **Connectivité**.

13 Dans la section **Passerelle Horizon Edge**, à l'aide des instructions qui suivent, modifiez les paramètres de la passerelle Passerelle Horizon Edge en fonction de vos objectifs et du type de déploiement sélectionné (**Azure Kubernetes Service** ou **Machine virtuelle unique**).

Note Si vous avez déployé une passerelle Edge (AKS) et que vous n'avez pas activé la haute disponibilité, activez maintenant l'option **Activer la haute disponibilité**.

a Pour activer Single Sign-On pour les ressources qui font partie de ce dispositif Horizon Edge, basculez **Utiliser SSO** et sélectionnez la configuration appropriée dans le menu déroulant **Configurations SSO**.

b Si vous le souhaitez, reconfigurez les paramètres du proxy.

Important L'activation de l'option **Utiliser le proxy sortant** peut avoir une incidence sur un ou plusieurs des services suivants jusqu'à la fin du redéploiement.

- Single Sign-On pour la connectivité aux postes de travail.

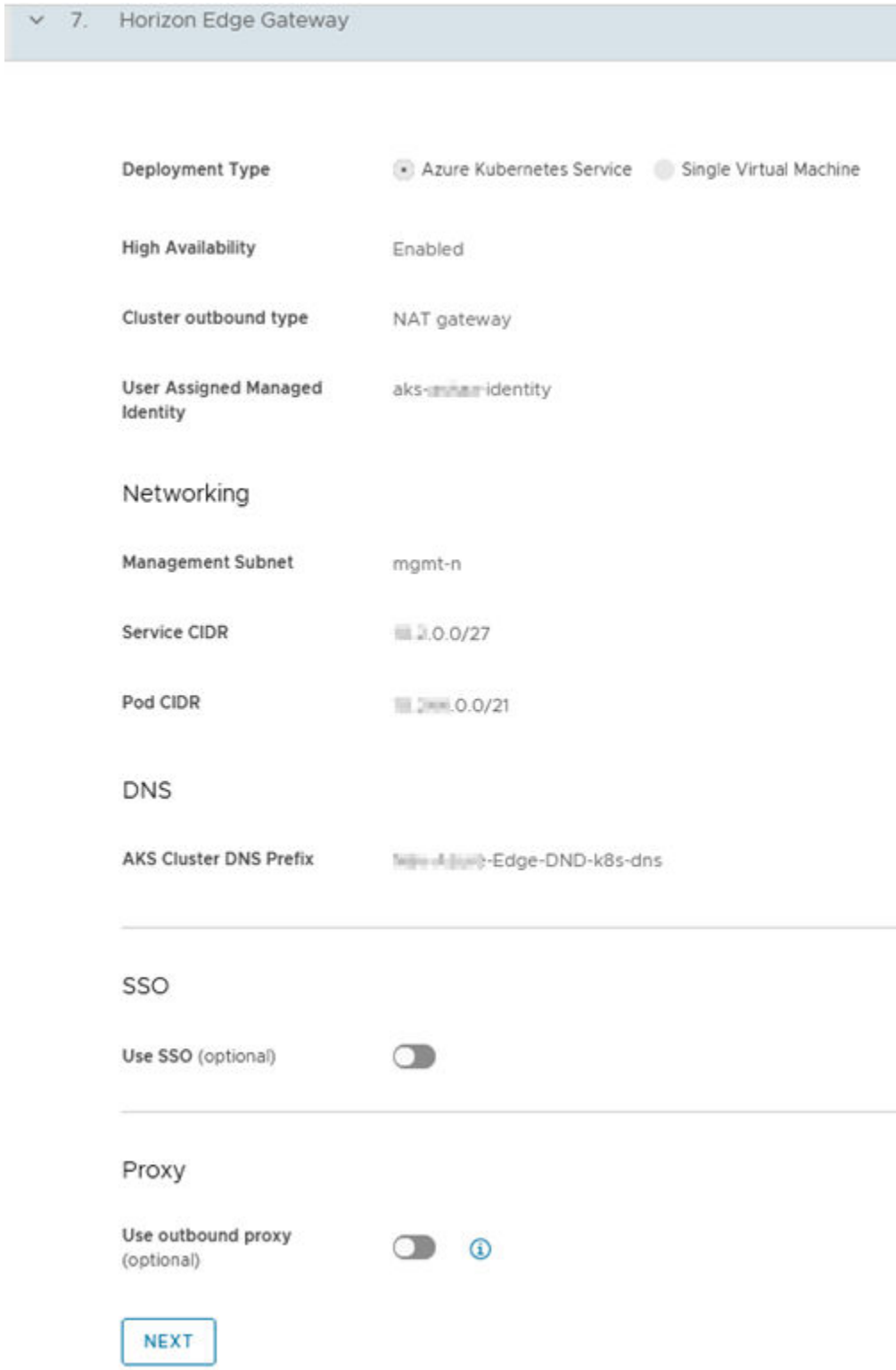
  Vous pouvez toujours vous connecter à vos postes de travail avec votre nom d'utilisateur et votre mot de passe.
- Mise à jour du certificat pour Universal Access Gateway.
- Surveillance de la perte de données pour Workspace ONE Intelligence.
- Collecte de journaux DCT (Data Collection Tool) de l'agent.
- Ajout et réplication d'applications App Volumes sur des partages de fichiers.
- Il est possible que les tests configurés de type Lancement de ressource simulé dans Surveillance de la disponibilité échouent lors du processus de redéploiement.

c Cliquez sur **Suivant**.

La plupart des options ne sont pas modifiables, y compris les options **Type de déploiement** et **Haute disponibilité**.

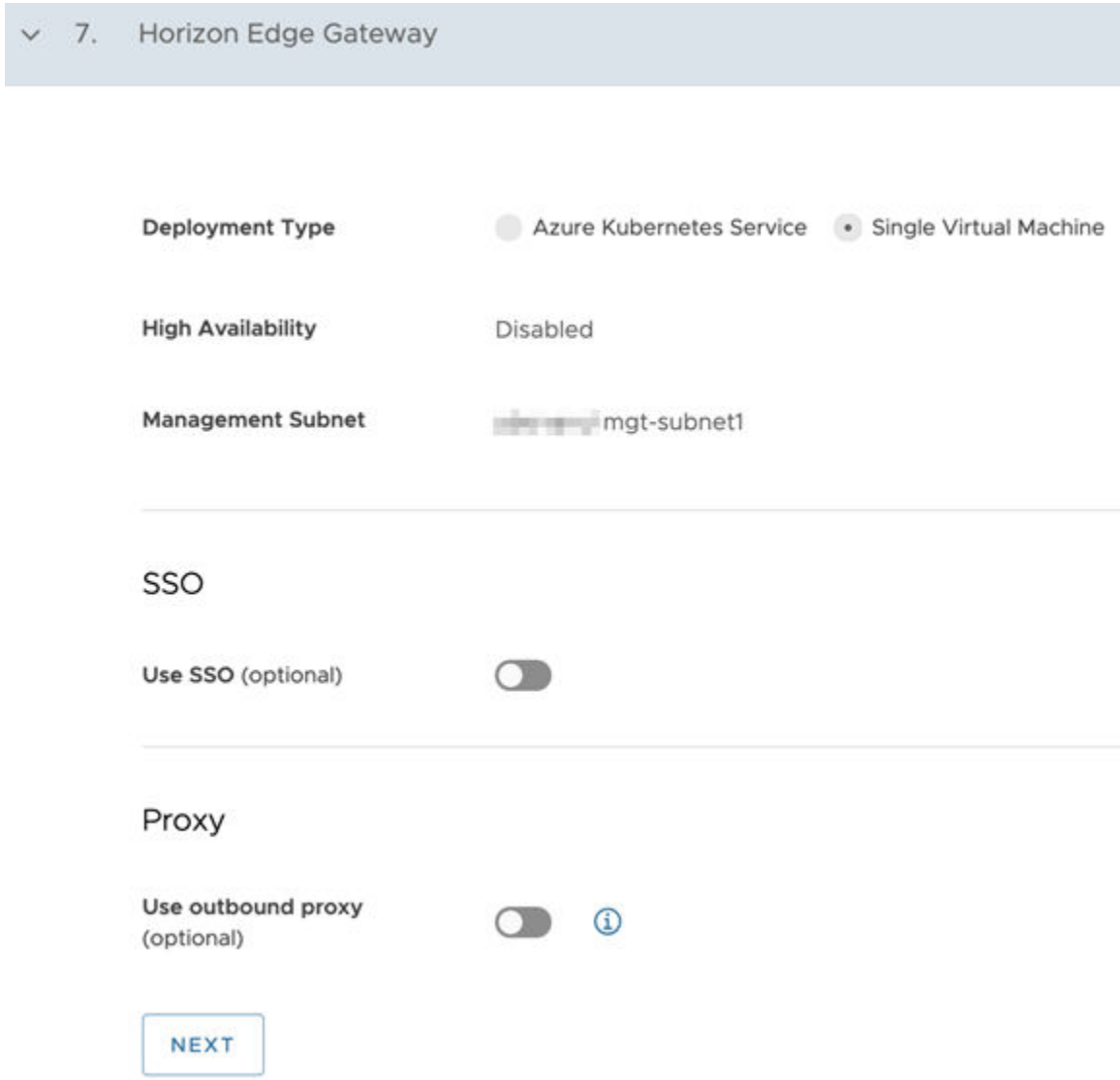
- **Azure Kubernetes Service**

  Cette option s'applique à la passerelle Edge (AKS). La capture d'écran suivante montre le type d'information affiché lorsque vous sélectionnez le type de déploiement **Azure Kubernetes Service**.



- **Machine virtuelle unique**

  Cette option s'applique à la passerelle Edge (VM). La capture d'écran suivante montre le type d'information affiché lorsque vous sélectionnez le type de déploiement **Machine virtuelle unique**.



14 Dans la section **Unified Access Gateway**, activez l'option **Adresse IP publique automatique** pour UAG ou désactivez-la si vous préférez utiliser une adresse IP publique manuelle.

   Cette option est activée par défaut. Si une adresse IP personnalisée manuelle est sélectionnée, une instance externe d'UAG est déployée avec une adresse IP frontale privée sur le réseau DMZ. Vous devez ensuite gérer le routage à partir de cette adresse IP privée vers l'adresse publique fournie par le client.

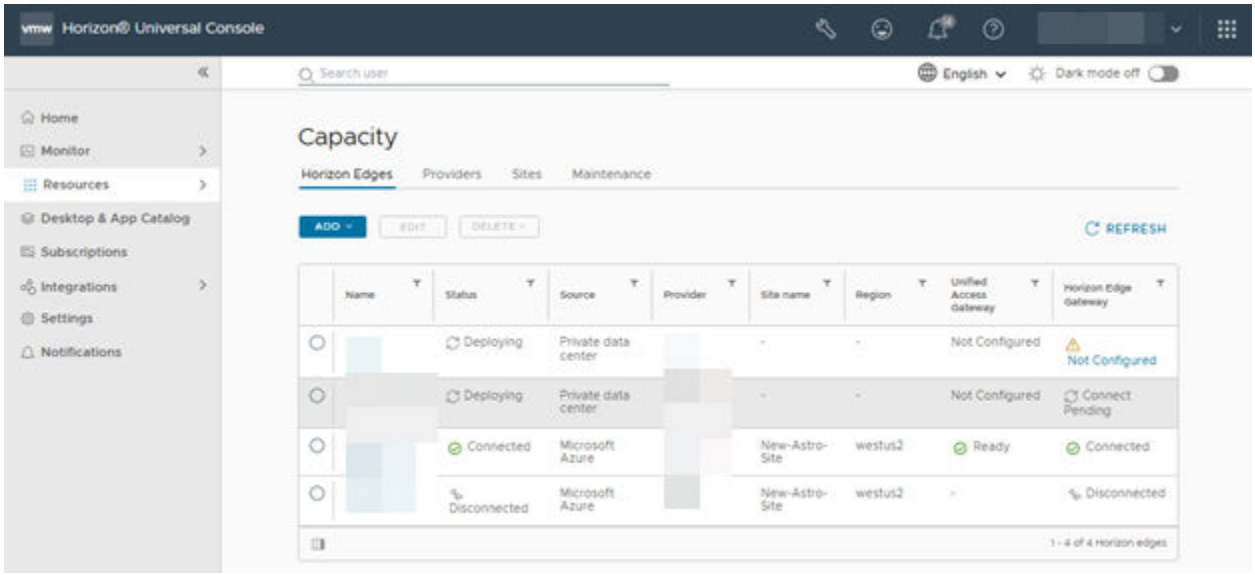
15 Cliquez sur **Enregistrer**.

Détails d'Horizon Edge

Après avoir ajouté un ou plusieurs dispositifs Dispositifs Horizon Edge, vous pouvez utiliser Horizon Universal Console pour accéder à la page Dispositifs Horizon Edge sur laquelle vous pouvez afficher les données générales d'une liste de dispositifs Dispositifs Horizon Edge. Vous pouvez également cliquer sur le nom d'un dispositif Horizon Edge spécifique pour afficher des informations détaillées sur ce Horizon Edge spécifique.

Afficher les dispositifs Dispositifs Horizon Edge déployés et effectuer des actions sur un dispositif Horizon Edge spécifique

La page Dispositifs Dispositifs Horizon Edge fournit des informations de base sur chaque dispositif Horizon Edge de votre déploiement. Cette page permet également d'ajouter, de modifier et de supprimer des dispositifs Dispositifs Horizon Edge.



Pour afficher la page Dispositifs Dispositifs Horizon Edge, sélectionnez **Ressources > Capacité**.

La page Dispositifs Horizon Edge affiche un tableau de vos dispositifs Dispositifs Horizon Edge.

Info-bulle

- Vous pouvez modifier la manière dont la page présente vos dispositifs Dispositifs Horizon Edge en utilisant l'un des nombreux filtres disponibles dans les en-têtes de colonnes du tableau, tels que **Nom**, **État** et **Passerelle Horizon Edge**, entre autres.
- La colonne **État** affiche l'état du déploiement de chaque dispositif Horizon Edge.
- La colonne **Passerelle Horizon Edge** affiche l'état de chaque **Passerelle Horizon Edge**.
- La colonne **Unified Access Gateway** affiche l'état d'Unified Access Gateway associé à chaque **Passerelle Horizon Edge**.
- La colonne **Source** répertorie le type de fournisseur de chaque instance d'Horizon Edge. Par exemple, « Microsoft Azure » s'adresse à un dispositif Microsoft Azure Edge et « Centre de données privé » est destiné à un dispositif Horizon 8 Edge. Les types de fournisseurs qui peuvent s'afficher dans la colonne **Source** dépendent du type de licence dont vous disposez et du type de dispositif Horizon Edge que vous avez déployé précédemment.

Fournisseurs

Vous pouvez ajouter ou modifier un type de fournisseur associé à un dispositif Horizon Edge, une image ou un pool.

1 Connectez-vous à Horizon Universal Console.

- Horizon Edge : accédez à **Ressources > Capacité > Fournisseurs > Ajouter** et sélectionnez un type de fournisseur dans la liste déroulante.
- Image : cliquez sur **Images**, puis sur **Démarrer** et sélectionnez un fournisseur dans la liste déroulante.
- Pool : cliquez sur **Pools**, puis sur **Démarrer** et sélectionnez le fournisseur dans la liste déroulante.

Fonctionnalité	Type de fournisseur
Horizon Edge	Microsoft Azure et Windows 365
Image	Microsoft Azure et Horizon 8
Pool	Microsoft Azure

2 Entrez et enregistrez les détails du type de fournisseur que vous avez sélectionné.

3 Pour modifier un fournisseur, sélectionnez-le dans la liste, puis cliquez sur **Modifier**.

Toutes les valeurs ne sont pas modifiables. Les valeurs qui ne sont pas modifiables varient selon le type de fournisseur.

4 Pour afficher les détails d'un fournisseur, cliquez sur la double flèche en regard du fournisseur.

Le volet de droite affiche les détails du fournisseur. Le type d'informations répertoriées varie selon le type de fournisseur.

5 Pour supprimer un fournisseur, sélectionnez-le dans la liste, puis cliquez sur **Supprimer**.

Afficher les détails et effectuer des actions sur un dispositif Horizon Edge spécifique

Pour afficher des données sur un dispositif Horizon Edge spécifique ou effectuer des actions (telles que la modification ou la suppression) sur celui-ci, cliquez sur le nom du dispositif Horizon Edge sur la page Dispositifs Dispositifs Horizon Edge.

La page de détails d'un dispositif Horizon Edge spécifique fournit diverses informations relatives au dispositif Horizon Edge, notamment des informations sur le fournisseur, Unified Access Gateway, Passerelle Horizon Edge, etc. Cependant, les informations disponibles sur la page de détails diffèrent considérablement selon que le dispositif Horizon Edge est déployé dans un environnement Microsoft Azure ou dans un environnement Horizon 8.

Différence significative sur la page de détails d'un dispositif Microsoft Azure Edge et d'un dispositif Horizon 8 Edge : un dispositif Horizon 8 Edge inclut les onglets **Résumé**, **Surveillance de l'infrastructure** et **Fonctionnalités**. Pour un dispositif Microsoft Azure Edge, la page de détails contient des informations récapitulatives directement sur la page, mais pas d'informations sur la surveillance de l'infrastructure pour le moment.

Les captures d'écran suivantes affichent une partie de la page de détails d'Horizon Edge des différents types de dispositifs Horizon Edge.

Figure 5-1. Microsoft Azure Edge

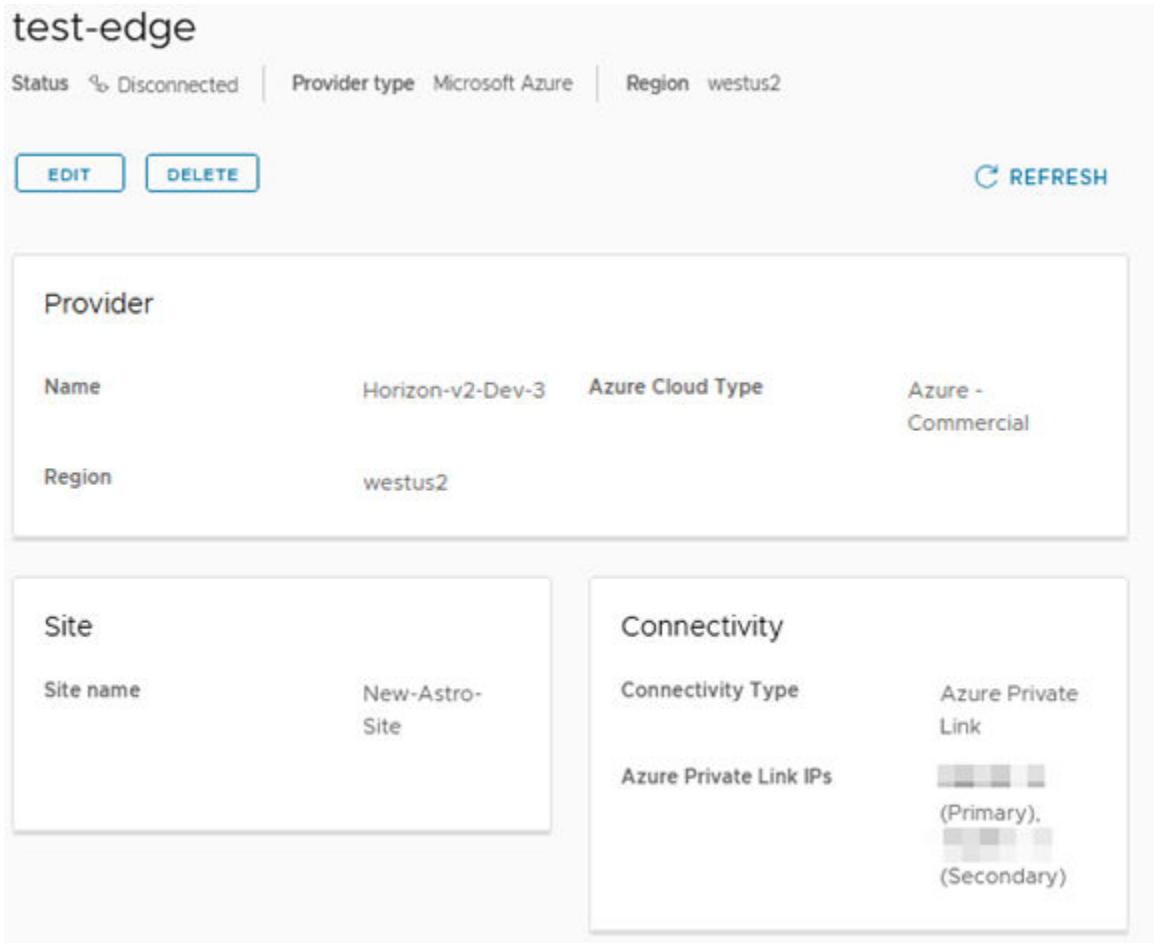
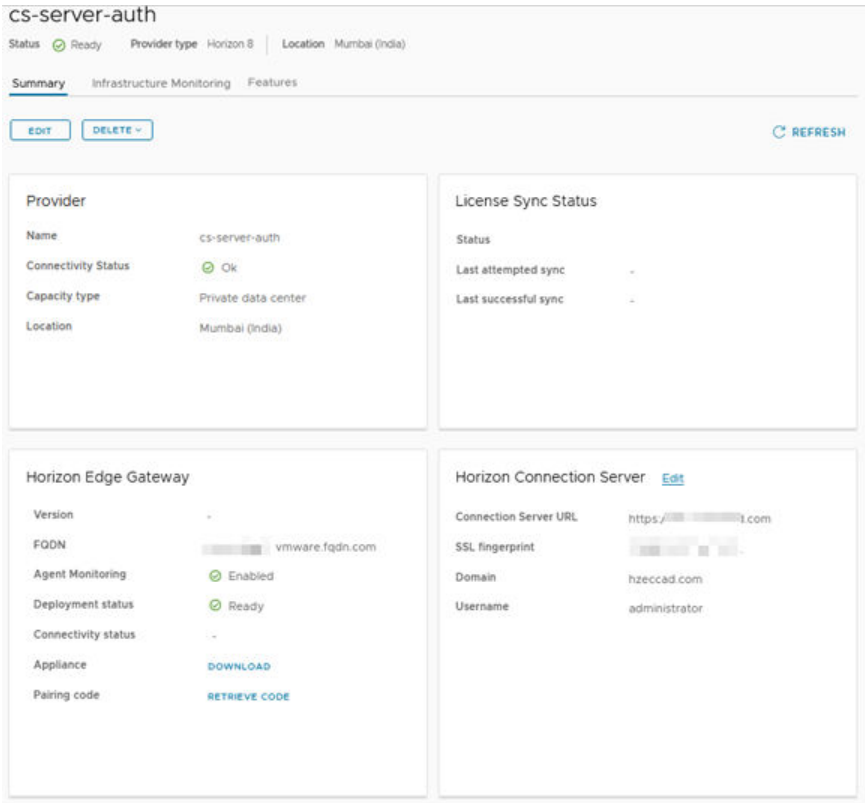


Figure 5-2. Horizon 8 Edge



Pour un dispositif Horizon 8 Edge, sur la page **Résumé**, vous pouvez ajouter des instances d'UAG à surveiller en procédant comme suit.

1 Dans la section **Unified Access Gateway**, cliquez sur **Ajouter des instances d'Unified Access Gateway pour la surveillance**.

2 Sur la page **Instances d'Unified Access Gateway**, dans la section **Équilibrage de charge**, ajoutez un **Nom** et un **Nom de domaine complet ou une adresse IP**, puis cliquez sur **Enregistrer**.

3 Dans la section Passerelles, vous pouvez ajouter et enregistrer des informations d'équilibrage de charge pour ajouter les passerelles. Cliquez sur **Ajouter** pour **ajouter Unified Access Gateway**.

4 Ajoutez un **Nom**, un **Point de terminaison de gestion** qui est le nom de domaine complet, l'adresse IP ou le nom d'hôte du point de terminaison de gestion de la passerelle, le **Nom d'utilisateur** et le **Mot de passe** pour United Access Gateway.

Il est possible d'ajouter et de charger un certificat signé par une autorité de certification ou un certificat auto-signé dans cette instance d'UAG. Pour un certificat auto-signé, l'utilisateur reçoit une notification pour vérifier et confirmer les détails du certificat. L'utilisateur doit cliquer sur Confirmer s'il approuve ce certificat. Sinon, une erreur de surveillance se produit. Si l'utilisateur clique sur Confirmer, il ne reçoit pas de notification pour confirmation la prochaine fois.

Note Les certificats signés par une autorité de certification sont recommandés pour tous les environnements de production, tandis que les certificats auto-signés sont recommandés uniquement pour la validation technique ou les tests.

5 Cliquez sur **Enregistrer**.

Une fois la tâche précédente terminée, vous pouvez surveiller l'instance d'UAG que vous venez d'ajouter dans l'onglet **Surveillance de l'infrastructure**. Pour plus d'informations sur les données présentées dans l'onglet **Surveillance de l'infrastructure** disponibles pour un dispositif Horizon 8 Edge, reportez-vous à la section Surveillance des données d'infrastructure d'Passerelle Horizon Edge et d'Unified Access Gateway dans un environnement Horizon 8.

Configurer un point de terminaison privé pour un compte de stockage de l'application App Volumes

Si l'état du point de terminaison privé d'un compte de stockage est `Not Configured`, utilisez l'option **Configurer le point de terminaison privé** pour configurer un point de terminaison privé pour le compte de stockage.

Note Après la configuration du point de terminaison privé, il est recommandé que les utilisateurs finaux se déconnectent de leurs machines virtuelles, puis se reconnectent à celles-ci.

1 Dans la console Horizon Universal Console, accédez à **Ressources > Capacité**.

2 Cliquez sur le dispositif Horizon Edge dans lequel le point de terminaison privé doit être configuré.

3 Accédez à la section **Stockage de l'application App Volumes**.

4 Dans le tableau **Comptes de stockage Azure**, cliquez sur l'icône de dépassement de capacité (trois points verticaux) du compte de stockage dont l'état du point de terminaison privé est `Not Configured` ou `Disconnected`.

5 Cliquez sur **Configurer le point de terminaison privé**.

6 Dans la fenêtre **Configurer le point de terminaison privé du compte de stockage**, assurez-vous que toutes les conditions requises sont remplies et cochez la case **Autorisations**.

Pour plus d'informations sur ces conditions requises, reportez-vous à la section Point de terminaison privé Azure pour un compte de stockage d'applications App Volumes.

7 Sélectionnez un réseau virtuel dans la zone déroulante **vNet de point de terminaison privé**.

8 Sélectionnez un sous-réseau dans la zone déroulante **Sous-réseau**.

9 Cliquez sur **Enregistrer**.

L'état du point de terminaison privé est `Connected`.

Une fois le point de terminaison privé configuré pour un compte de stockage dans un déploiement d'Horizon Edge existant, procédez comme suit avant de désactiver l'accès au réseau public du compte de stockage :

- Assurez-vous que la connectivité entre le compte de stockage et Horizon Edge, et le compte de stockage et chacun des pools de postes de travail est réussie.
- Les utilisateurs finaux disposant de pièces jointes d'applications existantes, qui ont été attribuées avant la configuration du point de terminaison privé, doivent se déconnecter de leurs machines virtuelles.

Dans le portail Azure, accédez à la section **Comptes de stockage > Sécurité + mise en réseau > Pare-feu et réseaux virtuels** et définissez l'option **Accès au réseau public** pour le compte de stockage spécifique sur `Disabled`. Pour plus d'informations, reportez-vous à la documentation de *Microsoft* correspondante.

S'il existe des problèmes de connectivité entre l'un des pools de postes de travail existants et les partages de fichiers affectant la distribution d'applications et que vous souhaitez revenir à l'accès au réseau public pour le compte de stockage tant que vous n'avez pas résolu ces problèmes, vous pouvez utiliser l'option **Supprimer le point de terminaison privé**. Cette option supprime le point de terminaison privé configuré et active automatiquement l'accès au réseau public pour le compte de stockage dans le portail Azure. Une fois ces problèmes résolus, vous pouvez configurer le point de terminaison privé à l'aide de l'option **Configurer le point de terminaison privé**.

Mettre à jour les paramètres d'Unified Access Gateway ou d'Horizon Connection Server dans Horizon Cloud Service - next-gen

Vous pouvez apporter des modifications aux paramètres d'Horizon Cloud Service - next-gen spécifiés pour une configuration existante d'Unified Access Gateway ou de la passerelle Passerelle Horizon Edge directement depuis la console Horizon Universal Console.

À l'aide de la page **Ressources > Capacité** de la console Horizon Universal Console, vous pouvez apporter des modifications à une configuration spécifiée d'Unified Access Gateway ou de la passerelle Passerelle Horizon Edge spécifiée dans la séquence de menus de l'indicateur d'étape.

Pour obtenir des informations complémentaires, reportez-vous à Réessayer le déploiement d'Horizon Edge et à Réessayer le déploiement d'Unified Access Gateway dans Horizon Cloud Service - next-gen.

Vous pouvez ouvrir et modifier le paramètre d'Unified Access Gateway pour les dispositifs Microsoft Azure Edge ou Horizon Connection Server pour les dispositifs Horizon Edge, comme indiqué dans les scénarios suivants.

Réessayez Unified Access Gateway à partir de la page de listes des dispositifs Edge lorsque l'état est ÉCHEC

Vous pouvez ouvrir et modifier l'étape de configuration d'Unified Access Gateway dans la séquence de menus de l'indicateur d'étape Microsoft Azure Edge à partir de la page de listes **Ressources > Capacité > Dispositifs Edge**.

1 Connectez-vous à Horizon Cloud Service - next-gen et affichez la console Horizon Universal Console.

2 Accédez à la page de listes **Ressources > Capacité > Dispositifs Edge**.

3 Cliquez sur l'icône **Échec** du déploiement d'Unified Access Gateway ayant échoué pour afficher l'aide de signpost, puis cliquez sur **Réessayer**.

La page de modification de Microsoft Azure Edge s'ouvre à l'étape Unified Access Gateway, ce qui vous permet de modifier les paramètres du dispositif Edge et de recommencer le déploiement.

Réessayez Unified Access Gateway à partir de la page de détails du dispositif Edge lorsque l'état est ÉCHEC

Vous pouvez ouvrir et modifier l'étape de configuration d'Unified Access Gateway dans la séquence de menus de l'indicateur d'étape Microsoft Azure Edge à partir de la page de détails **Ressources > Capacité > Dispositifs Edge**.

1 Connectez-vous à Horizon Cloud Service - next-gen et affichez la console Horizon Universal Console.

2 Accédez à la page de détails **Ressources > Capacité > Dispositifs Edge** pour le déploiement ayant échoué.

3 Cliquez sur **Réessayer** à partir de l'alerte d'erreur dans la carte Unified Access Gateway.

La page de modification de Microsoft Azure Edge s'ouvre à l'étape Unified Access Gateway, ce qui vous permet de modifier les paramètres du dispositif Edge et de recommencer le déploiement.

Configurer Unified Access Gateway à partir de la page de listes des dispositifs Edge

Vous pouvez ouvrir et modifier l'étape de configuration d'Unified Access Gateway dans la séquence de menus de l'indicateur d'étape Microsoft Azure Edge à partir de la page de liste des dispositifs Edge.

1 Connectez-vous à Horizon Cloud Service - next-gen et affichez la console Horizon Universal Console.

2 Accédez à la page de liste **Ressources > Capacité > Dispositifs Edge**.

3 Cliquez sur le lien **Configurer** dans la colonne Unified Access Gateway.

La page de modification de Microsoft Azure Edge s'ouvre à l'étape Unified Access Gateway, ce qui vous permet de modifier les paramètres du dispositif Edge.

Configurer Unified Access Gateway à partir de la page de détails du dispositif Edge

Vous pouvez ouvrir et modifier l'étape de configuration d'Unified Access Gateway dans la séquence de menus de l'indicateur d'étape Microsoft Azure Edge à partir de la page de détails **Capacité > Edge**.

1 Connectez-vous à Horizon Cloud Service - next-gen et affichez la console Horizon Universal Console.

2 Accédez à la page de détails **Ressources > Capacité > Dispositifs Edge** qui ne contient aucun déploiement d'Unified Access Gateway.

3 Cliquez sur **Ajouter** dans la carte Unified Access Gateway.

La page Microsoft Azure Edge s'ouvre à l'étape Unified Access Gateway, ce qui vous permet de configurer les paramètres du dispositif Edge.

Modifier Unified Access Gateway sur la page de détails du dispositif Edge

Vous pouvez ouvrir et modifier l'étape de configuration d'Unified Access Gateway dans la séquence de menus de l'indicateur d'étape Microsoft Azure Edge à partir de la page de détails **Ressources > Capacité > Dispositifs Edge** pour un déploiement à l'état Prêt.

1 Connectez-vous à Horizon Cloud Service - next-gen et affichez la console Horizon Universal Console.

2 Accédez à la page de détails **Ressources > Capacité > Dispositifs Edge** avec le déploiement d'Unified Access Gateway à l'état Prêt.

3 Cliquez sur **Modifier** dans la carte Unified Access Gateway.

La page Microsoft Azure Edge s'ouvre à l'étape Unified Access Gateway, ce qui vous permet de modifier les paramètres du dispositif Edge.

Configurer Horizon Connection Server à partir de la page de listes des dispositifs Edge

Vous pouvez ouvrir et modifier l'étape de configuration d'Horizon Connection Server dans la séquence de menus de l'indicateur d'étape Horizon 8 Edge à partir de la page de détails **Ressources > Capacité > Dispositifs Edge**.

1 Connectez-vous à Horizon Cloud Service - next-gen et affichez la console Horizon Universal Console.

2 Accédez à la page de listes **Ressources > Capacité > Dispositifs Edge**.

3 Cliquez sur **Non configuré** dans la colonne Passerelle Horizon Edge de la carte Horizon Connection Server pour afficher l'aide de signpost, puis cliquez sur **Configurer**.

La page Modifier la vue s'ouvre à l'étape Serveur de connexion, ce qui vous permet de modifier les paramètres du dispositif Edge.

Configurer Horizon Connection Server à partir de la page de présentation

Vous pouvez ouvrir et modifier l'étape de configuration d'Horizon Connection Server dans la séquence de menus de l'indicateur d'étape Horizon 8 Edge à partir de la page de présentation **Ressources > Capacité > Dispositifs Edge**.

1 Connectez-vous à Horizon Cloud Service - next-gen et affichez la console Horizon Universal Console.

2 Accédez à la page de présentation **Ressources > Capacité > Dispositifs Edge**.

3 Cliquez sur **Configurer** dans la carte Horizon Connection Server.

La page Modifier la vue s'ouvre à l'étape Serveur de connexion, ce qui vous permet de modifier les paramètres du dispositif Edge.

Modifier Horizon Connection Server à partir de la page de résumé

Vous pouvez ouvrir et modifier l'étape de configuration d'Horizon Connection Server dans la séquence de menus de l'indicateur d'étape Horizon 8 Edge à partir de la page de résumé **Ressources > Capacité > Dispositifs Edge**.

1 Connectez-vous à Horizon Cloud Service - next-gen et affichez la console Horizon Universal Console.

2 Accédez à la page de résumé **Ressources > Capacité > Dispositifs Edge**.

3 Cliquez sur **Modifier** dans la carte Horizon Connection Server.

La page Modifier la vue s'ouvre à l'étape Serveur de connexion, ce qui vous permet de modifier les paramètres du dispositif Edge.

Réessayer le déploiement d'Horizon Edge

En cas d'échec de votre déploiement d'Horizon Edge, vous pouvez le réessayer sans devoir supprimer ni créer un déploiement d'Horizon Edge.

Procédure

1 Sur la page **Accueil**, cliquez sur **Dispositifs Horizon Edge** sur la vignette **Dispositifs Horizon Edge**.

2 Sur la page **Capacité**, cliquez sur le signpost sur **Échec de la création** de **Passerelle Horizon Edge** pour afficher les erreurs.

3 Corrigez les erreurs, puis cliquez sur **Réessayer** pour retenter le déploiement du dispositif Edge.

4 Cliquez sur **Afficher les journaux** pour afficher **Journal d'activité**.

5 Cliquez sur **Afficher tout** pour afficher la liste des erreurs.

Si l'option **Réessayer** échoue, une notification s'affiche sur la page **Capacité** qui indique le motif de l'échec.

Réessayer le déploiement d'Unified Access Gateway dans Horizon Cloud Service - next-gen

En cas d'échec de votre déploiement d'Unified Access Gateway, vous pouvez le réessayer sans devoir supprimer ni créer une instance d'Unified Access Gateway dans Horizon Cloud Service - next-gen.

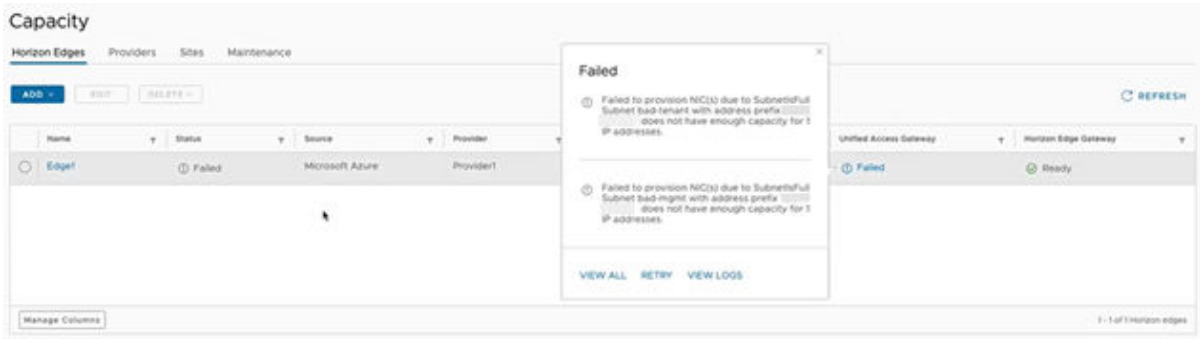
Votre déploiement d'Unified Access Gateway peut échouer en raison d'informations de mise en réseau inexactes. Vous avez la possibilité d'entrer à nouveau les informations de mise en réseau, telles que le réseau virtuel, le sous-réseau de VM, le sous-réseau de gestion et le sous-réseau de zone DMZ, puis de réessayer Unified Access Gateway.

Horizon Universal Console propose plusieurs façons de réessayer Unified Access Gateway en plus de la méthode décrite dans la procédure suivante. Par exemple, sur la page d'accueil, lorsque vous sélectionnez **Dispositifs Horizon Edge** et que vous cliquez sur le nom d'un dispositif Horizon Edge qui affiche **En échec** comme état dans la colonne **Unified Access Gateway**, vous pouvez faire défiler cette page de détails d'Horizon Edge vers le bas jusqu'à la section Unified Access Gateway. Dans cette section Unified Access Gateway, vous avez également la possibilité de cliquer sur **Réessayer** pour réessayer le déploiement d'Unified Access Gateway.

Procédure

1 Connectez-vous à Horizon Cloud Service - next-gen et cliquez sur Dispositifs Horizon Edge.

2 Cliquez sur le signpost de l'instance d'Unified Access Gateway dont l'état est **Échec**.



3 Cliquez sur **Tout afficher** pour afficher la liste complète des erreurs.

Le bouton **Afficher tout** s'affiche s'il y a plus de deux erreurs.

4 Cliquez sur **Réessayer**.

La page de modification de Microsoft Azure Edge s'ouvre à l'étape Unified Access Gateway.

5 Modifiez les valeurs appropriées, puis cliquez sur **Enregistrer**.

6 Si vous choisissez d'accéder à la page **Journal d'activité**, vous pouvez cliquer sur **Afficher les journaux**.

Supprimer un dispositif Edge

Vous pouvez supprimer le dispositif Edge, après quoi toutes les ressources du dispositif Edge seront supprimées.

Conditions préalables

- Les groupes de pools dans le dispositif Edge sont supprimés.
- Les pools du dispositif Edge sont supprimés.
- Les images du dispositif Edge sont supprimées.
- UAG est supprimé.

Procédure

1. Sélectionnez le dispositif Edge à supprimer sur la page Capacité.
2. Cliquez sur **Supprimer** et sélectionnez **Passerelle Horizon Edge** dans le menu déroulant.
3. Cliquez sur **Supprimer** dans la boîte de dialogue **Confirmer la suppression** pour supprimer tous les partages de fichiers de volumes d'application.

   Lorsque vous supprimez le dispositif Edge, toutes les ressources associées au dispositif Edge comme stockage d'applications (partages de fichiers), et Applications et modules App Volumes, sont supprimées en arrière-plan.

Configurer les enregistrements DNS requis après le déploiement de la passerelle Passerelle Horizon Edge et d'Unified Access Gateway

Après avoir déployé vos instances de la Passerelle Horizon Edge et d'Unified Access Gateway, créez des enregistrements DNS qui correspondent aux noms de domaine complets sur les instances d'Unified Access Gateway.

Effectuez cette tâche après avoir déployé les instances de la passerelle Passerelle Horizon Edge et d'Unified Access Gateway. Reportez-vous à la section Déploiement d'un dispositif Microsoft Azure Edge.

Note Si vous disposez de plusieurs clusters Unified Access Gateway, configurez le serveur DNS pour tous les réseaux virtuels non appairés.

La configuration du serveur DNS pour tous les réseaux virtuels non appairés s'applique également à l'avenir si vous créez d'autres groupes de pools dans lesquels vous devez spécifier le sous-réseau.

Conditions préalables

Obtenez les adresses IP et les noms de domaine complets suivants à l'aide d'Horizon Universal Console. Par exemple, sélectionnez **Ressources > Capacité**, cliquez sur le nom de l'instance de la passerelle Passerelle Horizon Edge à configurer, puis notez les adresses IP et les noms de domaine complets correspondants comme suit.

Dans la section Unified Access Gateway, obtenez les adresses IP de l'équilibrage de charge et le nom de domaine complet associé à l'instance d'Unified Access Gateway. La liste inclut des étiquettes pour le ou les types d'équilibrage de charge que vous avez configurés lorsque vous avez déployé l'instance de la passerelle Passerelle Horizon Edge. Si vous avez configuré un équilibrage de charge interne et externe, les étiquettes associées à l'équilibrage de charge correspondantes s'affichent dans la section Unified Access Gateway.

Étiquette	Description
Adresse IP de l'équilibrage de charge	Adresse IP de l'équilibrage de charge public (externe)
Adresse IP privée de l'équilibrage de charge	Adresse IP de l'équilibrage de charge interne
Nom de domaine complet	Nom de domaine complet des instances d'Unified Access Gateway. Ce nom de domaine complet peut être utilisé pour les adresses IP d'équilibrage de charge interne et externe.

Procédure

1 Pour Unified Access Gateway, effectuez l'étape appropriée qui suit, en fonction de la configuration de votre équilibrage de charge :

   - Si vous avez sélectionné **Accès externe sur Internet**

     Créez un enregistrement DNS et utilisez le nom de domaine complet pour pointer vers l'adresse IP publique de l'équilibrage de charge externe dans la configuration d'Unified Access Gateway.

   - Si vous avez sélectionné **Accès interne sur un réseau d'entreprise**

     Créez un enregistrement DNS et utilisez le nom de domaine complet pour pointer vers l'adresse IP privée de l'équilibrage de charge interne dans la configuration d'Unified Access Gateway.

     Cette adresse IP privée de l'équilibrage de charge se trouve dans le sous-réseau de poste de travail (locataire) que vous avez sélectionné lors du déploiement du cluster Unified Access Gateway.

   - Si vous avez sélectionné **Accès interne et externe**

     Dans votre DNS interne, mappez le nom de domaine complet Unified Access Gateway à l'adresse IP privée de l'équilibrage de charge interne.

     En outre, dans votre DNS externe, mappez le nom de domaine complet Unified Access Gateway à l'adresse IP publique de l'équilibrage de charge externe.

2 Vérifiez toutes les mises à jour que vous effectuez.

Configuration des intégrations

Dans Horizon Cloud Service - next-gen, configurez diverses intégrations, telles qu'Identity Manager et des volumes d'applications dans le cadre de la configuration et de la mise en place du déploiement.

Gestion des identités et des accès dans un environnement Horizon Cloud Service - next-gen

Cette page de documentation fournit une brève présentation de l'utilisation de la gestion des identités et des accès dans un environnement Horizon Cloud Service - next-gen et répertorie les liens d'accès aux pages contenant des informations plus détaillées.

Présentation de l'identité d'utilisateur et de l'identité de machine

Horizon Cloud Service - next-gen diffère des autres environnements dans la manière dont il gère l'identité. Dans Horizon Cloud Service - next-gen, le service fait la distinction entre l'identité d'utilisateur et l'identité de machine, et il s'appuie sur les deux types d'identité lors de l'établissement d'une connexion sécurisée entre un client et une application ou un poste de travail distant.

Note Cette distinction entre identité d'utilisateur et identité de machine peut vous sembler nouvelle si vous connaissez mieux les environnements qui utilisent un fournisseur d'identité unique pour authentifier à la fois l'identité d'utilisateur et de machine, comme l'environnement Horizon Cloud de première génération ou un environnement Horizon 8 sur site.

Dans Horizon Cloud Service - next-gen, vous devez configurer une configuration d'identité composée d'un fournisseur d'identité pour authentifier l'identité d'utilisateur et d'un fournisseur d'identité pour authentifier l'identité de machine.

Identité d'utilisateur

Horizon Cloud Service - next-gen nécessite l'enregistrement d'un fournisseur d'identité utilisateur. Le service utilise ce fournisseur d'identité pour authentifier les utilisateurs clients qui tentent d'accéder à des applications et des postes de travail distants.

Identité de machine

Horizon Cloud Service - next-gen nécessite également l'enregistrement d'un fournisseur d'identité de machine. Le service utilise ce fournisseur d'identité pour établir l'identité de machine des machines virtuelles qui fournissent des applications et des postes de travail distants.

Par le biais du fournisseur d'identité de machine, le service joint les postes de travail distants et les sources de machines virtuelles pour les applications distantes au domaine de réseau approuvé auquel les utilisateurs clients sont autorisés à accéder.

Configuration requise pour l'identité d'utilisateur et l'identité de machine

Pour obtenir des informations détaillées sur les configurations d'identité prises en charge par Horizon Cloud Service - next-gen et les conditions détaillées en matière d'identité d'utilisateur et d'identité de machine, reportez-vous à la section Liste de vérification des conditions requises pour le déploiement d'un dispositif Microsoft Azure Edge.

Administrateurs et contrôle d'accès basé sur les rôles (RBAC)

Pour l'accès administrateur à votre environnement, le service fournit un contrôle d'accès basé sur les rôles à l'aide des fonctionnalités de VMware Cloud services. Ces contrôles garantissent que seul le personnel autorisé dispose des niveaux d'accès appropriés. Les contrôles sont basés sur le principe du moindre privilège. Pour plus d'informations, reportez-vous à la section À propos de l'ajout d'autres utilisateurs et de l'attribution de rôles disponible sur la page d'intégration.

En savoir plus

Utilisez les liens suivants pour accéder à d'autres informations sur la configuration de la gestion des identités et des accès pour votre environnement.

Configuration de votre domaine Active Directory

Dans Horizon Cloud Service - next-gen, procédez comme suit dans Horizon Universal Console pour enregistrer le premier domaine Active Directory dans le service ou enregistrer les domaines Active Directory supplémentaires.

Note Cette page de documentation s'applique lorsque votre environnement dispose d'un déploiement d'Horizon Edge dans Microsoft Azure. Elle ne s'applique pas aux déploiements d'Horizon 8 ni à l'abonnement Horizon Plus.

Comme décrit dans Gestion des identités et des accès dans un environnement Horizon Cloud Service - next-gen, le service utilise le domaine Active Directory enregistré pour l'identité de machine pour les postes de travail virtuels et les applications distantes.

Conditions préalables

Conditions requises pour Active Directory

L'assistant **Enregistrement de domaine** de la console nécessite la saisie d'informations spécifiques. Avant d'effectuer ces étapes dans la console, vérifiez que vous ou votre équipe informatique avez répondu aux exigences relatives à Active Directory, comme décrit dans la section Exigences relatives à Active Directory dans la liste de vérification des exigences pour le déploiement d'un dispositif Microsoft Azure Edge.

Points clés et conditions requises propres à LDAPS

Si vous prévoyez d'utiliser LDAPS dans votre déploiement, notez les points clés et conditions requises suivants.

- Les certificats d'autorité de certification racine et intermédiaire codés au format PEM doivent être prêts pour le chargement.

- Les certificats auto-signés ne sont pas pris en charge.
- Le service nécessite que votre DNS dispose d'enregistrements SRV pour les domaines configurés pour utiliser LDAPS. Choisir d'utiliser LDAPS pour un domaine impose implicitement l'utilisation d'enregistrements SRV.
- Il est fortement recommandé de configurer votre environnement AD pour appliquer la liaison de canal. L'application de la liaison de canal est une partie essentielle de la sécurisation correcte de LDAPS, en particulier pour éviter les attaques de l'intercepteur (MITM).
- La configuration de votre pare-feu doit autoriser les connexions sortantes depuis la passerelle Passerelle Horizon Edge vers vos contrôleurs de domaine avec les ports et protocoles suivants, comme décrit dans la section Conditions requises pour les ports et les protocoles pour votre déploiement d'Horizon Cloud dans Microsoft Azure.
  - Port 88/TCP : authentification Kerberos
  - Ports 636/TCP et 3269/TCP : communication LDAPS
- Vous devez disposer d'un point de terminaison de révocation HTTP défini pour tous les certificats de la chaîne d'approbation, à l'exception du certificat racine. Ce point de terminaison doit être accessible sur `HTTP`. Cette condition requise inclut les points suivants :
  - LDAP ne doit pas être utilisé pour les points de terminaison de révocation.
  - Le service effectuera des vérifications de révocation à l'aide des URL `HTTP` OCSP ou CRL qui sont définies dans vos certificats.
  - Le service ne peut pas vérifier la révocation si un certificat ne définit pas de point de terminaison OCSP ou CRL pour le protocole HTTP. Dans ce cas, la connectivité LDAPS échoue.
  - La révocation de la vue directe doit être disponible pour les points de terminaison. Vos pare-feu ne doivent pas bloquer le trafic sortant vers votre point de terminaison de révocation sur `HTTP`.

Procédure

1 Cliquez sur **Intégrations** dans le volet de gauche, puis, dans la vignette **Identité et accès**, cliquez sur **Gérer**.

2 Dans l'onglet **Domaines**, démarrez l'assistant **Enregistrement de domaine** en cliquant sur **Ajouter**.

3 Dans la première étape de l'assistant, fournissez les informations indiquées

Champ	Description
Nom	Nom du domaine Active Directory.
Description	Description facultative.

Champ	Description
Nom de domaine DNS	Nom complet de ce domaine Active Directory (par exemple, `our-ad.example.com`).
Unité d'organisation par défaut	Entrez une unité d'organisation par défaut appropriée. Cette unité d'organisation est l'unité d'organisation Active Directory que vous souhaitez que le service utilise par défaut lorsqu'il ajoute les identités de machine qu'il crée pour les postes de travail virtuels et les applications distantes. Tapez le nom unique complet de l'unité d'organisation, tel que `OU=MyOrg,DC=our-ad,DC=example,DC=com`. **Note** Si vous souhaitez utiliser la valeur par défaut `CN=Computers`, vous devez l'entrer dans le champ. Même si vous pouvez voir l'interface utilisateur afficher cette valeur par défaut dans le champ, l'assistant ne rendra pas le bouton **Suivant** disponible, sauf si vous l'entrez directement dans ce champ.
Comptes de liaison de domaine	Fournissez les noms d'utilisateur et les mots de passe des deux comptes de service que vous ou votre équipe informatique avez configurés à cette fin, comme décrit dans la section Exigences relatives à Active Directory dans la liste de vérification des exigences pour le déploiement d'un dispositif Microsoft Azure Edge. Ces comptes de service sont utilisés pour effectuer des recherches dans le domaine Active Directory. Le premier compte entré est le compte principal que le service utilise à cette fin. Le compte auxiliaire est une sauvegarde du compte principal. Assurez-vous que les comptes entrés ici répondent aux exigences détaillées dans la liste de vérification des exigences.
Comptes de jonction de domaine	Fournissez les noms d'utilisateur et les mots de passe des deux comptes de service que vous ou votre équipe informatique avez configurés à cette fin, comme décrit dans la section Exigences relatives à Active Directory dans la liste de vérification des exigences pour le déploiement d'un dispositif Microsoft Azure Edge. Ces comptes de service sont utilisés pour joindre les identités de machine au domaine Active Directory et pour effectuer des opérations Sysprep. Le premier compte entré est le compte principal que le service utilise à cette fin. Le compte auxiliaire est une sauvegarde du compte principal. Assurez-vous que les comptes entrés ici répondent aux exigences détaillées dans la liste de vérification des exigences.
Protocole	Sélectionnez le protocole, **LDAP** ou **LDAPS**, à utiliser pour connecter votre annuaire Active Directory à la passerelle Passerelle Horizon Edge. Si vous sélectionnez **LDAPS**, utilisez la fonctionnalité **Parcourir** pour charger vos certificats d'autorité de certification racine et intermédiaire codés au format PEM, qui sont référencés dans les conditions préalables de cette tâche.

Une fois que vous avez saisi toutes les informations requises, le système rend le bouton **Suivant** disponible.

4 Passez à l'étape suivante de l'assistant en cliquant sur **Suivant**.

À ce stade, l'assistant rend l'action **Enregistrer** disponible pour terminer l'enregistrement des informations de domaine dans le système.

- Si vous ne prévoyez pas d'utiliser SSO, vous pouvez terminer l'assistant d'interface utilisateur à ce stade en cliquant sur **Enregistrer**.

- Si vous prévoyez d'utiliser la fonctionnalité True SSO, passez à l'étape suivante de cette page. L'utilisation de la fonctionnalité True SSO nécessite une autorité de certification d'entreprise Microsoft, comme décrit dans Types d'autorité de certification pris en charge pour l'utilisation de SSO avec un dispositif Horizon Edge dans Microsoft Azure.
- Si vous prévoyez d'utiliser la fonctionnalité SSO qui repose sur l'autorité VMware CA ou les autorités de certification autre qu'une autorité de certification d'entreprise Microsoft, vous pouvez exécuter l'assistant d'interface utilisateur à ce stade en cliquant sur **Enregistrer**. Par la suite, vous pouvez effectuer cette configuration SSO en suivant les étapes décrites dans Ajouter une configuration SSO à Horizon Cloud Service - nouvelle génération pour une autorité de certification VMware CA.

5 (Facultatif) Si vous prévoyez d'utiliser True SSO avec les postes de travail virtuels et les applications distantes de vos utilisateurs finaux, dans la section **Compte de service d'inscription de domaine** de l'assistant, activez l'option **Utiliser le compte d'inscription de domaine**.

Lorsque cette option est activée, l'interface utilisateur affiche des champs vous permettant d'entrer les informations d'identification des comptes d'inscription de domaine requis par la fonctionnalité True SSO. Fournissez les informations en question.

Attention Si vous prévoyez plutôt d'utiliser la fonctionnalité SSO qui repose sur l'autorité VMware CA, vous pouvez ignorer cette étape de saisie des informations du compte d'inscription de domaine.

Un compte d'inscription de domaine est un compte de service d'inscription utilisé par la fonctionnalité True SSO pour obtenir des certificats de courte durée des Services de certificats Active Directory (AD CS). True SSO utilise les certificats pour l'authentification, afin d'éviter d'inviter les utilisateurs à entrer les informations d'identification Active Directory. Vous pouvez voir Horizon Universal Console utiliser de façon interchangeable les termes Compte d'inscription de domaine, Compte de service d'inscription et Compte de service d'inscription de domaine.

Une fois les champs remplis, l'assistant rend disponible l'action **Enregistrer** pour terminer l'action d'enregistrement des informations de domaine dans le système.

Cliquez sur **Enregistrer** pour terminer l'enregistrement de toutes les informations fournies dans l'assistant.

Résultats

Votre configuration d'Active Directory avec Horizon Edge est terminée. Cependant, lorsque vous continuez à configurer votre déploiement, reportez-vous à la section Diagnostic de Dispositifs Horizon Edge : connectivité Active Directory pour les déploiements Microsoft Azure si vous détectez des problèmes avec la connexion Active Directory.

Étape suivante

À la fin des étapes précédentes, le service dispose des informations de domaine Active Directory dont il a besoin pour un déploiement Horizon Cloud on Microsoft Azure.

Pour en savoir plus sur l'ajout de la possibilité pour vos utilisateurs finaux de disposer de la fonctionnalité Single Sign-On (SSO) lors de l'accès à leurs postes de travail et applications, reportez-vous à la section Types d'autorité de certification pris en charge pour l'utilisation de SSO avec un dispositif Horizon Edge dans Microsoft Azure.

Modification de votre domaine Active Directory - Horizon Cloud Service - next-gen

Après avoir ajouté un domaine Active Directory, vous pouvez utiliser Horizon Universal Console pour modifier ce domaine.

Les conditions préalables et les étapes impliquées dans la modification de votre domaine Active Directory sont très semblables aux étapes initiales de configuration de votre domaine Active Directory. Pour plus de détails, reportez-vous à la section Configuration de votre domaine Active Directory. Les conditions préalables que vous devez remplir pour cette tâche dépendent des informations de domaine que vous prévoyez de mettre à jour. Par exemple, si vous remplacez le protocole LDAP par LDAPS, vous devez remplir les conditions préalables liées à LDAPS, telles que la préparation des certificats d'autorité de certification racine et intermédiaire codés au format PEM et la mise à disposition des ports LDAPS appropriés.

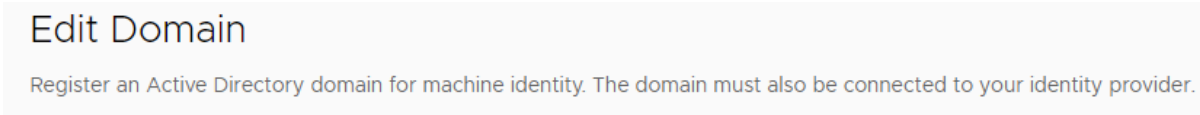
Procédure

1 Accédez à l'onglet **Domaines** de la console.

Cliquez sur **Intégrations** dans le volet de gauche, puis, dans la vignette **Identité et accès**, cliquez sur **Gérer**.

2 Sélectionnez un domaine à modifier, puis cliquez sur **Modifier**.

3 Modifiez les informations que vous souhaitez mettre à jour.



Champ	Description
Informations générales	Modifiez les informations générales, telles que **Nom** et **Unité d'organisation par défaut** si nécessaire.
Comptes de liaison de domaine	Le cas échéant, mettez à jour les noms d'utilisateur et les mots de passe des deux comptes de service que vous ou votre équipe informatique avez configurés à cette fin, comme décrit dans la section Conditions requises pour Active Directory dans la liste de vérification des conditions requises pour le déploiement d'un dispositif Microsoft Azure Edge.

Champ	Description
Comptes de jonction de domaine	Le cas échéant, fournissez les noms d'utilisateur et les mots de passe des deux comptes de service que vous ou votre équipe informatique avez configurés à cette fin, comme décrit dans la section Conditions requises pour Active Directory dans la liste de vérification des conditions requises pour le déploiement d'un dispositif Microsoft Azure Edge.
Protocole	Le cas échéant, remplacez le protocole **LDAP** par **LDAPS** ou **LDAPS** par **LDAP**. Si vous passez de **LDAP** à **LDAPS**, utilisez la fonctionnalité **Parcourir** pour charger vos certificats d'autorité de certification racine et intermédiaire codés au format PEM, qui sont référencés dans les conditions préalables de cette tâche.

4 Cliquez sur **Enregistrer**.

5 (Facultatif) Si vous prévoyez d'utiliser True SSO avec les postes de travail virtuels et les applications distantes de vos utilisateurs finaux, dans la section **Compte de service d'inscription de domaine** de l'assistant, activez l'option **Utiliser le compte d'inscription de domaine**.

Lorsque cette option est activée, l'interface utilisateur affiche des champs vous permettant d'entrer les informations d'identification des comptes d'inscription de domaine requis par la fonctionnalité True SSO. Fournissez les informations en question.

Attention Si vous prévoyez plutôt d'utiliser la fonctionnalité SSO qui repose sur l'autorité VMware CA, vous pouvez ignorer cette étape de saisie des informations du compte d'inscription de domaine.

Un compte d'inscription de domaine est un compte de service d'inscription utilisé par la fonctionnalité True SSO pour obtenir des certificats de courte durée des Services de certificats Active Directory (AD CS). True SSO utilise les certificats pour l'authentification, afin d'éviter d'inviter les utilisateurs à entrer les informations d'identification Active Directory. Vous pouvez voir Horizon Universal Console utiliser de façon interchangeable les termes Compte d'inscription de domaine, Compte de service d'inscription et Compte de service d'inscription de domaine.

Une fois les champs remplis, l'assistant rend disponible l'action **Enregistrer** pour terminer l'action d'enregistrement des informations de domaine dans le système.

Cliquez sur **Enregistrer** pour terminer l'enregistrement de toutes les informations fournies dans l'assistant.

Résultats

Votre mise à jour d'Active Directory avec Horizon Edge est terminée. Par exemple, si vous détectez des problèmes avec la connexion Active Directory, reportez-vous à la section Diagnostic de Dispositifs Horizon Edge : connectivité Active Directory pour les déploiements Microsoft Azure.

Suppression d'un domaine

Si vous souhaitez supprimer un domaine, vous devez supprimer toutes les ressources associées. Lorsqu'aucune ressource n'est associée à un domaine, il peut être supprimé.

Procédure

1. Connectez-vous à Horizon Universal Console.
2. Cliquez sur **Intégrations** dans la barre de navigation.
3. Cliquez sur **Gérer** sur la vignette **Identité et accès**.
4. Sélectionnez un domaine à supprimer sur la page **Identité et accès**, puis cliquez sur **Supprimer**.
5. Supprimez l'authentification unique **SSO** et les **Groupes de pool** associés au domaine.

   Vous ne pouvez pas supprimer un domaine si des ressources sont associées au domaine. Aucune ressource n'est associée au domaine. Vous pouvez le supprimer définitivement sans étapes supplémentaires.

Types d'autorité de certification pris en charge pour l'utilisation de SSO avec un dispositif Horizon Edge dans Microsoft Azure

Cette page de documentation répertorie les catégories de types d'autorité de certification que Horizon Cloud Service - next-gen prend en charge pour fournir la fonctionnalité Single Sign-On aux postes de travail virtuels et aux applications distantes de l'utilisateur final.

Introduction

Lorsque vous souhaitez que vos utilisateurs finaux disposent de Single Sign-On (SSO) dans leurs applications et postes de travail virtuels fournis par un dispositif Horizon Edge dans Microsoft Azure, vous devez configurer les éléments dont Horizon Cloud a besoin pour fournir cette capacité SSO.

Un élément clé est l'autorité de certification qui fournira les certificats à court terme pour la fonctionnalité SSO du service à utiliser pour l'authentification, afin d'éviter d'inviter les utilisateurs à fournir les informations d'identification Active Directory.

Types pris en charge

Pour ses capacités SSO, Horizon Cloud Service - next-gen prend actuellement en charge l'utilisation du type d'autorité de certification suivant.

Autorité de certification Microsoft Enterprise (Services de certificats Active Directory)

L'expression Autorité de certification d'entreprise Microsoft fait référence à une autorité de certification Microsoft (Microsoft CA) exécutée en mode Entreprise. Dans la procédure Microsoft de configuration d'une autorité de certification d'entreprise Microsoft, le rôle des services de certificats Active Directory (AD CS) est installé et configuré pour s'exécuter en tant qu'autorité de certification d'entreprise.

Lorsque vous souhaitez utiliser ce type (autorité de certification d'entreprise Microsoft) pour ces certificats, dans Horizon Universal Console, vous choisissez l'option nommée **Microsoft CA**. Cette sélection configure Horizon Edge pour qu'il utilise la fonctionnalité True SSO afin de fournir à l'utilisateur final la capacité Single Sign-On.

Autres autorités de certification

Cette catégorie inclut l'autorité de certification autonome Microsoft et les autorités de certification de tiers. L'expression Autorité de certification autonome Microsoft fait référence à une autorité de certification Microsoft s'exécutant en mode autonome (type d'autorité de certification autonome dans le processus de configuration du rôle AD CS).

Si vous souhaitez utiliser ce type d'autorité de certification pour les certificats, dans Horizon Universal Console, choisissez l'option nommée **VMware CA**. Cette sélection configure Horizon Edge pour qu'il utilise la fonctionnalité VMware CA afin de fournir la capacité Single Sign-On de l'utilisateur final.

Informations supplémentaires

Pour en savoir plus sur l'utilisation du type d'autorité de certification actuellement pris en charge, reportez-vous à la section :

Pour en savoir plus sur l'utilisation de chaque type et pour obtenir des liens vers leurs conditions préalables, reportez-vous aux sections suivantes :

- Horizon Cloud : conditions requises de True SSO - Autorité de certification d'entreprise Microsoft, modèles de certificat requis
- Ajouter une configuration SSO à Horizon Cloud Service - nouvelle génération pour utiliser True SSO avec vos dispositifs Horizon Edge
- Ajouter une configuration SSO à Horizon Cloud Service - nouvelle génération pour une autorité de certification VMware CA

Horizon Cloud : conditions requises de True SSO - Autorité de certification d'entreprise Microsoft, modèles de certificat requis

Pour Horizon Cloud Service - next-gen, cette page décrit les éléments requis pour utiliser la fonctionnalité True SSO avec un dispositif Horizon Edge dans Microsoft Azure.

Vous êtes peut-être déjà familiarisé avec l'utilisation de True SSO dans vos déploiements d'Horizon antérieurs, tels qu'Horizon 8 sur site ou un déploiement d'Horizon Cloud on Microsoft Azure de première génération.

Pour un environnement Horizon Cloud Service - next-gen, les éléments requis pour utiliser la fonctionnalité True SSO afin de fournir à vos utilisateurs finaux un accès Single Sign-On (SSO) à leurs postes de travail et applications sont une autorité de certification d'entreprise Microsoft et des modèles de certificat spécifiquement configurés dans cette autorité de certification d'entreprise Microsoft.

Autorité de certification d'entreprise Microsoft

L'utilisation de True SSO nécessite l'autorité de certification d'entreprise Microsoft.

Le terme Autorité de certification d'entreprise Microsoft fait référence à une autorité de certification Microsoft (Microsoft CA) exécutée en mode entreprise. Comme True SSO nécessite la configuration d'entreprise, la documentation de True SSO utilise l'expression Autorité de certification d'entreprise Microsoft.

Info-bulle Dans les environnements de production, il est recommandé de disposer d'au moins deux (2) autorités de certification de ce type pour assurer la redondance et l'équilibrage de charge.

Si une autorité de certification n'est pas déjà configurée, vous devez ajouter le rôle Services de certificats Active Directory (AD CS) à un serveur Microsoft Windows et le configurer en tant qu'autorité de certification d'entreprise.

Dans la procédure Microsoft de configuration d'une autorité de certification d'entreprise Microsoft, vous installez le rôle Services de certificats Active Directory (AD CS). Le processus de configuration d'AD CS vous donne le choix entre l'exécution de l'autorité de certification en tant qu'autorité de certification d'entreprise ou en tant qu'autorité de certification autonome.

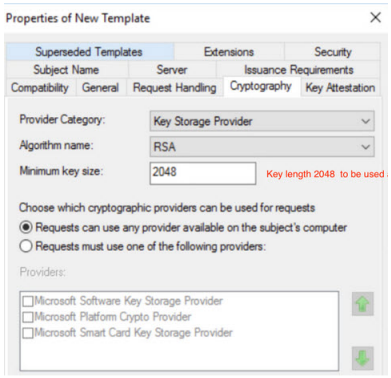
Configurer les modèles de certificat requis pour True SSO avec Horizon Cloud

Spécifiez les paramètres suivants, y compris la taille de clé minimale pour le certificat de signature Windows Server pour le modèle True SSO. Pour un certificat de signature Windows Server, la taille de clé minimale requise est de 2 048. La spécification d'une taille de clé minimale inférieure à 2 048 entraîne l'échec de l'authentification.

Pour le modèle True SSO, spécifiez les paramètres suivants dans l'onglet **Chiffrement**.

1. Pour **Catégorie de fournisseur**, sélectionnez **Fournisseur de stockage de clés**.
2. Pour **Nom d'algorithme**, sélectionnez **RSA**.
3. Pour **Taille de clé minimale**, spécifiez **2 048**.
4. Pour **Choisir les fournisseurs de chiffrement pouvant être utilisés pour les demandes**, sélectionnez **Les demandes peuvent utiliser n'importe quel fournisseur disponible sur l'ordinateur du sujet**.
5. Pour **Demande de hachage**, spécifiez **SHA384**.
6. Cliquez sur **Enregistrer**.

Une capture d'écran partielle s'affiche ci-dessous, ce qui illustre la valeur de taille de clé minimale de 2 048.



Activer le traitement non persistant des certificats

Pour chaque Autorité de certification d'entreprise Microsoft utilisée par True SSO, il est recommandé d'activer le traitement non persistant des certificats.

Si le traitement des certificats non persistant n'est pas activé sur l'Autorité de certification d'entreprise Microsoft, les certificats True SSO restent stockés dans la base de données de l'autorité de certification d'entreprise, ce qui a les effets suivants :

- La base de données de l'autorité de certification d'entreprise augmente inutilement rapidement. True SSO demande un nouveau certificat pour chaque nouvelle connexion.
- Incidence sur les performances, car l'autorité de certification d'entreprise manque d'espace disque à mesure que sa base de données croît.

Comme décrit dans l'article 2149312 de la base de connaissances VMware, pour éviter les problèmes ci-dessus, il est recommandé d'activer le paramètre `DBFLAGS_ENABLEVOLATILEREQUESTS`. Reportez-vous à l'article de la base de connaissances pour connaître les étapes à suivre.

Note En plus de décrire la recommandation d'activation de `DBFLAGS_ENABLEVOLATILEREQUESTS`, cet article de la base de connaissances décrit également l'utilisation d'un autre paramètre, `CRLF_REVCHECK_IGNORE_OFFLINE`. L'activation du paramètre `CRLF_REVCHECK_IGNORE_OFFLINE` dépend de votre architecture PKI. L'activation du paramètre `CRLF_REVCHECK_IGNORE_OFFLINE` n'est pas une exigence stricte pour True SSO et Horizon Cloud.

Configurer les modèles de certificat requis pour True SSO avec Horizon Cloud

La fonctionnalité True SSO nécessite la configuration des modèles de certificat sur l'Autorité de certification d'entreprise Microsoft que vous fournissez pour une utilisation avec True SSO et votre dispositif Horizon Edge.

Les modèles de certificat constituent la base des certificats générés par l'autorité de certification d'entreprise Microsoft pour une utilisation avec True SSO.

Les comptes de service d'inscription nécessitent des autorisations de `lecture` et d'`inscription` sur les deux modèles, le modèle `TrueSsoEnrollmentAgent` et le modèle `TrueSso`.

Conditions préalables

- Vérifiez que vous disposez des instances d'Autorité de certification d'entreprise Microsoft (AD CS) requises par la fonctionnalité True SSO, comme décrit dans Types d'autorité de certification pris en charge pour l'utilisation de SSO avec un dispositif Horizon Edge dans Microsoft Azure.
- Configurez votre pare-feu pour permettre aux dispositifs Horizon Edge déployés de communiquer avec les instances de l'autorité de certification avec la combinaison de protocole et de ports requise, comme décrit dans Conditions requises pour les ports et les protocoles pour votre déploiement d'Horizon Cloud dans Microsoft Azure.

  La communication utilise les services de certificats Active Directory (AD CS). Le protocole requis est RPC/TCP (RPC sur TPC). Le premier port est le port 135 et le second port est compris entre 49152 et 65535.
- Pour une configuration plus conviviale du pare-feu, vous pouvez configurer vos instances d'Autorité de certification d'entreprise Microsoft (AD CS) pour utiliser un port DCOM statique et configurer le pare-feu pour autoriser le port 135 et le port DCOM statique que vous avez choisi, en configurant ce port statique pour qu'il soit le même sur toutes les instances. Cette configuration est décrite dans Microsoft TechNet Comment configurer un port DCOM statique pour AD CS.

Note Les étapes suivantes ont été effectuées à l'aide d'une autorité de certification d'entreprise Microsoft exécutant le système d'exploitation Microsoft Windows Server 2016 Standard. Les captures d'écran dans les étapes ont été effectuées à partir de ce système. Par conséquent, les étiquettes mentionnées dans les étapes et les captures d'écran reflètent ce système d'exploitation. Si votre autorité de certification d'entreprise Microsoft exécute une version de système d'exploitation différente de Windows Server, vous pouvez voir des différences mineures dans votre système par rapport aux étiquettes et captures d'écran ci-dessous.

Procédure

1 Créez un groupe de sécurité universel dans Active Directory.

Créer ce groupe vous permet de disposer d'un groupe de sécurité unique auquel vous pouvez attribuer les autorisations requises pour émettre des certificats pour le compte des utilisateurs. Tous les comptes de service d'inscription peuvent donc hériter de ces autorisations requises en devenant un membre de ce groupe.

a Ouvrez l'outil Utilisateurs et ordinateurs Active Directory dans le menu **Outils** du Gestionnaire de serveur ou en exécutant la commande **`dsa.msc`**.

b Dans l'outil Utilisateurs et ordinateurs Active Directory, créez un groupe pour les comptes d'inscription de domaine dont True SSO a besoin.

Donnez au groupe le nom de votre choix, par exemple **`Comptes d'inscription True SSO`**. Définissez également :

Paramètre	Valeur
Portée du groupe	Universel
Type de groupe	Sécurité

c Cliquez sur **OK** pour enregistrer le nouveau groupe.

d Ajoutez ensuite les comptes d'inscription de domaine en tant que membres de ce nouveau groupe.

Ajoutez chaque compte de service d'inscription de domaine qui vous servira pour utiliser True SSO.

Ces comptes sont les mêmes que ceux que vous avez ajoutés dans le flux de l'interface utilisateur d'enregistrement de domaine en utilisant Horizon Universal Console, comme décrit dans la section Configuration de votre domaine Active Directory.

2 Configurez le modèle de certificat d'agent d'inscription de True SSO à l'aide de l'outil Autorité de certification et de sa console de modèles de certificat.

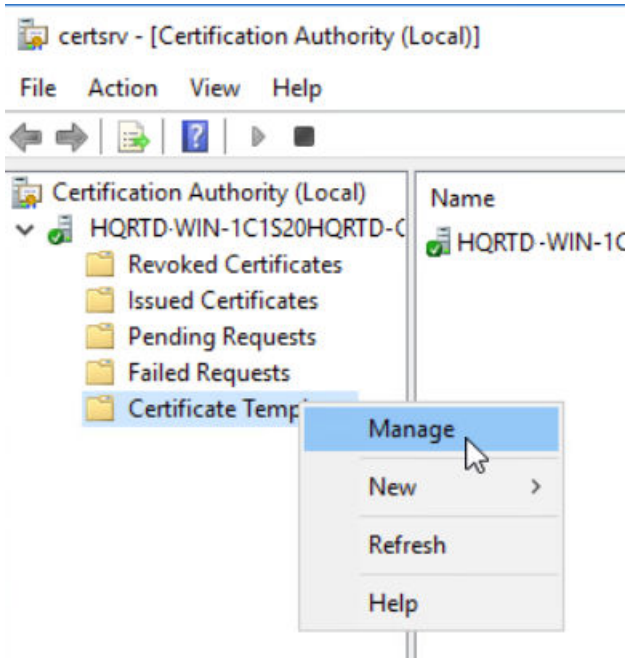
a Ouvrez l'outil Autorité de certification.

Vous pouvez ouvrir cet outil en utilisant le menu **Outils** du gestionnaire de serveur, les outils d'administration de Windows du menu **Démarrer** ou en exécutant `certsrv.msc`.

b Dans l'arborescence de gauche de l'outil Autorité de certification, développez le nom de l'autorité de certification locale jusqu'à ce que le dossier Modèles de certificat s'affiche.

c Ouvrez la console des modèles de certificat en cliquant avec le bouton droit sur le dossier Modèles de certificat et en sélectionnant **Gérer**.

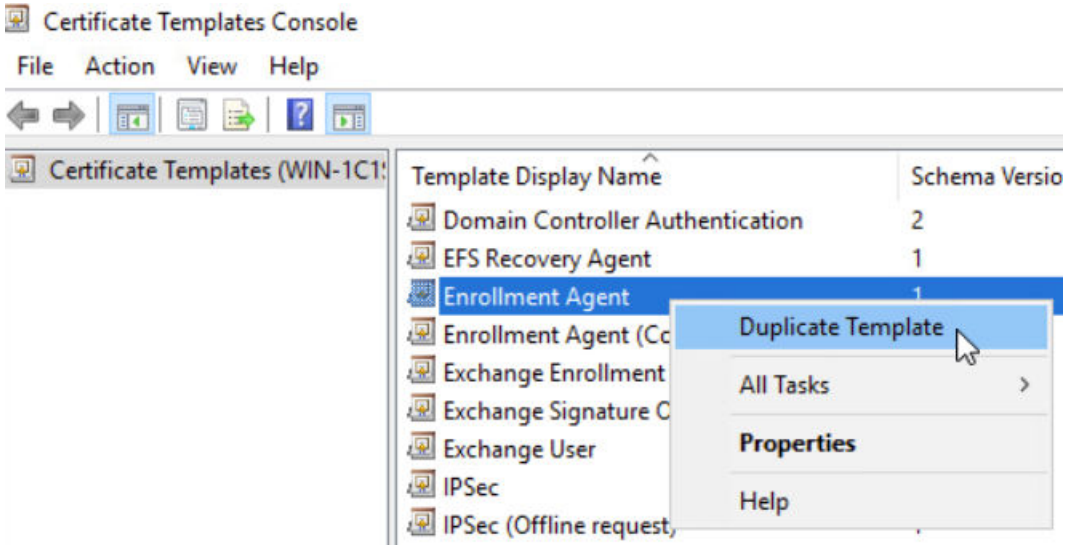
La capture d'écran suivante illustre cette étape dans un système exécutant Windows Server 2016.



La console des modèles de certificat s'affiche.

d Cliquez avec le bouton droit sur le modèle **Agent d'inscription** répertorié, puis sélectionnez **Dupliquer le modèle**.

La capture d'écran suivante illustre cette étape dans un système exécutant Windows Server 2016.



La fenêtre **Propriétés du nouveau modèle** s'affiche.

e Entrez les informations dans les onglets de la fenêtre, comme décrit dans les sections suivantes.

Note Les captures d'écran ci-dessous ont été effectuées à l'aide d'une autorité de certification d'entreprise Microsoft exécutant le système d'exploitation Microsoft Windows Server 2016 Standard. Si votre autorité de certification d'entreprise Microsoft exécute une version de système d'exploitation différente de Windows Server, vous pouvez voir des différences mineures dans l'interface utilisateur de votre système Windows.

Onglet Général

Important Utilisez uniquement des caractères ASCII dans les noms de vos modèles de True SSO. En raison de ce problème connu, si les noms de modèles de True SSO contiennent des caractères non-ASCII ou ASCII étendus, vous ne pouvez pas configurer True SSO avec votre environnement Horizon Cloud.

Nom complet du modèle

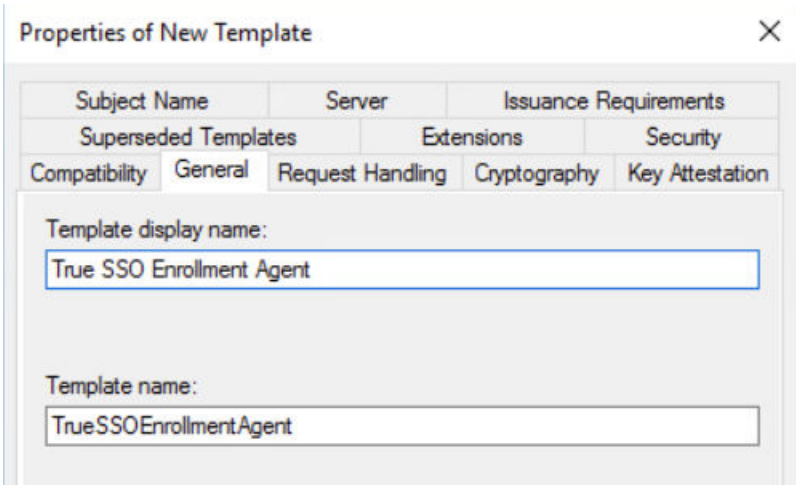
Entrez un nom qui indique que ce nouveau modèle correspond à l'agent d'inscription True SSO, par exemple **`Agent d'inscription SSO`**.

Nom du modèle

Lorsque vous tapez le **Nom complet du modèle** précédent, l'outil entre automatiquement ce nom ici pour qu'il corresponde à votre entrée du **Nom complet du modèle** sans espace.

Par exemple, si vous avez entré **`Agent d'inscription True SSO`** dans **Nom complet du modèle**, l'outil définit automatiquement ce **Nom de modèle** sur `TrueSsoEnrollmentAgent`.

La capture d'écran suivante illustre cet onglet après avoir entré le **Nom complet du modèle** comme **`Agent d'inscription True SSO`**.

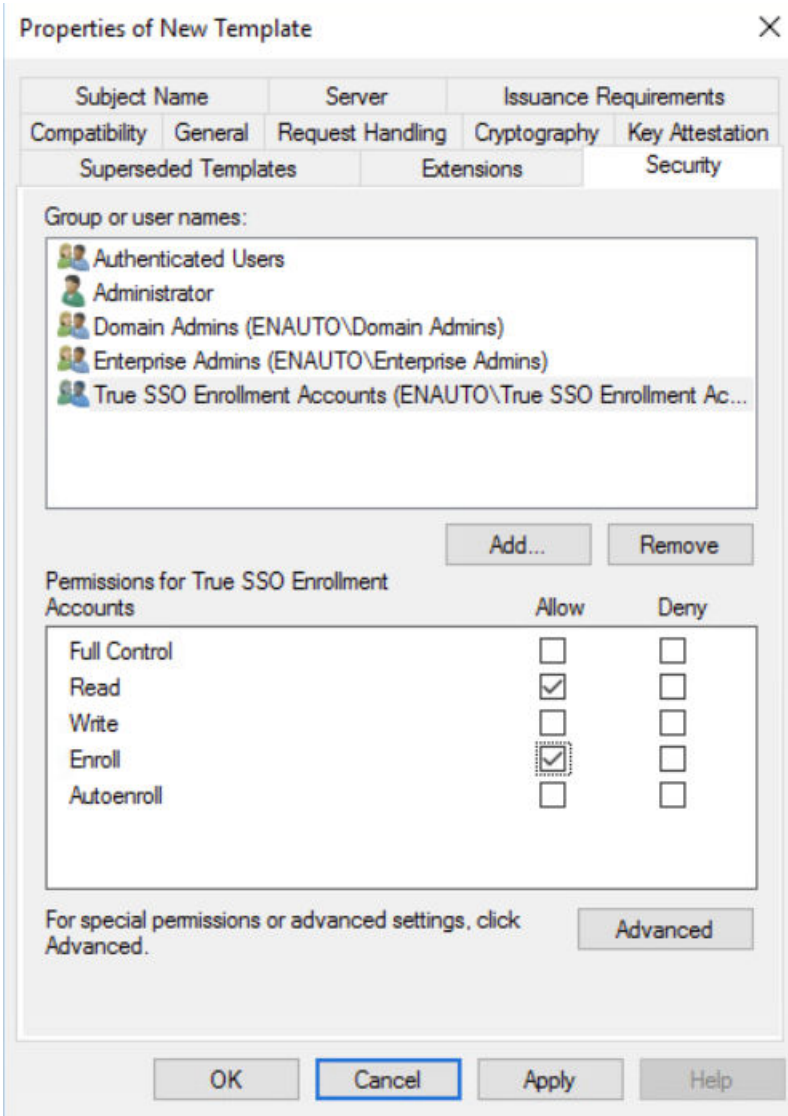


Onglet Sécurité

Dans l'onglet **Sécurité**, attribuez les autorisations `Read` et `Enroll` au nouveau groupe de sécurité universel que vous avez créé pour les comptes d'inscription True SSO.

1 Dans la section **Noms de groupes ou d'utilisateurs**, ajoutez le groupe que vous avez créé pour les comptes d'inscription True SSO.

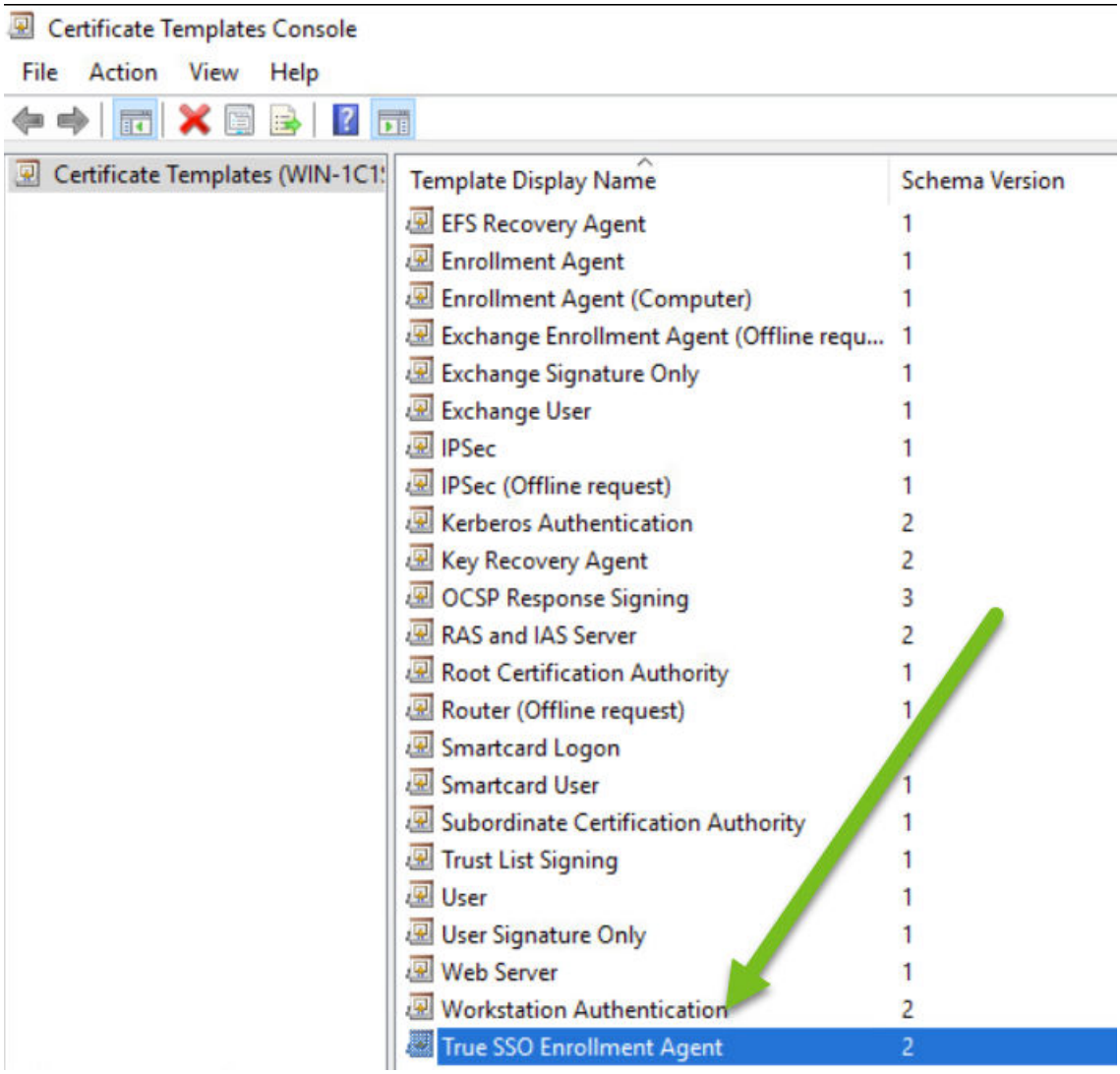
2 Sélectionnez ce groupe et dans la section Autorisations, sélectionnez **Autoriser** pour les autorisations `Read` et `Enroll`.



f Enregistrez le nouveau modèle Agent d'inscription True SSO en cliquant sur **OK** dans la fenêtre **Propriétés du nouveau modèle**.

Le nouveau modèle Agent d'inscription True SSO est répertorié dans la console des modèles de certificat, affiché à l'aide du **Nom complet du modèle** que vous lui avez donné et avec l'objectif affiché d'agent de demande de certificat.

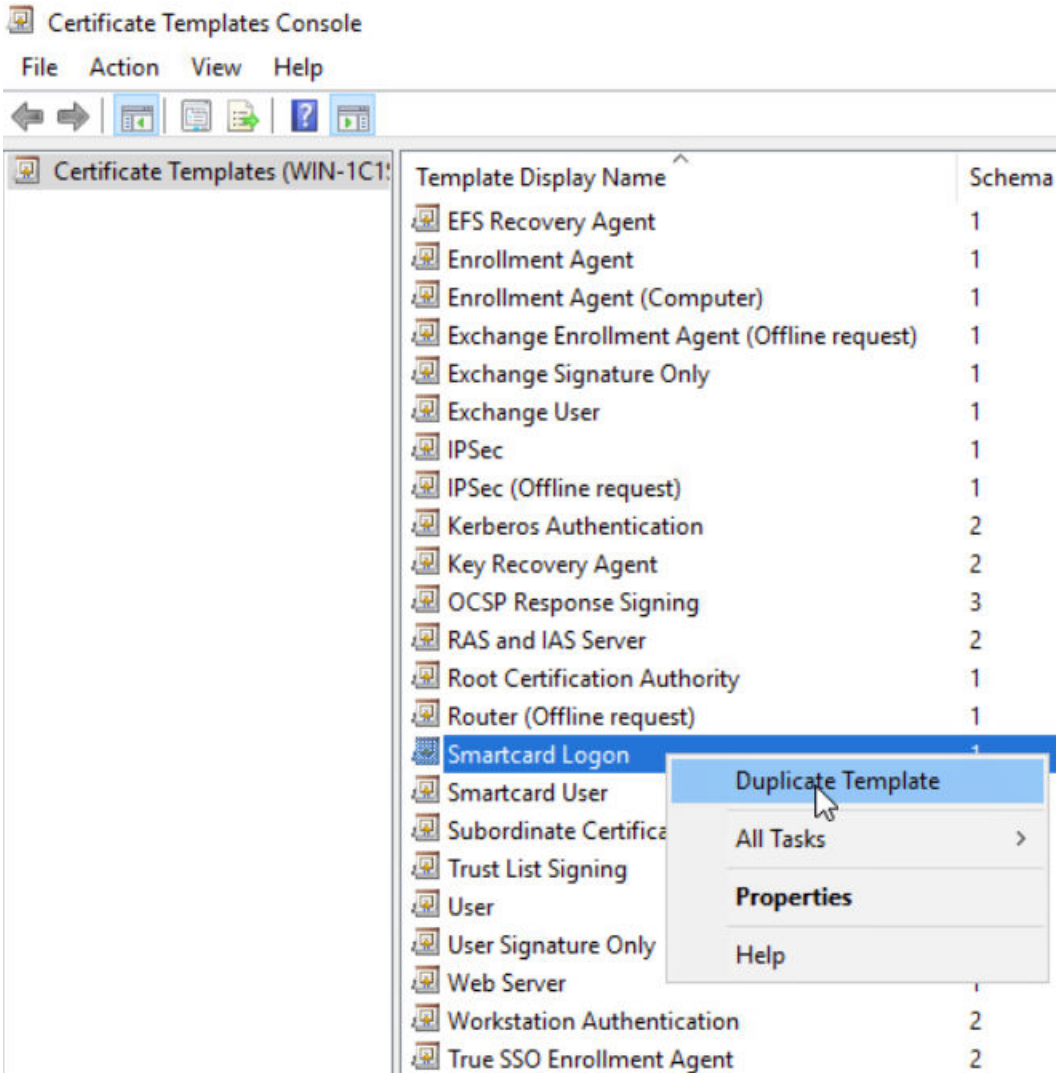
La capture d'écran suivante illustre le nouveau modèle répertorié.


Certificate Templates Console
File Action View Help
Certificate Templates (WIN-1C1
Template Display Name
Schema Version
EFS Recovery Agent 1
Enrollment Agent 1
Enrollment Agent (Computer) 1
Exchange Enrollment Agent (Offline requ... 1
Exchange Signature Only 1
Exchange User 1
IPSec 1
IPSec (Offline request) 1
Kerberos Authentication 2
Key Recovery Agent 2
OCSP Response Signing 3
RAS and IAS Server 2
Root Certification Authority 1
Router (Offline request) 1
Smartcard Logon
Smartcard User 1
Subordinate Certification Authority 1
Trust List Signing 1
User 1
User Signature Only 1
Web Server 1
Workstation Authentication 2
True SSO Enrollment Agent 2

3 Dans la même console de modèles de certificat, configurez le modèle d'ouverture de session de carte à puce True SSO.

   a Dans la console des modèles de certificat, cliquez avec le bouton droit sur le modèle **Ouverture de session par carte à puce** répertorié et sélectionnez **Dupliquer le modèle**.

   La capture d'écran suivante illustre cette étape dans un système exécutant Windows Server 2016.



La fenêtre **Propriétés du nouveau modèle** s'affiche.

b Entrez les informations dans les onglets de la fenêtre, comme décrit dans les sections suivantes.

Attention Assurez-vous de suivre ces points, sinon le système vous empêchera de définir les valeurs requises, vous forçant à annuler et à répéter vos étapes. Cette exigence est un comportement du système Windows.

- Ne cliquez pas sur **Appliquer** ni **OK** dans la fenêtre Propriétés avant d'avoir procéder aux réglages requis dans les trois onglets comme décrit au point suivant, dans l'ordre spécifique déterminé.

  Si vous ne suivez pas ces instructions de configuration des paramètres dans les trois onglets comme décrit ci-dessous avant d'appliquer ou d'enregistrer dans la fenêtre, Windows force la **Catégorie du fournisseur** de l'onglet chiffrement sur lecture seule, et le paramètre ne peut pas être modifié ultérieurement par le paramètre **Fournisseur de stockage de clés** requis par True SSO.

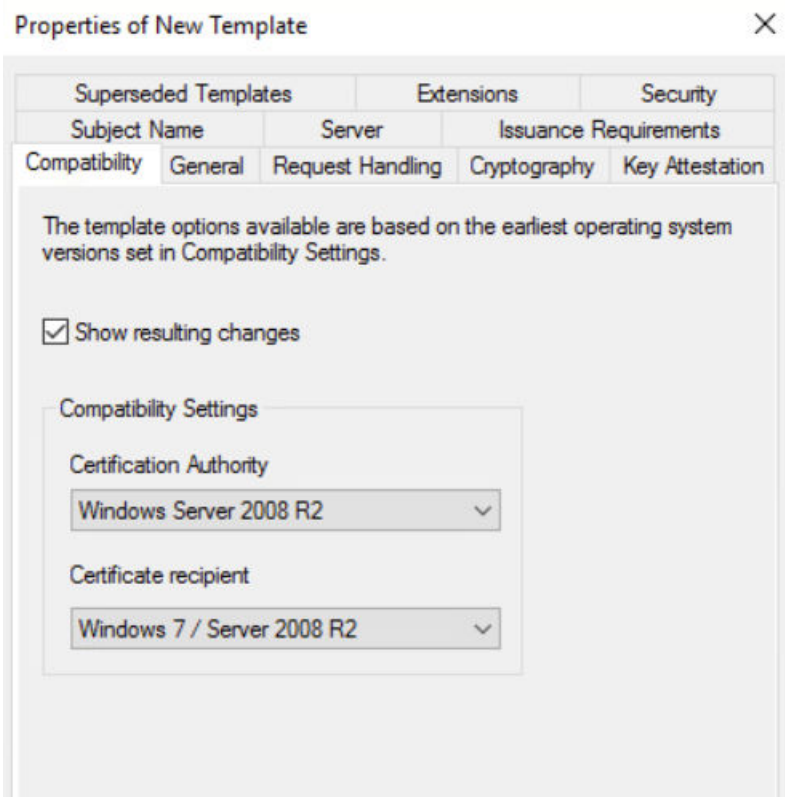
  Par conséquent, vous devez vous assurer que vous effectuez la configuration dans les trois onglets suivants dans l'ordre approprié indiqué ci-dessous avant d'appliquer ou d'enregistrer dans la fenêtre.

- Configurez ces onglets en premier et configurez-les dans cet ordre précis :

Onglet Compatibilité

Note Vous devez effectuer ces sélections dans l'onglet **Compatibilité** afin que les options appropriées soient disponibles dans l'onglet **Chiffrement**.

- Cochez la case **Afficher les modifications résultantes**.
- **Autorité de certification** : le système présente les choix que Microsoft Windows met à disposition pour ce paramètre. Pour répondre aux exigences de True SSO, sélectionnez l'option **Windows Server 2008 R2** ou l'une des versions ultérieures présentées dans le menu.
- **Destinataire du certificat** : le système présente les options que Microsoft Windows met à disposition pour ce paramètre. Pour répondre aux exigences de True SSO, sélectionnez l'option **Windows 7/Server 2008 R2** ou l'une des versions ultérieures présentées dans le menu.



Onglet Général

Important Utilisez uniquement des caractères ASCII dans les noms de vos modèles de True SSO. En raison de ce problème connu, si les noms de modèles de True SSO contiennent des caractères non-ASCII ou ASCII étendus, vous ne pouvez pas configurer True SSO avec votre environnement Horizon Cloud.

Nom complet du modèle

Entrez un nom qui indique que ce nouveau modèle est destiné à être utilisé par True SSO, par exemple **`True SSO`**.

Nom du modèle

Lorsque vous tapez le **Nom complet du modèle** précédent, l'outil entre automatiquement ce nom ici pour qu'il corresponde à votre entrée du **Nom complet du modèle** sans espace.

Par exemple, si vous avez entré **`True SSO`** dans **Nom complet du modèle**, l'outil définit automatiquement ce **Nom du modèle** sur `TrueSSO`.

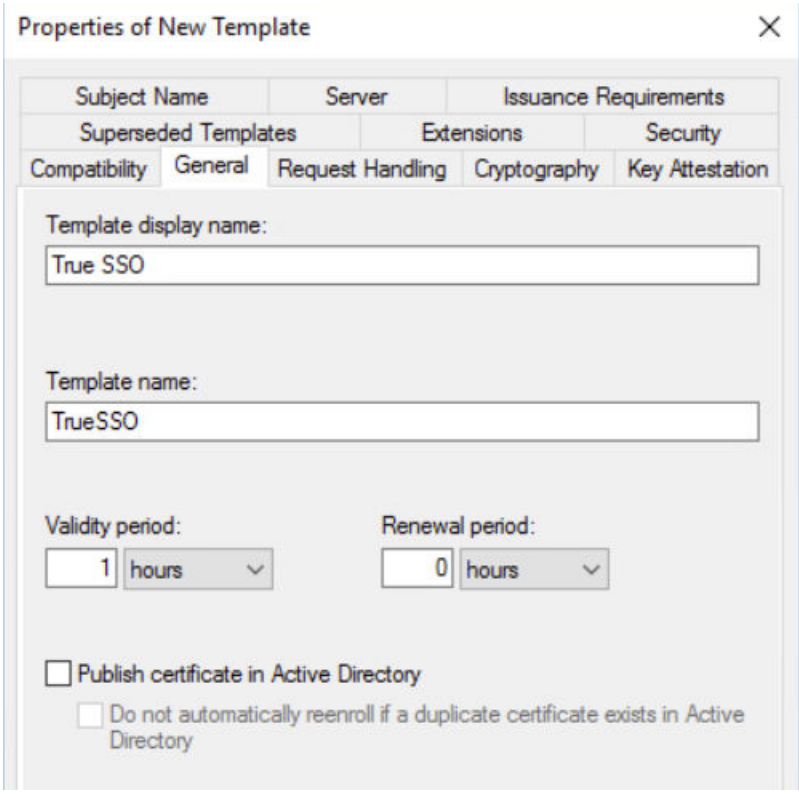
Période de validité

1 heure (une heure)

Période de renouvellement

0 semaine (zéro semaine)

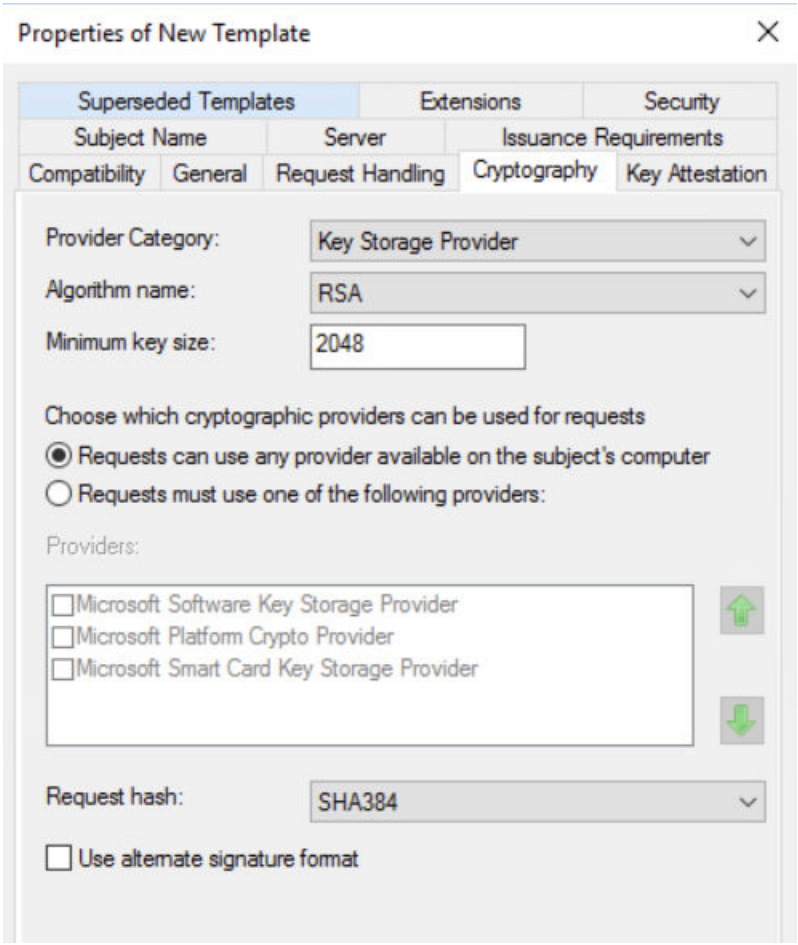
La capture d'écran suivante illustre cet onglet après avoir entré **`True SSO`** comme **Nom complet du modèle**.



Onglet Chiffrement

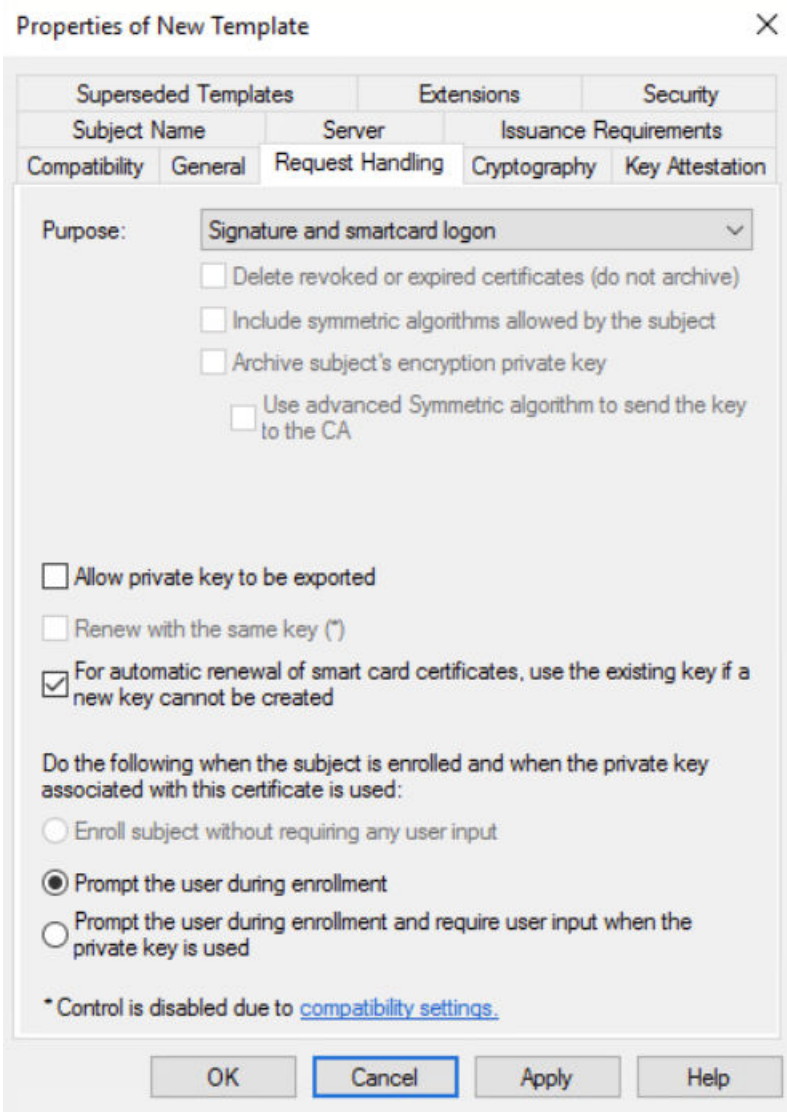
- Catégorie de fournisseurs : fournisseur de stockage de clés
- Nom d'algorithme : RSA
- Taille de clé minimale : 2048

- Cochez la case d'option **Les demandes peuvent utiliser n'importe quel fournisseur disponible dans l'ordinateur du sujet**
- Demande de hachage : SHA384



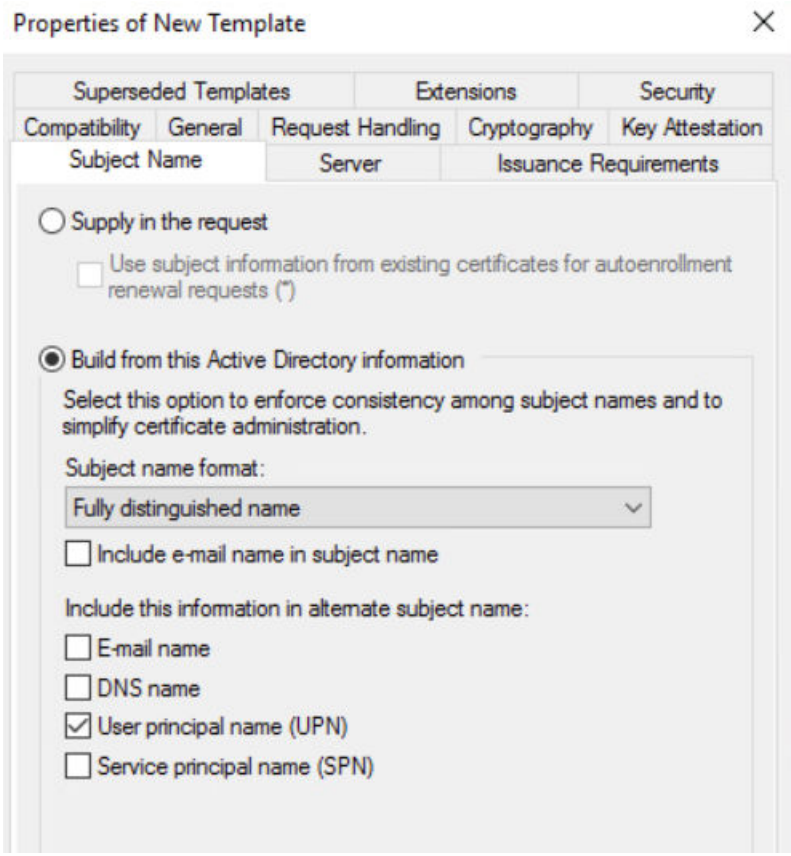
Onglet Traitement de la demande

- Objectif : ouverture de session par signature et carte à puce
- Cochez la case **Pour le renouvellement automatique des certificats par carte à puce, utilisez la clé existante si une nouvelle clé ne peut pas être créée**
- Cochez la case d'option **Inviter l'utilisateur lors de l'inscription**.



Onglet Nom du sujet

- Cochez la case d'option **Créer à partir de ces informations Active Directory**.
- Format du nom du sujet : nom unique
- Cochez la case **Nom principal d'utilisateur (UPN)**.



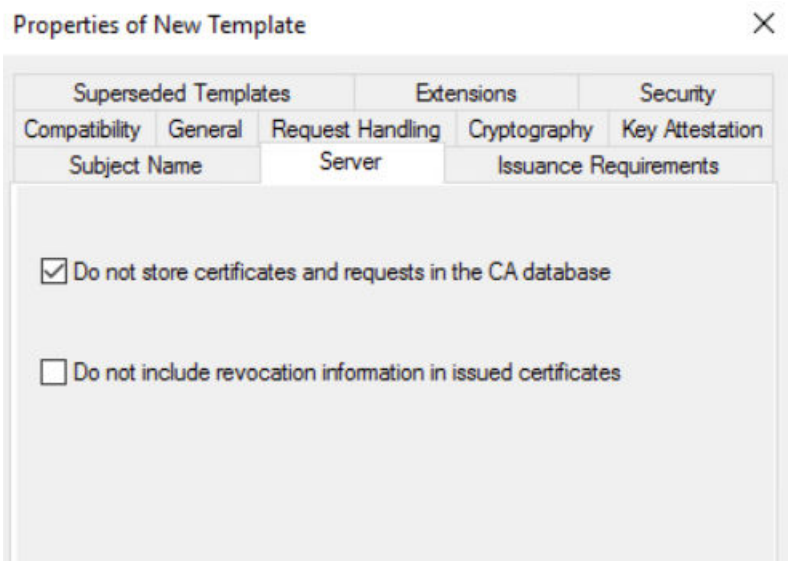
Onglet Serveur

Cochez la case **Ne pas stocker les certificats et les demandes dans la base de données de l'autorité de certification**.

Important Assurez-vous de décocher la deuxième case intitulée **Ne pas inclure les informations de révocation dans les certificats émis**.

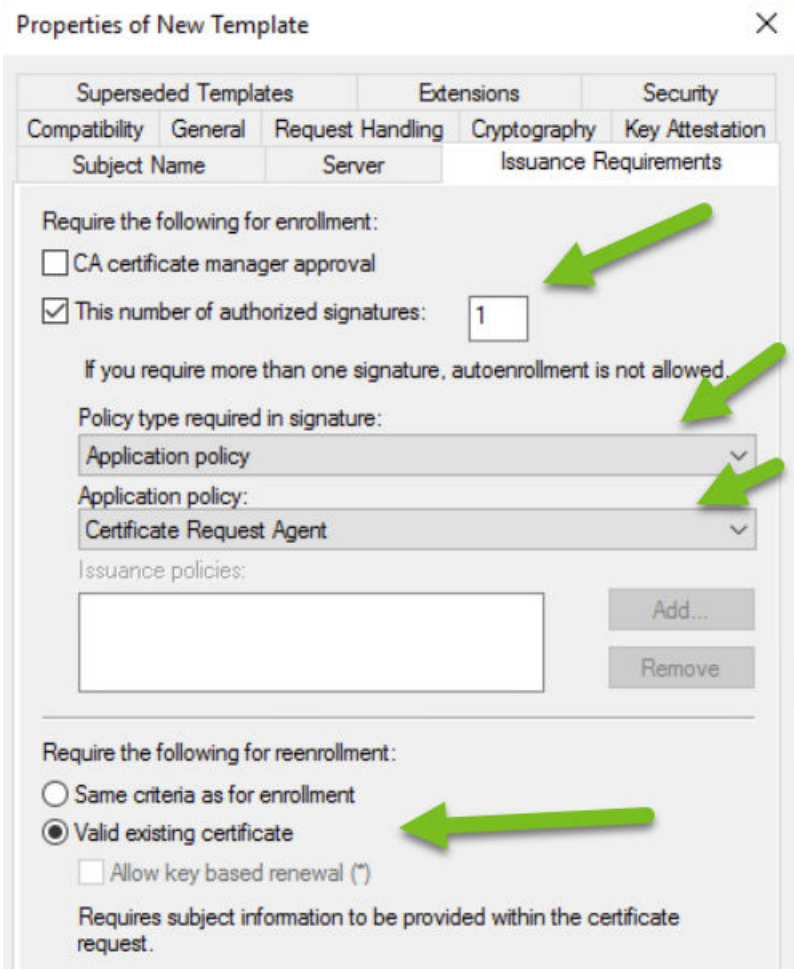
Lorsque vous cochez la première case, le système coche automatiquement **Ne pas inclure les informations de révocation dans les certificats émis**.

Veillez à décochez cette deuxième case **Ne pas inclure les informations de révocation dans les certificats émis**.



Onglet Exigences d'émission

- Nécessite les informations suivantes pour l'inscription : sélectionnez **Ce nombre de signatures autorisées**, puis entrez **1**.
- Type de stratégie requis dans la signature : stratégie d'application
- Politique d'application : agent de demande de certificat
- Nécessite les informations suivantes pour la réinscription : certificat existant valide

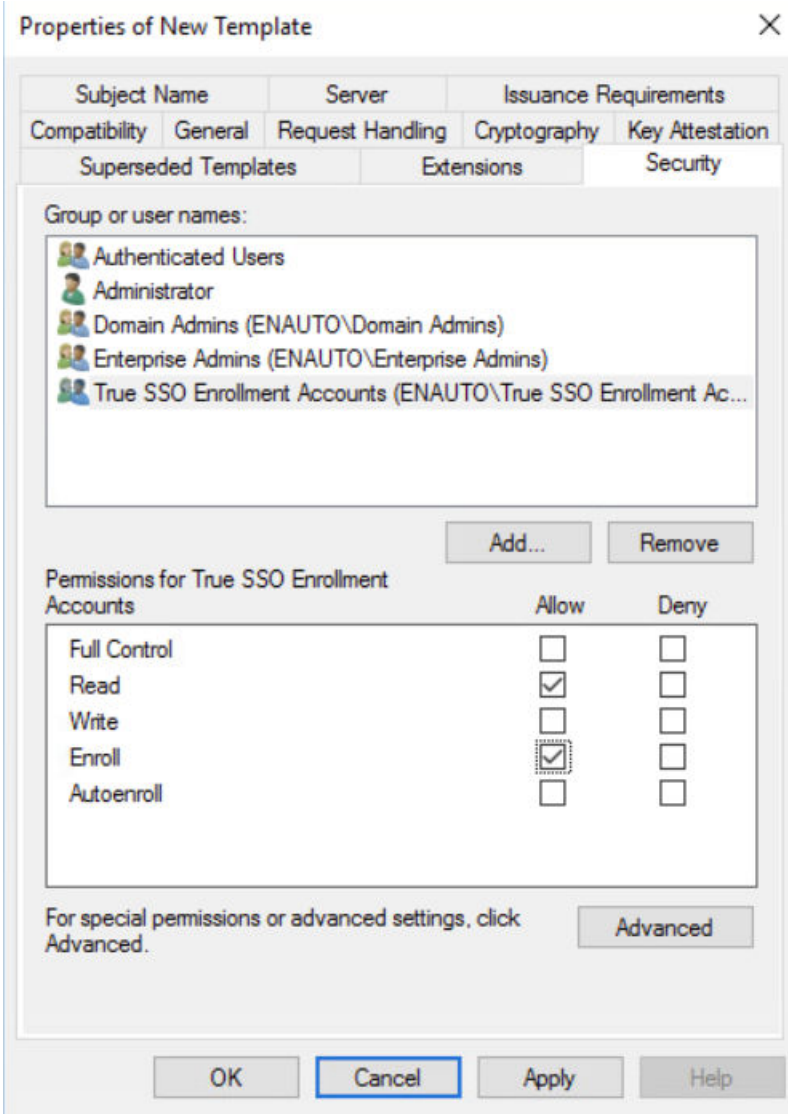


Onglet Sécurité

Dans l'onglet **Sécurité**, attribuez les autorisations `Read` et `Enroll` au nouveau groupe de sécurité universel que vous avez créé pour les comptes d'inscription True SSO.

1 Dans la section **Noms de groupes ou d'utilisateurs**, ajoutez le groupe que vous avez créé pour les comptes d'inscription True SSO.

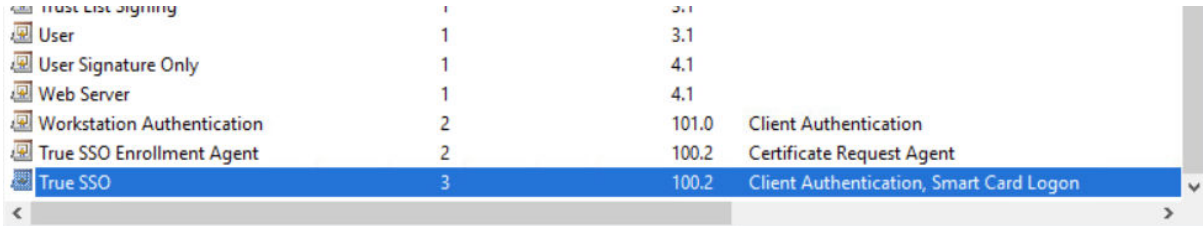
2 Sélectionnez ce groupe et dans la section Autorisations, sélectionnez **Autoriser** pour les autorisations `Read` et `Enroll`.



c Terminez l'enregistrement de ce nouveau modèle True SSO en cliquant sur **OK** dans la fenêtre **Propriétés du nouveau modèle**.

Le nouveau modèle True SSO est répertorié dans la console des modèles de certificat et affiché à l'aide du **Nom complet du modèle** que vous lui avez donné et avec l'objectif affiché d'authentification client et d'ouverture de session par carte à puce.

La capture d'écran suivante illustre le nouveau modèle répertorié.

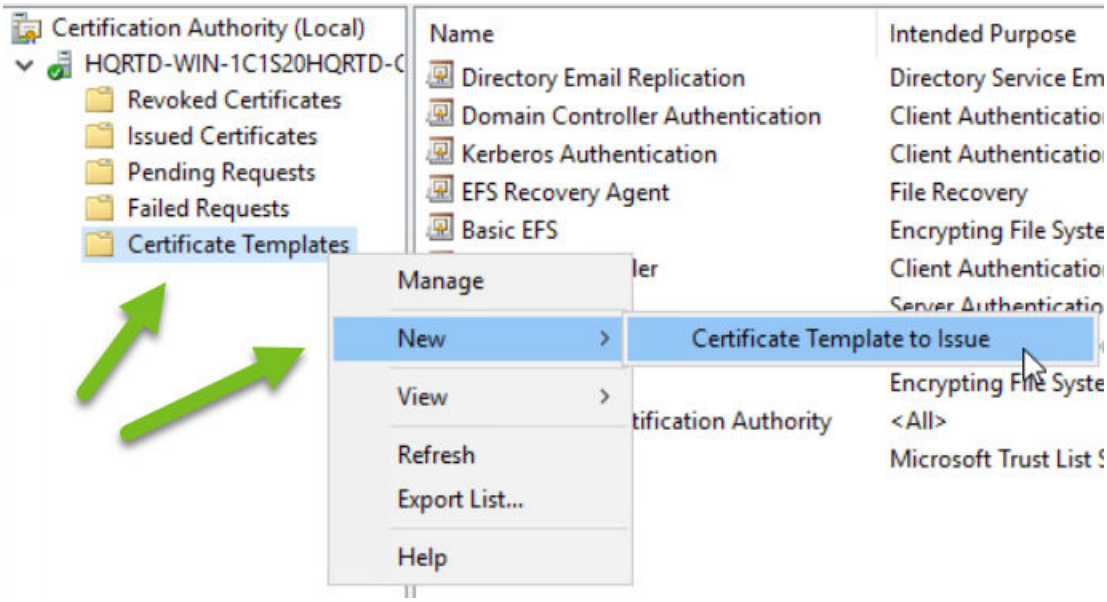


4 Vous pouvez maintenant fermer la console des modèles de certificat et revenir à l'outil Autorité de certification.

5 Émettez le modèle pour True SSO.

a Dans l'outil Autorité de certification, cliquez avec le bouton droit sur le dossier Modèles de certificat et sélectionnez **Nouveau > Modèle de certificat à émettre**.

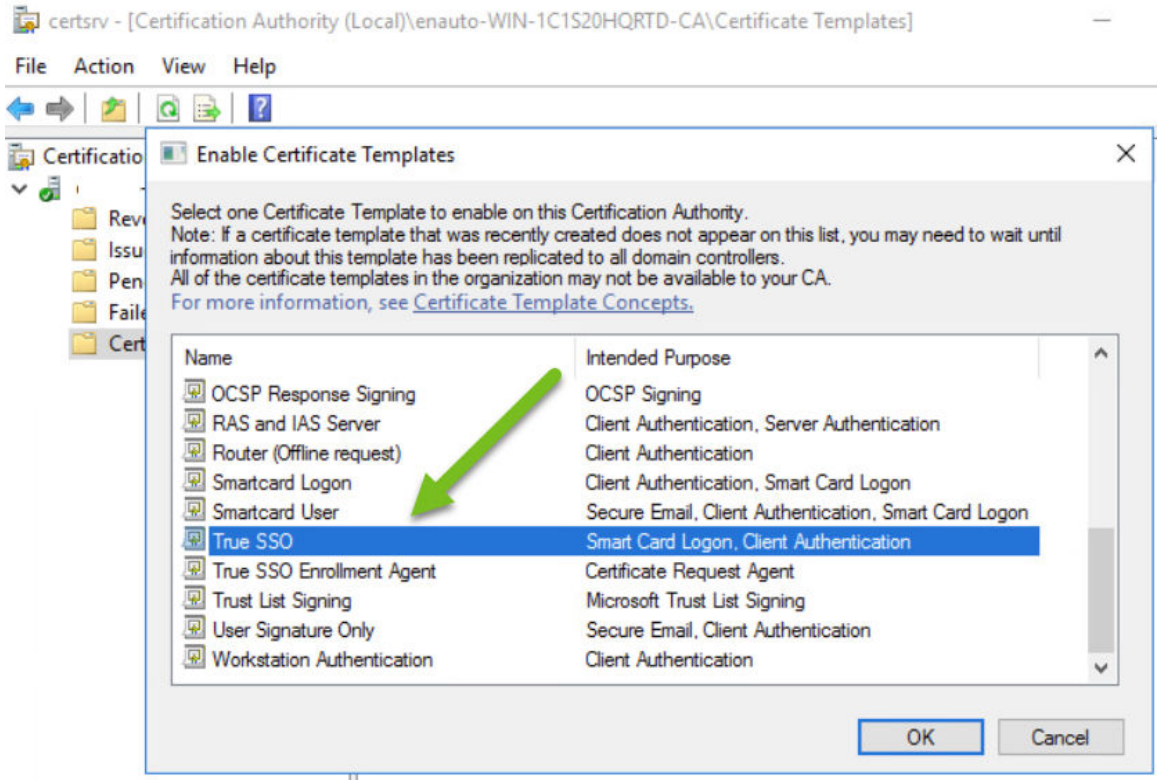
La capture d'écran suivante illustre cette étape dans un système exécutant Windows Server 2016.



La fenêtre Activer les modèles de certificat s'affiche.

b Sélectionnez le modèle True SSO que vous avez créé lors des étapes précédentes et cliquez sur **OK**.

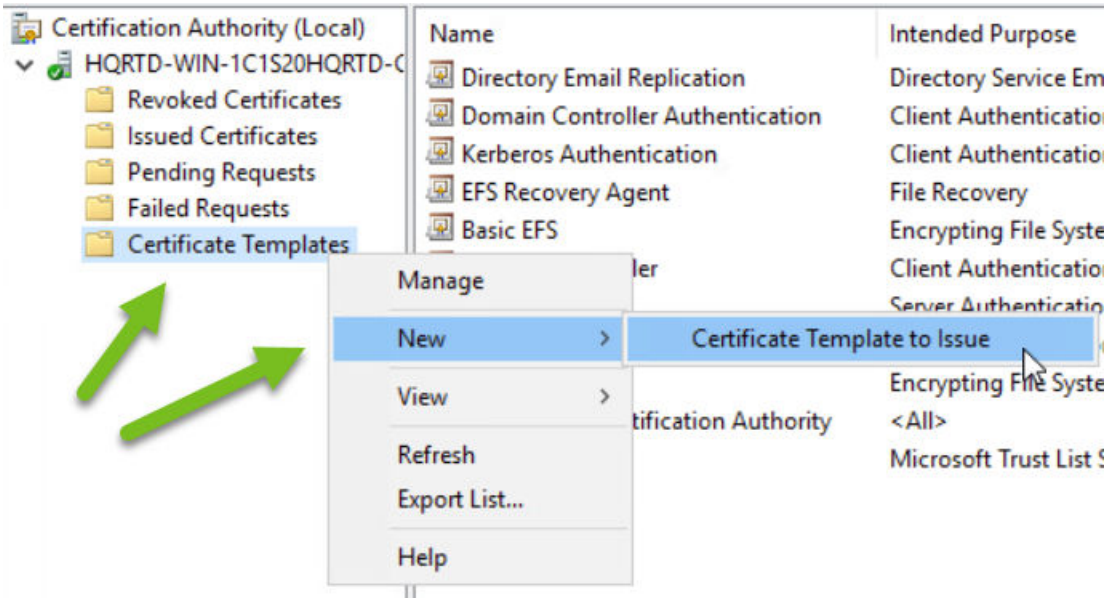
La capture d'écran suivante illustre cette étape dans un système exécutant Windows Server 2016.



Important Vous devez effectuer ces actions sur chaque instance d'autorité de certification d'entreprise Microsoft que vous prévoyez d'utiliser pour la fonctionnalité True SSO.

6 Répétez la même étape d'émission pour le modèle d'agent d'inscription True SSO.

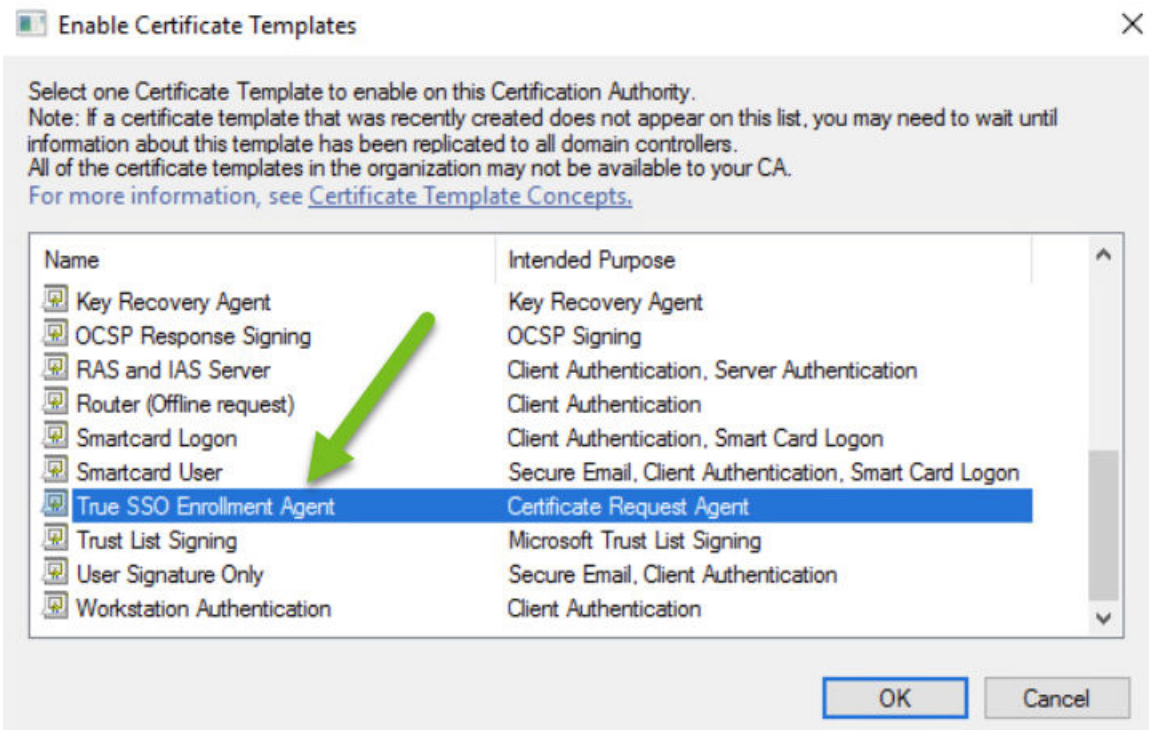
a Dans l'outil Autorité de certification, cliquez avec le bouton droit sur le dossier Modèles de certificat et sélectionnez **Nouveau > Modèle de certificat à émettre**.



La fenêtre Activer les modèles de certificat s'affiche.

b Sélectionnez le modèle Agent d'inscription True SSO que vous avez créé lors des étapes précédentes et cliquez sur **OK**.

La capture d'écran suivante illustre cette étape dans un système exécutant Windows Server 2016.



Important Vous devez effectuer ces actions sur chaque instance d'autorité de certification Microsoft Enterprise que vous prévoyez d'utiliser pour True SSO.

L'autorité de certification d'entreprise Microsoft est désormais configurée avec les modèles de certificat requis pour être utilisée avec la fonctionnalité True SSO.

Ajouter une configuration SSO à Horizon Cloud Service - nouvelle génération pour utiliser True SSO avec vos dispositifs Horizon Edge

Cette page de documentation décrit les étapes à suivre pour ajouter une configuration SSO qui configure l'utilisation de la fonctionnalité True SSO avec un dispositif Horizon Edge. Utilisez Horizon Universal Console pour ajouter la configuration SSO et l'associer au dispositif Horizon Edge.

Ajoutez une configuration SSO pour chaque forêt de domaines à partir de laquelle les utilisateurs lanceront des postes de travail qui utilisent SSO.

Vous pouvez effectuer ces étapes à l'aide d'Horizon Universal Console.

Vous pouvez créer plusieurs configurations True SSO pour la même forêt. Un domaine ne peut être associé qu'à une seule configuration True SSO (c'est-à-dire ajouté à une seule configuration True SSO).

Dans ce scénario, lorsqu'un utilisateur lance un poste de travail ou une application distante, le système choisit la configuration True SSO à utiliser en fonction des critères suivants par ordre de préférence :

1 Configuration True SSO qui contient le domaine de l'utilisateur.

2 Configuration True SSO provenant de la même forêt que le domaine de l'utilisateur.

Note Comme décrit à la page Types d'autorité de certification pris en charge pour l'utilisation de SSO avec un dispositif Horizon Edge dans Microsoft Azure, pour la fonctionnalité de True SSO, Horizon Universal Console utilise l'étiquette **Autorité de certification Microsoft**. Lorsque vous voyez l'étiquette **Autorité de certification Microsoft**, notez que celle-ci est associée à la fonctionnalité True SSO.

Conditions préalables

Vérifiez que vous ou votre équipe avez effectué les tâches suivantes.

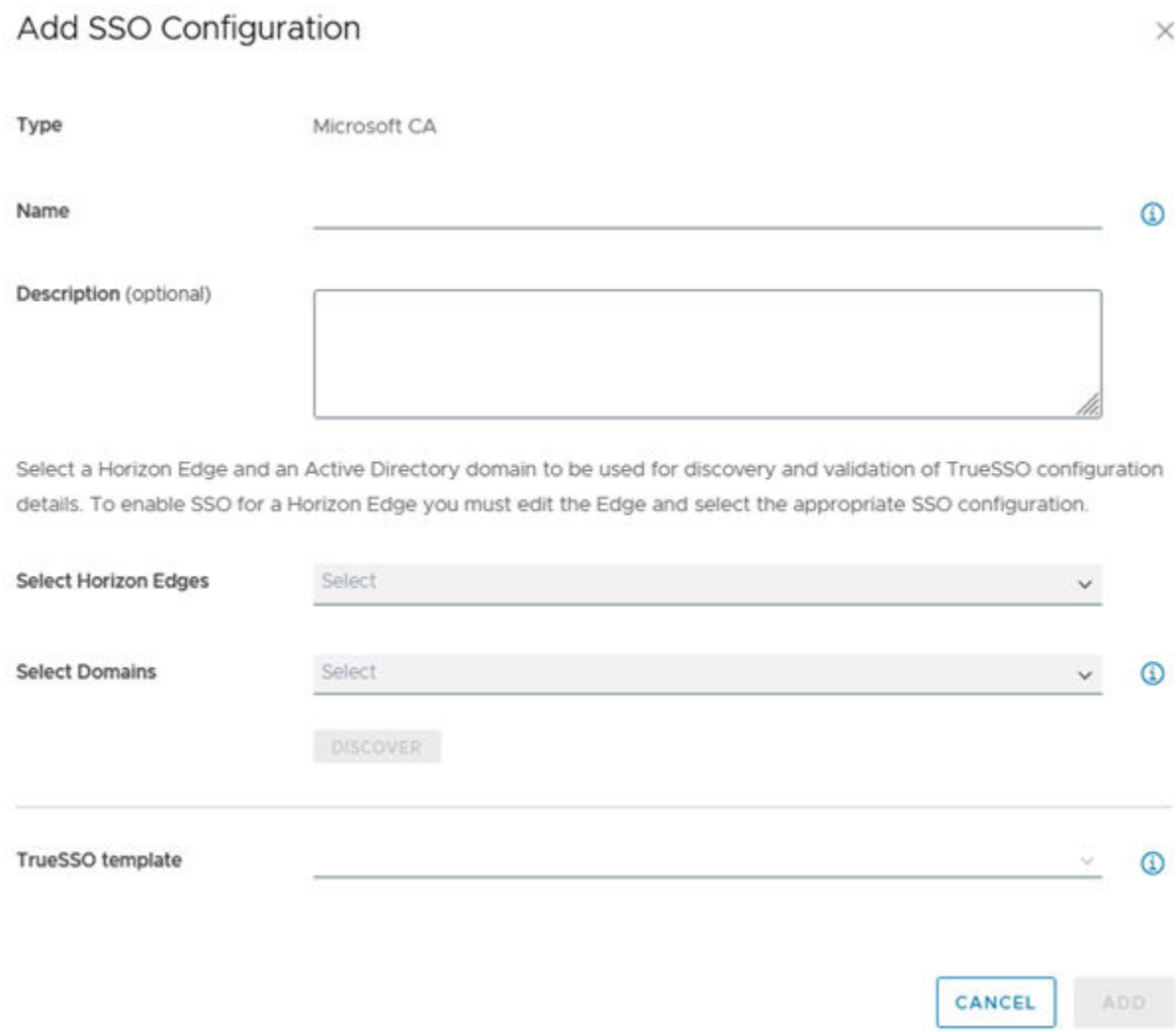
- Créez des comptes d'inscription de domaine dans les domaines Active Directory que vous prévoyez de sélectionner dans cette configuration SSO. Comme décrit sur la page Configuration de votre domaine Active Directory, un compte d'inscription de domaine est un compte de service d'inscription que la fonctionnalité True SSO utilise pour obtenir des certificats de courte durée auprès des services de certificats Microsoft Active Directory (AD CS). True SSO utilise les certificats pour l'authentification, afin d'éviter d'inviter les utilisateurs à entrer les informations d'identification Active Directory. Vous pouvez voir la console utiliser de façon interchangeable les termes Compte d'inscription de domaine, Compte de service d'inscription et Compte de service d'inscription de domaine.

- Assurez-vous que vous disposez d'au moins deux autorités de certification d'entreprise jointes au domaine configurées et disponibles pour True SSO.
- Créez un groupe de sécurité universel dans les domaines Active Directory et ajoutez ces comptes d'inscription de domaine à ce groupe, comme décrit dans Configurer les modèles de certificat requis pour True SSO avec Horizon Cloud.
- Suivez les étapes de création des modèles requis dans votre autorité de certification d'entreprise Microsoft, comme décrit dans Configurer les modèles de certificat requis pour True SSO avec Horizon Cloud.
- Pour les domaines Active Directory que vous prévoyez de sélectionner dans cette configuration SSO, spécifiez les comptes d'inscription dans la section **Compte de service d'inscription du domaine** de l'enregistrement de domaine Active Directory, comme décrit dans Configuration de votre domaine Active Directory.
- Choisissez les dispositifs Horizon Edge auxquels vous souhaitez appliquer cette configuration True SSO. Sélectionnez les dispositifs Horizon Edge dans le flux de l'interface utilisateur **Ajouter une configuration SSO**, décrit dans les étapes ci-dessous.

Procédure

1. Cliquez sur **Intégrations** dans la barre de navigation.
2. Cliquez sur **Gérer** sur la vignette **Identité et accès**.

3 Cliquez sur **Configurations SSO**, puis sélectionnez **Ajouter > Autorité de certification Microsoft** pour accéder à la page **Ajouter une configuration SSO**.



4 Ajoutez un **Nom** unique pour votre configuration SSO.

5 Sélectionnez un dispositif Horizon Edge dans le menu déroulant **Sélectionner les dispositifs Horizon Edge**.

Vous devez sélectionner au moins un dispositif Horizon Edge.

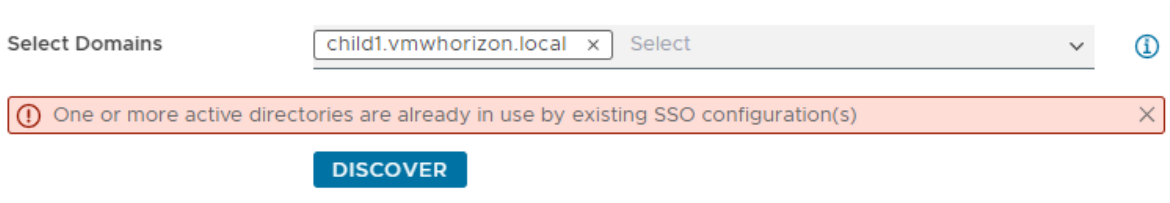
6 Sélectionnez les domaines pour votre configuration SSO dans le menu déroulant **Sélectionner des domaines**, puis cliquez sur **Ajouter**.

Vous pouvez ajouter plusieurs domaines pour votre configuration SSO. Les domaines doivent appartenir à la même forêt Active Directory.

Dans ce menu, la console répertorie tous les domaines enregistrés dans l'environnement (affichés dans l'onglet **Domaines** de la page Identité et accès de la console).

Cependant, chaque domaine que vous sélectionnez pour ce nouvel enregistrement de configuration SSO ne doit pas déjà être utilisé dans une autre configuration SSO déjà enregistrée dans le système.

Vous devez sélectionner un domaine qui n'est pas déjà spécifié dans une autre configuration SSO. L'interface utilisateur valide ce fait lorsque vous cliquez sur **Détecter** comme illustré dans la capture d'écran suivante. Au moment de la rédaction de ce document, le message de validation s'affiche comme indiqué.



7 Cliquez sur **Détecter** pour valider vos sélections.

Lorsque vous cliquez sur **Détecter**. Le système valide un certain nombre des conditions préalables décrites en haut de cette page, telles que :

- L'un des domaines sélectionnés est-il déjà utilisé dans une autre configuration SSO ?
- Les domaines sélectionnés disposent-ils de comptes de service d'inscription spécifiés dans leurs enregistrements de domaine (les enregistrements répertoriés dans l'onglet **Domaines** de la page Identité et accès de la console) ?
- Le système peut-il localiser les modèles de certificat requis dans l'autorité de certification d'entreprise Microsoft que vous ou votre équipe avez configurée en fonction des exigences de True SSO ?

Si la validation du système réussit pour tous les domaines, l'interface utilisateur met à disposition les menus suivants pour vos sélections.

8 Dans les menus déroulants **Modèle TrueSSO** et **Modèle d'agent d'inscription**, acceptez la sélection par défaut ou sélectionnez un autre modèle dans l'un menus ou les deux.

Note Si les deux modèles sélectionnés ont des instances d'autorité de certification en commun, ils sont répertoriés dans le menu déroulant **Autorités de certification**.

9 Cliquez sur **Ajouter** pour terminer l'enregistrement de la nouvelle configuration SSO dans le système.

Résultats

Le système envoie la configuration SSO à vos dispositifs Horizon Edge sélectionnés.

Note En ce qui concerne la page Configurations SSO, les configurations de True SSO sont répertoriées sur la page avec « CA Microsoft » comme valeur pour la colonne Type. En outre, pour les configurations d'autorité de certification Microsoft, le mode d'autorité de certification et le délai d'expiration du certificat ne s'appliquent pas. Par conséquent, les colonnes « Mode d'autorité de certification » et « Délai d'expiration du certificat » restent vides.

Étape suivante

À présent que votre configuration SSO est terminée, vous pouvez associer cette configuration SSO à un dispositif Horizon Edge spécifique. Sélectionnez **Capacité > Dispositifs Horizon Edge**, sélectionnez un dispositif Horizon Edge auquel associer votre configuration SSO récemment ajoutée, puis cliquez sur **Modifier**. Dans l'assistant **Modifier le dispositif Horizon Edge**, cliquez sur **Suivant** pour chaque étape de l'assistant jusqu'à ce que vous atteigniez la section **Passerelle Horizon Edge**, puis sélectionnez l'option **Utiliser SSO** pour l'activer. Sélectionnez le nom de votre configuration SSO récemment ajoutée, puis cliquez sur **Suivant** si nécessaire pour terminer l'assistant.

Vous pouvez spécifier l'utilisation de True SSO pour les postes de travail d'utilisateurs finaux et les applications distantes que ces dispositifs Dispositifs Horizon Edge fournissent. La spécification de l'utilisation de SSO pour les postes de travail et les applications distantes est définie au niveau d'un groupe de pools. Utilisez la navigation Horizon Universal Console **Ressources** pour accéder aux groupes de pools appropriés, puis modifiez les groupes de pools appropriés pour activer SSO sur chaque groupe de pools.

Pour utiliser la console afin de vérifier la configuration SSO définie sur un dispositif Horizon Edge spécifique, affichez sa page de détails en accédant à **Capacité > Dispositifs Horizon Edge** et en sélectionnant le nom du dispositif Horizon Edge.

Utilisation d'une instance de VMware CA pour SSO avec Horizon Cloud Service - next-gen

Pour fournir à vos utilisateurs finaux un accès Single Sign-On (SSO) à leurs postes de travail et applications à l'aide d'une autorité de certification (CA) VMware, utilisez VMware CA pour délivrer des certificats de carte à puce de courte durée pour SSO. Pour des raisons de transparence et de sécurité, le processus inclut un script PowerShell qui utilise des utilitaires Microsoft établis.

La liste suivante fournit des informations sur la configuration de VMware CA. Lorsque vous configurerez SSO, comme décrit dans les rubriques qui suivent, vous rencontrerez un grand nombre de ces mêmes détails contextuels. Par exemple, Ajouter une configuration SSO à Horizon Cloud Service - nouvelle génération pour une autorité de certification VMware CA fournit des instructions pour le téléchargement du bundle VMware CA. Ce bundle contient le script VMware PowerShell que vous exécuterez pour configurer SSO, comme indiqué dans Publier le bundle VMware SSO CA dans la forêt Active Directory.

- Pour activer la fonctionnalité requise par SSO avec une instance de VMware CA, votre forêt Active Directory doit présenter l'une des situations suivantes :
  - La forêt Active Directory dispose d'au moins une autorité de certification Microsoft Enterprise en ligne configurée à l'intérieur, auquel cas les résultats suivants s'affichent.
    - L'autorité de certification Microsoft Enterprise publie automatiquement ses certificats d'autorité de certification et ses listes de révocation de certificats (CRL) dans la forêt.
    - Les contrôleurs de domaine sont inscrits automatiquement pour les certificats.

    - La forêt Active Directory utilise une autorité de certification tierce ou une autorité de certification Microsoft autonome, auquel cas les conditions suivantes doivent s'appliquer.
        - Tous les certificats d'autorité de certification doivent être publiés manuellement dans la forêt à l'aide d'un utilitaire tel que `certutil`.
        - Les informations de révocation doivent toujours être disponibles sur HTTP.
        - Les contrôleurs de domaine doivent être émis avec des certificats autorisant l'authentification client, l'authentification du serveur, l'ouverture de session par carte à puce et l'authentification KDC.
- Vous pouvez configurer VMware CA comme autorité de certification racine ou intermédiaire. Toutefois, il est recommandé de sélectionner une autorité de certification intermédiaire pour l'infrastructure à clé publique (PKI, Public Key Infrastructure).
- Si vous utilisez une autorité de certification racine, le certificat VMware CA est valide pendant 5 ans.
- Si vous utilisez une autorité de certification intermédiaire, l'autorité de certification émettrice détermine la période de validité du certificat VMware CA.
- Si vous utilisez une autorité de certification intermédiaire, le certificat VMware CA peut être signé par une autorité de certification Microsoft ou par n'importe quelle autorité de certification tierce.
- Si vous utilisez cette dernière, assurez-vous que les machines membres du domaine ont accès à tous les certificats et aux informations de révocation nécessaires à la validation du certificat VMware CA.
- Pour que l'instance de VMware CA soit approuvée, vous devez publier le bundle VMware CA à différents emplacements de la forêt Active Directory.
- Publiez le bundle VMware CA en exécutant le script VMware PowerShell en tant qu'administrateur disposant d'autorisations appropriées sur une machine membre du domaine.
- Vous ne devez utiliser que le script VMware PowerShell. Active Directory réplique les données PKI publiées sur tous les contrôleurs de domaine et postes de travail de tous les domaines de la forêt Active Directory. Vous pouvez utiliser un utilitaire tel que `Repadmin` dans des déploiements d'Active Directory complexes pour garantir une réplication rapide du contexte d'attribution de nom de configuration entre des contrôleurs de domaine dans différents domaines ou sites avant de tenter SSO.
- Le script PowerShell utilise des utilitaires Microsoft `certreq` et `certutil` pour une transparence complète. Avant d'exécuter le script PowerShell, vous pouvez le lire pour connaître précisément ses fonctions.

Préparer Active Directory pour une configuration SSO avec une autorité de certification VMware CA et applicable à plusieurs forêts

Lorsque vous configurez SSO pour votre instance d'Horizon Cloud, vous devez effectuer les tâches appropriées ci-après, en fonction de la configuration de votre autorité de certification VMware (CA).

Résumé des procédures qui suivent

Lorsque vous créez un bundle SSO, utilisez le script PowerShell pour publier le bundle dans la forêt pour laquelle le bundle a été créé. Cette action garantit que l'authentification unique SSO est fonctionnelle pour la forêt du bundle.

Pour que SSO soit compatible avec des forêts d'approbation supplémentaires, des certificats racines et intermédiaires provenant du chemin de certification de VMware CA doivent être publiés dans la forêt d'approbation, comme suit.

- Les certificats d'autorité de certification racine doivent être publiés sur la forêt d'approbation.
- Les certificats d'autorité de certification intermédiaire doivent être publiés sur la forêt d'approbation.
- Les certificats d'autorité de certification racine doivent être publiés sur le magasin NTAuth.
- Les informations de révocation doivent toujours être disponibles sur HTTP pour l'intégralité de la chaîne de certificats.

Ajouter le certificat racine aux autorités de certification racine approuvées

Le certificat racine terminant le chemin de certification VMware CA doit être ajouté à la stratégie de groupe Autorités de certification racines de confiance dans Active Directory.

Procédure

1. Dans toutes les forêts Active Directory qui font partie de la configuration d'approbation, ajoutez le certificat racine aux autorités de certification racine de confiance.
   a. Sélectionnez **Démarrer > Outils d'administration > Gestion de stratégie de groupe**.
   b. Développez votre domaine, cliquez avec le bouton droit sur **Stratégie de domaine par défaut**, puis cliquez sur **Modifier**.
2. Développez la section **Configuration ordinateur** et ouvrez le dossier **Paramètres Windows\Paramètres de sécurité\Clé publique**.
3. Cliquez avec le bouton droit sur **Autorités de certification racines de confiance** et sélectionnez **Importer**.
4. Suivez les invites de l'assistant pour importer le certificat racine (par exemple, `rootCA.cer`) et cliquez sur **OK**.
5. Fermez la fenêtre Stratégie de groupe.

Résultats

Tous les systèmes du domaine contiennent désormais une copie du certificat racine dans leur magasin racine approuvé.

Étape suivante

Si une autorité de certification (CA) intermédiaire émet vos certificats d'ouverture de session par carte à puce ou de contrôleur de domaine, ajoutez le certificat intermédiaire à la stratégie de groupe Autorités de certification intermédiaires dans Active Directory. Reportez-vous à la section Ajouter un certificat intermédiaire à des autorités de certification intermédiaires.

Ajouter un certificat intermédiaire à des autorités de certification intermédiaires

Vous devez ajouter tous les certificats intermédiaires du chemin de certification VMware CA à la stratégie de groupe Autorités de certification intermédiaires dans Active Directory.

Procédure

1. Dans toutes les forêts Active Directory qui font partie de la configuration de l'approbation, ajoutez tous les certificats intermédiaires faisant partie de la chaîne de certificats VMware CA aux autorités de certification intermédiaires. Sur le serveur Active Directory, accédez au plug-in Gestion de stratégie de groupe et effectuez les étapes suivantes :
   a. Sélectionnez **Démarrer > Outils d'administration > Gestion de stratégie de groupe**.
   b. Développez votre domaine, cliquez avec le bouton droit sur **Stratégie de domaine par défaut** et cliquez sur **Modifier**.
2. Développez la section **Configuration ordinateur** et ouvrez la stratégie de **Paramètres Windows\Paramètres de sécurité\Clé publique**.
3. Cliquez avec le bouton droit sur **Autorités de certification intermédiaires** et sélectionnez **Importer**.
4. Suivez les invites de l'assistant pour importer le certificat intermédiaire (par exemple, `intermediateCA.cer`) et cliquez sur **OK**.
5. Fermez la fenêtre Stratégie de groupe.

Résultats

Tous les systèmes du domaine contiennent désormais une copie du certificat intermédiaire dans leur magasin d'autorité de certification intermédiaire.

Ajouter le certificat racine au magasin Enterprise NTAuth

Vous devez ajouter le certificat racine terminant le chemin de certification VMware CA au magasin Enterprise NTAuth dans Active Directory.

Procédure

- Sur votre serveur Active Directory, utilisez la commande `certutil` pour publier le certificat dans le magasin Enterprise NTAuth.

  Par exemple : **`certutil -dspublish -f path_to_root_CA_cert NTAuthCA`**

Résultats

L'autorité de certification est désormais approuvée pour émettre des certificats de ce type.

Ajouter une configuration SSO à Horizon Cloud Service - nouvelle génération pour une autorité de certification VMware CA

Vous pouvez ajouter une configuration SSO pour qu'une autorité de certification VMware CA puisse se déployer sur la passerelle Horizon Edge.

Ajoutez une configuration SSO pour chaque forêt de domaines à partir de laquelle les utilisateurs lanceront des postes de travail qui utilisent SSO.

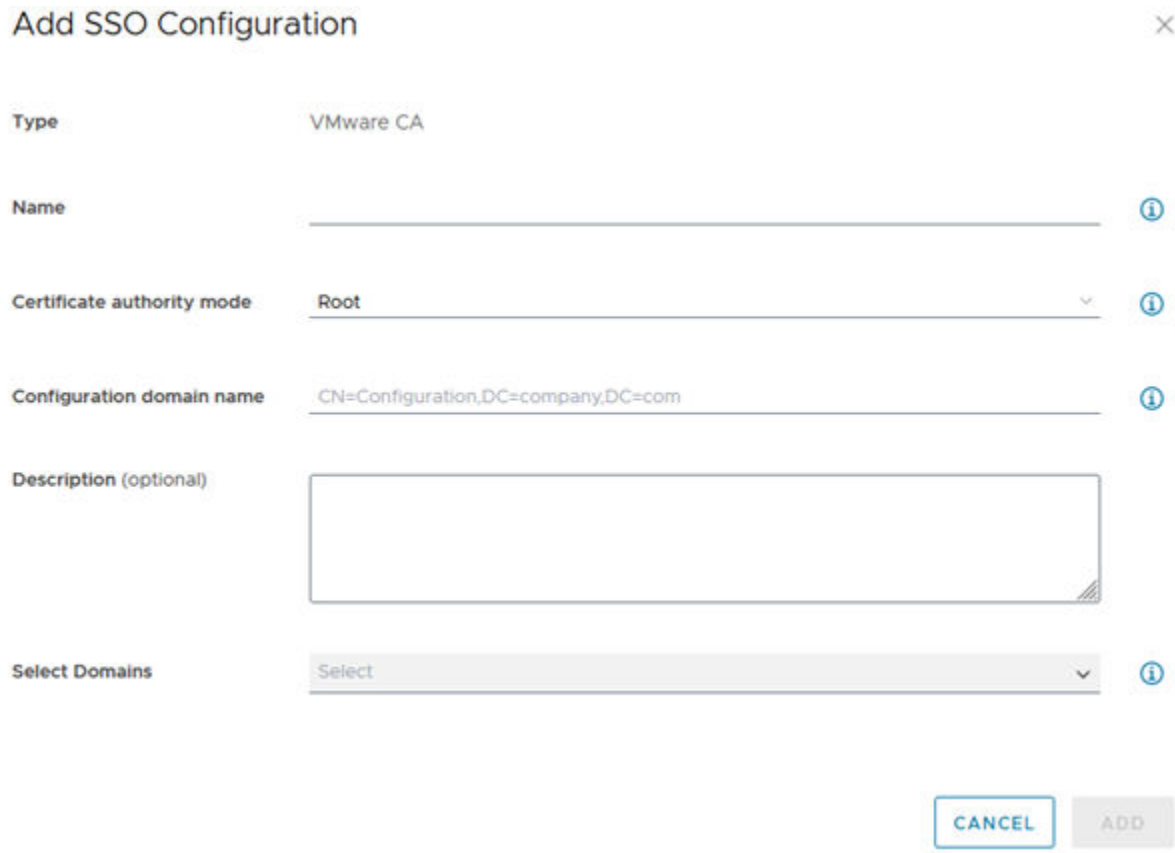
Conditions préalables

Choisissez le mode d'autorité de certification à utiliser pour votre autorité de certification VMware CA, autorité de certification racine ou autorité de certification intermédiaire. Reportez-vous à la section Utilisation d'une instance de VMware CA pour SSO avec Horizon Cloud Service - next-gen.

Procédure

1. Cliquez sur **Intégrations** dans la barre de navigation.
2. Cliquez sur **Gérer** sur la vignette **Identité et accès**.

3 Cliquez sur **Configurations SSO**, puis sélectionnez **Ajouter > VMware CA** pour accéder à la page **Ajouter une configuration SSO**.



4 Ajoutez un **Nom** unique pour votre configuration SSO.

5 Sélectionnez un mode **Autorité de certification** entre **Racine** et **Intermédiaire** pour déterminer le type de bundle d'autorité de certification (CA) à télécharger et à installer sur le serveur AD.

Le mode Racine crée un bundle d'autorité de certification avec un certificat racine auto-signé. Le mode intermédiaire crée un bundle d'autorité de certification avec un fichier de demande de signature de certificat (CSR). Le script PowerShell affiche une interface utilisateur permettant à l'administrateur de choisir l'autorité de certification d'entreprise à laquelle la CSR sera envoyée pour obtenir un certificat.

6 Ajoutez un **Nom de domaine de la configuration** pour déterminer le contexte d'attribution de nom de configuration de la forêt AD pour votre configuration SSO.

Le **Nom de domaine de la configuration** est généralement composé de CN=Configuration et de noms uniques relatifs au domaine de configuration et au domaine racine de la forêt (CN=Configuration,DC=company,DC=com). Pour identifier le contexte d'attribution de nom de la configuration, connectez-vous à une machine jointe au domaine et exécutez la commande PowerShell `"C:> Get-ADRootDSE -Server "`.

7 Sélectionnez l'option **Domaines** pour votre configuration SSO et cliquez sur **Ajouter**.

Vous pouvez ajouter plusieurs domaines pour votre configuration SSO. Les domaines doivent appartenir à la même forêt AD. Chaque domaine ne peut se trouver que dans une seule configuration SSO.

8 Après avoir ajouté la configuration SSO, cliquez sur son menu (trois points verticaux) et téléchargez le bundle d'autorité de certification (CA) à installer sur AD.

Étape suivante

- Publiez le bundle téléchargé. Reportez-vous à la section Publier le bundle VMware SSO CA dans la forêt Active Directory.
- Avant l'expiration d'un certificat d'autorité de certification VMware SSO, demandez un nouveau bundle d'autorité de certification.

  Note Des notifications s'affichent dans Horizon Universal Console pour vous informer que l'expiration de vos certificats d'autorité de certification approche.

  - Vous pouvez vérifier la date d'expiration de vos certificats d'autorité de certification sur la page Configurations SSO, en particulier dans la colonne **Délai d'expiration du certificat**.
  - Demandez le bundle d'autorité de certification sur la page Configuration SSO à tout moment en cliquant sur le menu de cette configuration SSO (trois points verticaux) et en sélectionnant **Générer un bundle d'autorité de certification**. Cette action génère le bundle d'autorité de certification et le télécharge sur votre système. Reportez-vous à la section Publier le bundle VMware SSO CA dans la forêt Active Directory.
- À présent que votre configuration SSO est terminée, vous pouvez associer cette configuration SSO à un dispositif Horizon Edge spécifique. Sélectionnez **Capacité > Dispositifs Horizon Edge**, sélectionnez un dispositif Horizon Edge auquel associer votre configuration SSO récemment ajoutée, puis cliquez sur **Modifier**. Dans l'assistant **Modifier le dispositif Horizon Edge**, cliquez sur **Suivant** pour chaque étape de l'assistant jusqu'à ce que vous atteigniez la section **Passerelle Horizon Edge**, puis sélectionnez l'option **Utiliser SSO** pour l'activer. Sélectionnez le nom de votre configuration SSO récemment ajoutée, puis cliquez sur **Suivant** si nécessaire pour terminer l'assistant.

Publier le bundle VMware SSO CA dans la forêt Active Directory

Pour fournir aux utilisateurs finaux un accès Single Sign-On (SSO) à leurs postes de travail et applications, administrez SSO sur l'instance d'Passerelle Horizon Edge correspondante.

Cette procédure permet aux utilisateurs finaux d'accéder à leurs postes de travail et applications une fois qu'ils ont entré une fois leurs informations d'identification.

Pour plus d'informations générales sur la configuration de VMware CA, reportez-vous à la section Utilisation d'une instance de VMware CA pour SSO avec Horizon Cloud Service - next-gen

Reportez-vous à la documentation Microsoft si nécessaire pour terminer cette procédure. Par exemple, pour installer une autorité de certification d'entreprise, reportez-vous à la section Installer l'autorité de certification.

Conditions préalables

- Utilisez Horizon Universal Console pour créer et télécharger un bundle d'autorité de certification (CA). Reportez-vous à la section Ajouter une configuration SSO à Horizon Cloud Service - nouvelle génération pour une autorité de certification VMware CA.
- Pour exécuter le script PowerShell extrait du bundle VMware CA, comme décrit dans cette procédure, confirmez que vous disposez des autorisations appropriées.

  Cette procédure nécessite l'exécution du script VMware PowerShell. Vous disposez de quelques options pour exécuter le script VMware PowerShell, notamment l'exécution du script en tant que membre du groupe d'administrateurs d'entreprise. Les instructions suivantes vous suggèrent d'utiliser des autorisations moins puissantes, mais l'exécution du script en tant que membre du groupe d'administrateurs d'entreprise est à votre disposition. La suggestion ici consiste à confirmer que vous disposez des autorisations suivantes.

  - Autorisations de contrôle total sur le conteneur « Services de clés publiques » dans Active Directory.
  - Autorisations d'inscription sur le modèle de certificat « SubCA » dans Active Directory.

Procédure

1. Connectez-vous à une machine membre du domaine, chargez le fichier de bundle d'autorité de certification sur le serveur et décompressez le contenu du fichier.

   Tant que vous disposez des autorisations appropriées, vous pouvez exécuter le script PowerShell à partir de n'importe quelle machine membre du domaine.

2 Ouvrez PowerShell, exécutez les commandes et répondez aux invites, comme décrit dans les sous-étapes suivantes.

Important Si votre déploiement se compose de plusieurs contrôleurs de domaine ou que vous installez le bundle à partir d'une machine distante, la propagation du certificat d'autorité de certification à tous les contrôleurs de domaine peut prendre plusieurs heures. Vous pouvez réduire le délai d'exécution en exécutant `'gpupdate.exe /Target:Computer /Force'` sur toutes les instances de contrôleurs de domaine.

a Exécutez la commande suivante.

```
Unblock-File -Path Path to ps1 file
```

b Exécutez le script PowerShell `ps1` extrait du bundle d'autorité de certification et répondez aux invites.

Par exemple, `PS C:\ca\VmwAuthEngine-CA_1> .\VmwAuthEngine-CA_1.ps1`

Si vous avez ajouté votre configuration SSO comme autorité de certification intermédiaire, vous êtes invité à sélectionner une autorité de certification d'entreprise MSFT pour signer la CSR de VMware CA. Vous pouvez choisir une autorité de certification d'entreprise MSFT racine ou intermédiaire pour traiter la CSR de VMware CA. Le cas échéant, sélectionnez l'autorité de certification d'entreprise appropriée. Vous devez activer le modèle **Autorité de certification subordonnée** pour l'autorité de certification d'entreprise sélectionnée.

Répondez à l'invite de confirmation requise suivante avec **`Y`** comme illustré.

```
Confirmation requise. Voulez-vous effectuer la publication dans AD ?
```

`N] No [Y] Yes [?] Help (default is "N"):Y`

Résultats

Le résultat attendu est que le script s'exécute sans erreur. Cependant, si vous rencontrez le type d'erreur suivant, effectuez la suggestion de dépannage fournie.

```
2022-03-22T15:35:39 [INFO ] [VmwAuthEngine-CA-62351bb62ff3dd5966ad3575-1.ps1,67] certutil.exe
-dspublish -f C:\SSO-C\Vmw
AuthEngine-CA-62351bb62ff3dd5966ad3575-1.crl
error : 2022-03-22T15:35:39 [ERROR][-2147016563][] Failed to publish base CRL
At C:\SSO-C\VmwAuthEngine-CA-62351bb62ff3dd5966ad3575-1.ps1:303 char:5
+     error $retCode "Failed to publish base CRL"
+     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException
    + FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,error
```

Exécutez la commande `Get-ADRootDSE` suivante et vérifiez la sortie pour savoir si le nom de domaine de configuration de l'autorité de certification utilisé pour créer la configuration SSO correspond aux éléments que la propriété suivante renvoie : `configurationNamingContext`.

```
C:\>
        Get-ADRootDSE -Server dnsDomainName
```

Par exemple, `C:\> Get-ADRootDSE -Server horizonv2.local`

Sortie :

```
configurationNamingContext       :  "CN=Configuration,DC=horizonv2,DC=local"
        ...other
        output fields...
```

Si le nom de domaine de configuration de l'autorité de certification ne correspond pas à la sortie, vous pouvez utiliser Horizon Universal Console pour modifier la configuration SSO, en particulier pour corriger le nom de domaine de la configuration de l'autorité de certification. Pour plus d'informations sur l'accès à la configuration SSO, reportez-vous à la section Ajouter une configuration SSO à Horizon Cloud Service - nouvelle génération pour une autorité de certification VMware CA. Pour modifier une configuration SSO, cliquez sur les trois points verticaux en regard de la configuration SSO et sélectionnez **Modifier**. Après avoir corrigé le nom de domaine, vous pouvez télécharger et publier le bundle d'autorité de certification mis à jour.

Étape suivante

Après avoir déployé Passerelle Horizon Edge, vérifiez que l'état de configuration SSO est défini correctement. Dans Horizon Universal Console, sélectionnez **Ressources > Capacité**, cliquez sur le nom de l'instance d'Passerelle Horizon Edge que vous avez configurée et modifiez la configuration pour activer l'option **Utiliser SSO**. Sélectionnez la configuration SSO pour l'associer à la Passerelle Horizon Edge. Enregistrez et vérifiez que l'état est correctement défini sur READY_TO_SERVE, ce qui indique que l'authentification SSO est fonctionnelle pour les utilisateurs finaux.

Connexion de votre fournisseur d'identité

Une fois les informations de domaine enregistrées dans Horizon Cloud Service - next-gen, connectez votre fournisseur d'identité pour l'authentification et l'accès des utilisateurs finaux.

Les informations suivantes s'appliquent à la tâche qui suit pour la connexion de votre fournisseur d'identité.

Lorsque Microsoft Entra ID est votre fournisseur d'identité, un utilisateur disposant de privilèges d'administrateur global doit effectuer les opérations suivantes.

- Approuvez les autorisations demandées.
- Donnez votre consentement à l'ensemble de l'organisation.

- Donnez votre consentement pour que l'application Entra ID accède aux données de votre organisation.

Lorsque Workspace ONE Access est votre fournisseur d'identité, un utilisateur disposant de privilèges d'administrateur doit effectuer les opérations suivantes.

- Approuvez les autorisations demandées.
- Donnez votre consentement à l'ensemble de l'organisation.

Procédure

1 Cliquez sur **Intégrations** dans la barre de navigation.

2 Cliquez sur **Gérer** sur la vignette **Identité et accès**.

3 Sur la page **Identité et accès**, sélectionnez le **Fournisseur d'identité** parmi **Microsoft Azure**, **Cloud Workspace ONE Access** et **Workspace ONE Access sur site** dans le menu déroulant.

Microsoft Azure

a Ajoutez le **Sous-domaine de locataire** pour l'**URL du Broker** pour que vos utilisateurs finaux disposent de leurs droits d'accès.

Si vous n'êtes pas **Administrateur global**, cliquez sur **Générer un lien** pour générer un lien et le partager avec votre administrateur pour demander son approbation.

b Cliquez sur **Se connecter**.

c Vérifiez le contenu de la page, puis cliquez sur **Accepter** pour accorder des autorisations permettant d'accéder à la console Horizon Universal Console.

Procédez comme suit selon les invites.

Cloud Workspace ONE Access

a Ajoutez le **Sous-domaine de locataire** pour l'**URL du Broker** pour que vos utilisateurs finaux disposent de leurs droits d'accès.

b Ajoutez le **Nom de domaine complet de locataire Workspace ONE Access** au format `yourcompany.workspaceoneaccess.com`.

c Cliquez sur **Se connecter** pour accéder à Horizon Universal Console.

Workspace ONE Access sur site

a Ajoutez le **Sous-domaine de locataire** pour l'**URL du Broker** pour que vos utilisateurs finaux disposent de leurs droits d'accès.

b Ajoutez le **Nom de domaine complet de locataire Workspace ONE Access** au format `yourcompany.workspaceoneaccess.com`.

c Entrez l'**ID de client** OAuth configuré sur WS1A sur site.

d Entrez le **Secret du client** OAuth configuré sur WS1A sur site.

e Cliquez sur **Se connecter** pour accéder à Horizon Universal Console.

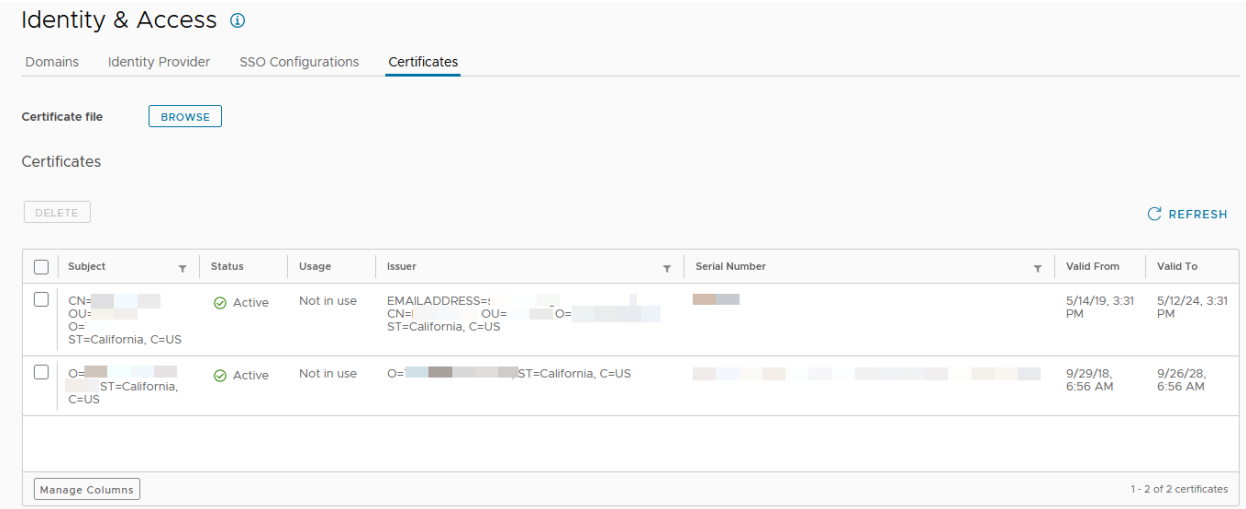
Étape suivante

Ajoutez un dispositif Horizon Edge.

Gestion des certificats PEM à utiliser avec LDAPS

Pour utiliser LDAPS avec Horizon Cloud Service - next-gen, vous devez charger des certificats d'autorité de certification racine et intermédiaire codés au format PEM, que vous pouvez gérer ultérieurement avec Horizon Universal Console sur la page Certificats.

Vous pouvez charger des certificats d'autorité de certification racine et intermédiaire codés au format PEM lorsque vous configurez votre domaine Active Directory. Ces certificats sont disponibles sur la page Certificats. Pour y accéder, cliquez sur **Intégrations** dans le volet de gauche, puis dans l'onglet **Identité et accès**, cliquez sur **Gérer**.



Vous pouvez effectuer les actions suivantes sur la page Certificats.

- Supprimer les certificats existants.
- Ajouter des certificats.

  Pour ajouter des certificats, cliquez sur **Parcourir**, sélectionnez le fichier codé au format PEM contenant les certificats de votre système à charger, puis, de retour sur la page Certificats, cliquez sur **Charger**.
- Effectuer une recherche dans les certificats existants à l'aide des filtres de colonne.

Note Utiliser la colonne État pour déterminer si les certificats expirent bientôt ou ont déjà expiré, et si vous devez charger de nouveaux certificats ou supprimer d'anciens certificats.

- **Actif** : le certificat est valide et n'expire pas bientôt.
- **Expiration** : le certificat expire dans les 30 jours.
- **Expiré** : le certificat a expiré.

Configuration de Dynamic Environment Manager dans Horizon Cloud Service - next-gen

Vous pouvez configurer Dynamic Environment Manager devant être utilisé par Horizon Agent pour personnaliser les VM.

Pour plus d'informations sur Dynamic Environment Manager, reportez-vous à la documentation de Dynamic Environment Manager.

Procédure

1. Cliquez sur **Paramètres** dans la barre de navigation.
2. Cliquez sur **Gérer** sur la vignette **Dynamic Environment Manager** pour accéder à la page **Dynamic Environment Manager**.
3. Dans **Dynamic Environment Manager**, cliquez sur **Ajouter** pour ajouter la configuration de Dynamic Environment Manager.
4. Sur la page **Ajouter une configuration de Dynamic Environment Manager**, ajoutez un nom unique pour votre configuration et fournissez le chemin d'accès au partage de fichiers dans lequel les paramètres de configuration sont stockés.
5. Cliquez sur **Enregistrer**.

   Vous pouvez également **modifier** ou **supprimer** votre configuration de Dynamic Environment Manager.

Configuration de votre fournisseur d'identité

Horizon Cloud Service - next-gen repose sur un fournisseur d'identité externe et prend actuellement en charge Microsoft Entra ID et Workspace ONE Access. Le fournisseur d'identité que vous configurez avec Horizon Cloud Service - next-gen effectue l'authentification requise lorsque les utilisateurs tentent d'accéder à leurs postes de travail.

Dans les deux cas, pour Microsoft Entra ID ou Workspace ONE Access, vous devez connecter un annuaire Active Directory sur site au fournisseur d'identité externe.

Si votre fournisseur d'identité n'est pas encore intégré à votre annuaire Active Directory sur site, suivez les instructions applicables ci-après en fonction de votre fournisseur d'identité choisi.

Configurer Microsoft Entra ID comme fournisseur d'identité

Dans Horizon Cloud Service - next-gen, si vous utilisez Microsoft Entra ID comme fournisseur d'identité, et que Microsoft Entra ID n'est pas encore intégré à votre annuaire Active Directory sur site, procédez comme suit.

Effectuez les tâches d'enregistrement et de synchronisation de Microsoft Azure.

Conditions préalables

- Vérifiez que vous avez accès à Horizon Cloud. Pour créer une connexion, reportez-vous à la section Chapitre 4 Intégration pour les administrateurs Horizon Cloud Service - next-gen.

- Vérifiez que le serveur Active Directory sur site est pris en charge.

Procédure

1. Si vous ne disposez pas d'un locataire existant, créez un locataire Microsoft Azure. Reportez-vous à la documentation de Microsoft, telle que Démarrage rapide : créer un locataire dans Azure Active Directory.
2. Créez un utilisateur sur Microsoft Azure avec un rôle Administrateur global.
3. Synchronisez votre annuaire Active Directory sur site avec Microsoft Azure.
   a. Sur le serveur Active Directory sur site, créez des utilisateurs et des groupes, et attribuez les utilisateurs aux groupes.

      Vérifiez que tous les utilisateurs sont membres d'un groupe.

   b. Installez Microsoft Entra ID Connect sur le serveur Active Directory sur site pour lier Microsoft Azure. Pour obtenir des instructions d'installation, reportez-vous à la documentation de Microsoft, telle que Conditions préalables pour Azure AD Connect.

   c. Lorsque la configuration de Microsoft Entra ID Connect est terminée, vérifiez que les utilisateurs et les groupes sont créés dans Microsoft Entra ID.

Étape suivante

Créez les comptes de domaine Active Directory requis. Reportez-vous à la section Création de comptes de liaison de domaine et de jonction de domaine dans Active Directory.

Configurer Workspace ONE Access comme fournisseur d'identité

Dans Horizon Cloud Service - next-gen, si vous utilisez Workspace ONE Access comme fournisseur d'identité et que Workspace ONE Access n'est pas encore intégré à votre annuaire Active Directory sur site, procédez comme suit.

Conditions préalables

- Vérifiez que vous avez accès à Horizon Cloud. Pour créer une connexion, reportez-vous à la section Chapitre 4 Intégration pour les administrateurs Horizon Cloud Service - next-gen.
- Vérifiez que le serveur Active Directory sur site est pris en charge.
- Vérifiez que vous disposez d'un locataire Workspace ONE Access.

Procédure

1. Intégrez votre annuaire Active Directory sur site à Workspace ONE Access.

   Reportez-vous à la rubrique Intégration d'annuaire à VMware Workspace ONE Access de la documentation de Workspace ONE Access.
2. Créez les comptes de domaine Active Directory requis.

   Reportez-vous à la section Création de comptes de liaison de domaine et de jonction de domaine dans Active Directory.

3 Effectuez les tâches de configuration suivantes, qui sont requises pour utiliser Workspace ONE Access comme fournisseur d'identité pour Horizon Cloud.

- Configurer les attributs utilisateur de Workspace ONE Access pour l'intégration à Horizon Cloud .
- Configurer la fonctionnalité People Search de Workspace ONE Access pour l'intégration à Horizon Cloud.

Création de comptes de liaison de domaine et de jonction de domaine dans Active Directory

Après avoir configuré votre fournisseur d'identité, créez deux comptes de liaison de domaine et deux comptes de jonction de domaine sur votre annuaire Active Directory sur site. Par la suite, utilisez Horizon Universal Console pour communiquer les détails de ces comptes à Horizon Cloud.

Horizon Cloud nécessite que vous spécifiiez deux instances des comptes AD suivants à utiliser comme comptes de service.

- Compte de liaison de domaine utilisé pour effectuer des recherches dans votre domaine AD.
- Compte de jonction de domaine utilisé pour joindre des comptes d'ordinateur au domaine, supprimer des comptes d'ordinateur du domaine et effectuer des opérations Sysprep.

Important Respectez les directives suivantes pour les comptes Active Directory que vous spécifiez pour ces comptes de service.

- Si les comptes de liaison de domaine principal et auxiliaire expirent ou deviennent inaccessibles, Single Sign-On ne fonctionne pas et vous ne pouvez pas rejoindre les nouveaux postes de travail. Si vous ne définissez pas l'option **N'expire jamais** dans les comptes de liaison de domaine principal et auxiliaire, assurez-vous que leurs délais d'expiration sont différents. Vous devez effectuer le suivi à mesure que le délai d'expiration approche et mettre à jour les informations du compte de liaison de domaine Horizon Cloud avant l'expiration du délai.
- Si les comptes de jonction de domaine principal et auxiliaire expirent ou deviennent inaccessibles, Single Sign-On ne fonctionne pas et vous ne pouvez pas rejoindre les nouveaux postes de travail. Si vous ne définissez pas l'option **N'expire jamais** dans les comptes de jonction de domaine principal et auxiliaire, assurez-vous que leurs délais d'expiration sont différents. Vous devez effectuer le suivi à mesure que le délai d'expiration approche et mettre à jour les informations du compte de jonction de domaine Horizon Cloud avant l'expiration du délai.

Compte de liaison de domaine - Autorisations Active Directory requises

Le compte de liaison de domaine doit disposer des autorisations d'accès en lecture qui peuvent rechercher les comptes AD de toutes les unités d'organisation (OU) AD que vous prévoyez d'utiliser dans les opérations DaaS (Desktop-as-a-Service) qu'Horizon Cloud fournit, telles que l'attribution de VM de poste de travail à vos utilisateurs finaux. Le compte de liaison de domaine doit pouvoir énumérer les objets depuis Active Directory. Le compte de liaison de domaine exige les autorisations suivantes sur l'ensemble des unités d'organisation et des objets que vous prévoyez d'utiliser avec Horizon Cloud :

- Contenu de la liste
- Toutes les propriétés - accès en lecture
- Autorisations d'accès en lecture
- tokenGroupsGlobalAndUniversal - accès en lecture (sous-entendu par l'autorisation Toutes les propriétés - accès en lecture)

Important En règle générale, les comptes de liaison de domaine doivent se voir accorder les autorisations prêtes à l'emploi qui sont liées à l'accès en lecture par défaut et qui sont généralement accordées aux Utilisateurs authentifiés dans un déploiement Microsoft Active Directory. Dans un déploiement de Microsoft Active Directory prêt à l'emploi, ces paramètres par défaut accordés aux Utilisateurs authentifiés donnent en général à un compte d'utilisateur de domaine standard la possibilité d'effectuer l'énumération requise dont Horizon Cloud a besoin pour le compte de liaison de domaine. Cependant, si les administrateurs AD de votre organisation ont choisi de verrouiller les autorisations liées à l'accès en lecture pour les utilisateurs standard, vous devez demander aux administrateurs AD de conserver les valeurs standard par défaut des utilisateurs authentifiés pour les comptes de liaison de domaine que vous utiliserez pour Horizon Cloud.

Compte de jonction de domaine - Autorisations Active Directory requises

Le compte de jonction de domaine est configuré au niveau du locataire. Le système utilise le compte de jonction de domaine qui est configuré dans l'enregistrement Active Directory pour toutes ses opérations liées à la jonction de domaine avec tous les espaces de la flotte de votre locataire.

Le système effectue des vérifications d'autorisations explicites dans le compte de jonction de domaine à l'intérieur de l'unité d'organisation que vous spécifiez dans le workflow d'enregistrement d'Active Directory (dans la zone de texte **Unité d'organisation par défaut** de ce workflow) et dans les unités d'organisation que vous spécifiez dans les batteries de serveurs et dans les attributions de poste de travail VDI que vous créez, si les zones de texte **Unité d'organisation de l'ordinateur** de ces batteries de serveurs et attributions de poste de travail VDI sont différentes de l'unité d'organisation par défaut dans l'enregistrement d'Active Directory.

Pour couvrir ces cas où vous ne pouvez jamais utiliser une sous-unité d'organisation, il est recommandé de définir ces autorisations requises pour les appliquer à tous les objets descendants de l'unité d'organisation de l'ordinateur.

Important

- Certaines des autorisations AD de la liste sont généralement attribuées par défaut par Active Directory à des comptes. En revanche, si vous avez limité l'autorisation de sécurité dans Active Directory, vous devez vérifier que le compte de jonction de domaine dispose de ces autorisations de lecture pour l'ensemble des unités d'organisation et des objets que vous prévoyez d'utiliser avec Horizon Cloud.
- Dans Microsoft Active Directory, lorsque vous créez une unité d'organisation, le système peut définir automatiquement l'attribut `Prevent Accidental Deletion` qui applique un `Deny` à l'autorisation Supprimer tous les objets enfants de l'unité d'organisation récemment créée et de tous les objets descendants. Par conséquent, si vous avez explicitement attribué l'autorisation Supprimer des objets de l'ordinateur au compte de jonction de domaine, dans le cas d'une unité d'organisation récemment créée, Active Directory peut avoir appliqué un remplacement à cette autorisation de suppression d'objets de l'ordinateur explicitement attribuée. Étant donné que l'effacement de l'indicateur **Empêcher la suppression accidentelle** peut ne pas effacer automatiquement la valeur `Deny` qu'Active Directory a appliquée à l'autorisation de suppression de tous les objets enfants, dans le cas d'une unité d'organisation récemment ajoutée, vous devrez peut-être vérifier et effacer manuellement l'autorisation `Deny` définie pour supprimer tous les objets enfants dans l'unité d'organisation et toutes les unités d'organisation enfants avant d'utiliser le compte de jonction de domaine dans Horizon Universal Console.

Réutilisation des comptes d'utilisateur

Les comptes d'utilisateur de jonction de domaine doivent être autorisés à réutiliser les comptes d'ordinateur existants en procédant comme suit :

- Créez un groupe de sécurité universel.
- Ajoutez tous les comptes d'utilisateur de jonction de domaine au nouveau groupe de sécurité.
- Pour tous les objets de stratégie de groupe (GPO) pertinents, activez **Contrôleur de domaine : autoriser la réutilisation du compte d'ordinateur lors de la jonction de domaine**.
- Cliquez sur **Modifier la sécurité...**
- Dans la boîte de dialogue **Paramètres de sécurité pour les propriétaires de comptes d'ordinateur approuvés**, cliquez sur **Ajouter...**
- Sélectionnez le nouveau groupe de sécurité, puis cliquez sur **OK**.

Effectuez ces étapes pour chaque domaine.

Configurer les attributs utilisateur de Workspace ONE Access pour l'intégration à Horizon Cloud

Si vous utilisez Workspace ONE Access comme fournisseur d'identité pour Horizon Cloud, utilisez la console Workspace ONE Access pour configurer les attributs utilisateur obligatoires.

L'objectif de cette procédure est d'ajouter d'autres attributs de Workspace ONE Access obligatoires pour configurer Workspace ONE Access comme fournisseur d'identité pour Horizon Cloud et de mapper ces attributs requis à vos attributs Active Directory.

Les attributs d'Workspace ONE Access userPrincipalName, objectGuid, sid et netBios sont obligatoires et doivent être mappés aux attributs Active Directory appropriés, comme décrit dans les étapes suivantes.

Conditions préalables

Avant de pouvoir configurer les attributs utilisateur dans la console Workspace ONE Access, vous devez installer Workspace ONE Access Connector et configurer l'intégration d'annuaire à Active Directory.

Procédure

1. Connectez-vous à la console Workspace ONE Access.
2. Cliquez sur **Paramètres > Attributs utilisateur**
3. Ajoutez les attributs personnalisés suivants, comme illustré dans la liste suivante, puis cliquez sur **Enregistrer**.

   Note Assurez-vous d'entrer les attributs sensibles à la casse exactement tels qu'ils apparaissent dans cette liste.

   - objectGuid
   - sid
   - netBios

   Même si userPrincipalName est également obligatoire pour cette intégration, comme il est déjà affiché dans la liste des attributs par défaut, vous n'avez pas à l'ajouter.

4 Cliquez sur **Intégrations > Annuaires** pour mapper les attributs Workspace ONE Access à vos attributs Active Directory.

   a À l'aide de la partie **Gérer** de la zone **Gestion des identités et des accès** de la console Workspace ONE Access, accédez à l'écran dans lequel les annuaires sont configurés et cliquez sur le nom de l'annuaire qui contient les utilisateurs et les groupes qui disposent de droits Horizon Cloud.

   b Dans l'écran de cet annuaire, cliquez sur l'onglet **Paramètres de synchronisation**, puis accédez à sa page **Attributs mappés**.

   c Mappez les attributs utilisateur Workspace ONE Access aux attributs Active Directory comme indiqué.

Attribut Workspace ONE Access	Attribut Active Directory
userPrincipalName	userPrincipalName
objectGuid	objectGUID
sid	objectSid
netBios	msDS-PrincipalName

5 Cliquez sur **Enregistrer**.

6 Vérifiez que vous avez sélectionné tous les utilisateurs et groupes qui se synchronisent avec votre environnement Horizon Cloud.

   Dans la console Workspace ONE Access, vous pouvez afficher et modifier les listes d'utilisateurs et de groupes en accédant à l'écran **Paramètres de synchronisation** du répertoire dans l'onglet **Utilisateurs** et l'onglet **Groupes**.

7 Dans la console Workspace ONE Access, revenez à la page de ce répertoire et cliquez sur **Synchroniser** pour synchroniser les utilisateurs et les groupes avec Workspace ONE Access, utilisant maintenant tous les attributs utilisateur corrects.

Configurer la fonctionnalité People Search de Workspace ONE Access pour l'intégration à Horizon Cloud

Si vous utilisez Workspace ONE Access comme fournisseur d'identité pour Horizon Cloud, vérifiez que la fonctionnalité People Search de la console Workspace ONE Access est activée, ce qui active également la recherche d'utilisateurs dans Horizon Cloud.

Lorsque Workspace ONE Access est le fournisseur d'identité pour Horizon Cloud, la fonctionnalité People Search de Workspace ONE Access doit être activée pour permettre à la recherche d'utilisateurs de fonctionner dans Horizon Universal Console.

Conditions préalables

Avant de pouvoir activer People Search dans la console Workspace ONE Access, vous devez installer Workspace ONE Access Connector et configurer l'intégration d'annuaire à Active Directory.

Procédure

1 Connectez-vous à la console Workspace ONE Access.

2 Cliquez sur **Intégrations > People Search**.

3 Sur la page Sélectionner un annuaire, sélectionnez l'annuaire.

4 Sur la page Sélectionner des attributs utilisateur, sélectionnez l'attribut **businessUnit** et mappez-le lorsque vous y êtes invité.

5 Pour mapper **Nom d'attribut dans Workspace ONE Access** à **Nom d'attribut dans Active Directory**, sélectionnez le nom d'attribut correspondant dans Active Directory.

   Dans **Attribut managerDN**, vous pouvez définir un attribut personnalisé afin qu'il puisse également être mappé.

6 Cliquez sur **Suivant**.

7 Dans la zone de texte **DN d'utilisateurs**, si la valeur par défaut s'applique, acceptez la valeur par défaut. Sinon, entrez le DN de l'utilisateur (tel que **`OU=Organization,DC=example,DC=com`**) et cliquez sur **Enregistrer et synchroniser**.

Utilisation d'App Volumes

Utilisez App Volumes pour fournir et gérer dynamiquement des applications. Ces applications sont celles que vous souhaitez fournir à l'intention de vos utilisateurs finaux.

Avertissement Lorsque vous effectuez un workflow App Volumes, assurez-vous que le domaine que vous sélectionnez est accessible à partir de l'instance d'Horizon Edge sélectionnée et qu'il s'agit du même domaine que celui du Gestionnaire de liaisons sélectionné. Si l'instance d'Horizon Edge sélectionnée ne peut pas accéder au domaine sélectionné ou si le Gestionnaire de liaisons sélectionné appartient à un domaine différent, des résultats inattendus se produisent, ce qui entraînera probablement l'échec du processus.

Présentation et conditions préalables à l'utilisation d'applications App Volumes dans Horizon Cloud Service - next-gen

À l'aide de la fonctionnalité d'applications App Volumes, vous pouvez gérer l'intégralité du cycle de vie des applications, notamment la création de modules, la mise à jour et le retrait

d'une application. Vous pouvez également personnaliser les droits d'applications pour fournir des versions spécifiques d'une application aux utilisateurs finaux.

Important

- Lorsqu'une fonctionnalité attendue ne s'affiche pas dans la console, contactez votre représentant du compte pour vérifier si votre configuration de licence et de compte de locataire vous autorise à l'utiliser.
- Pour les opérations telles que l'importation ou la suppression de modules d'application, le provisionnement de partages de fichiers et la réplication de modules d'application à partir des partages de fichiers intermédiaires vers ceux de livraison, le déploiement du dispositif Horizon Edge doit être connecté. Pour plus d'informations sur les partages de fichiers, reportez-vous à la section *Conditions préalables liées au dispositif Horizon Edge* sur cette page.

Pour la prise en charge des systèmes d'exploitation invités, reportez-vous à la Matrice d'interopérabilité des produits.

Présentation de la fonctionnalité App Volumes dans Horizon Cloud Service - next-gen

Le tableau suivant présente un aperçu des fonctionnalités de VMware App Volumes dan s Horizon Cloud Service - next-gen.

Zone fonctionnelle	Description
Déploiement	■ Déploiement rationalisé. Provisionnement automatique du composant d'infrastructure App Volumes, tel que le stockage. ■ Infrastructure Edge prenant en charge le module App Volumes pour gérer les partages de fichiers Microsoft Azure. ■ Provisionnement automatique des partages de fichiers Microsoft Azure pendant le déploiementHorizon Edge de l'espace pour stocker et fournir des applications.
Console de gestion	■ La console App Volumes est intégrée à Horizon Universal Console en toute transparence. Gérez les postes de travail et les applications au sein de la même console. ■ Expérience d'installation d'App Volumes Agent transparente intégrée dans les workflows de création d'image Horizon Cloud.
Agent App Volumes 4	Agent optimisé pour des performances unifiées utilisé pour les déploiements sur site et Microsoft Azure.
Création de module	■ Prend en charge les modules basés sur VHD fournis à l'aide des partages de fichiers de Microsoft Azure. ■ La création du module d'application s'effectue en mode natif dans Horizon Cloud. Aucun outil de ligne de commande n'est nécessaire. ■ Les clients peuvent importer des applications MSIX pour attacher des VHD et livrer ce nouveau format de module en utilisant App Volumes.
Gestion du cycle de vie des applications	Prend en charge la capacité Gestion d'applications simplifiée (SAM) déjà intégrée dans App Volumes 4 sur site. Les administrateurs peuvent désormais gérer l'intégralité du cycle de vie de l'application, y compris la création de module, la mise à jour et le retrait.

Zone fonctionnelle	Description
Attribution d'application	■ Les administrateurs peuvent personnaliser leurs droits d'applications (attributions) pour fournir des versions spécifiques d'une application aux utilisateurs finaux. ■ Prend en charge la distribution d'applications pour plusieurs dispositifs Edge.
Prise en charge du cloud hybride	Les clients sur site App Volumes peuvent désormais importer leurs modules d'applications à partir de leurs déploiements sur site dans Horizon Cloud sur Microsoft Azure. Réutilisez les modules sur site. Il n'est pas nécessaire de recréer les modules pour Microsoft Azure.

Présentation du processus d'applications App Volumes

La mise à disposition des applications App Volumes aux utilisateurs est un processus en deux étapes :

- Ajoutez une application App Volumes dans Horizon Universal Console. Il existe deux façons d'effectuer cette opération :
  - Ajoutez une application App Volumes en créant et en important un nouveau module d'application.

    Si aucun module d'application n'a encore été créé, vous pouvez le faire à l'aide de l'option **Ajouter un module**, qui utilise App Volumes pour créer le module d'application et l'importer automatiquement. Reportez-vous à la section Ajouter une application App Volumes à l'aide d'Horizon Cloud Service - next-gen.

    Vous pouvez également créer un module d'application lors de la création d'une application à l'aide de la fonctionnalité **Ajouter une application**.
  - Ajoutez une application App Volumes en important un module d'application existant.

    Si vous disposez d'un module d'application précédemment créé avec App Volumes, vous pouvez l'importer à l'aide de l'option **Importer l'application**. Cela signifie que vous pouvez réutiliser le module d'application à partir de déploiements sur site sans devoir recréer les modules des applications. Reportez-vous à la section Ajouter une application App Volumes en important un module d'application existant à l'aide d'Horizon Cloud Service - next-gen.
- Créez un droit App Volumes pour autoriser l'accès des utilisateurs à l'application App Volumes. Reportez-vous à la section Créer un droit pour une application App Volumes à l'aide d'Horizon Cloud Service - next-gen.

Exigences et conditions préalables à l'utilisation d'App Volumes avec vos déploiements d'Horizon Cloud on Microsoft Azure

Important Pour éviter de rendre vos applications App Volumes inaccessibles et invalider ainsi la prise en charge des fonctionnalités d'App Volumes dans votre déploiement d'Horizon Cloud on Microsoft Azure, la clé du compte de stockage lié à App Volumes ne doit pas être affectée d'une manière qui entraîne son expiration, sa modification ou sa rotation.

En cas de rotation manuelle ou via une stratégie Azure, le compte de stockage et les partages de fichiers sur lesquels App Volumes repose deviennent inaccessibles. Si cela se produit, App Volumes ne peut pas fournir les applications aux utilisateurs finaux, car la clé de stockage stockée dans le déploiement n'est pas valide.

Bien que le déploiement d'Horizon Cloud on Microsoft Azure réside dans votre abonnement Azure fourni, le compte de stockage lié à App Volumes du déploiement est un composant géré par VMware, identique aux modules Horizon Edge, aux machines Unified Access Gateway et aux autres ressources déployées par le service qui sont provisionnées dans votre abonnement Azure. Chaque déploiement d'Horizon Cloud on Microsoft Azure inclut le déploiement d'un compte de stockage lié à App Volumes.

Lorsque le service déploie Horizon Edge, le service provisionne ce compte de stockage lié à App Volumes dans votre abonnement Azure. L'objectif de ce compte de stockage est de fournir les partages de fichiers dans lesquels les fichiers d'application App Volumes sont provisionnés.

Les données de ce compte de stockage sont automatiquement chiffrées par le stockage Azure à l'aide de clés gérées par Microsoft. Si vous ou votre organisation provoquez l'expiration, la modification ou la rotation de la clé du compte de stockage, la clé de stockage n'est plus valide. Si cela se produit, App Volumes ne peut pas accéder aux partages de fichiers et ne peut pas fournir les applications aux utilisateurs finaux.

Avant d'ajouter des applications App Volumes à votre inventaire, vérifiez que votre environnement répond aux conditions préalables suivantes.

Conditions préalables liées à Horizon Edge

- Le déploiement doit disposer d'une configuration de passerelle (instances d'Unified Access Gateway). Vous avez alors terminé les étapes de mappage du nom de domaine complet d'Unified Access Gateway, tel que requis pour les déploiements d'Horizon Cloud on Microsoft Azure configurés avec des instances d'Unified Access Gateway.
- Assurez-vous que votre abonnement Azure n'est pas attribué avec une stratégie pour laquelle la définition `[Preview] Storage Account public access should be disallowed` est activée.

  Si la stratégie avec cette définition est activée, le service App Volumes ne parvient pas à provisionner des partages de fichiers pour le compte de stockage lors du déploiement.
- Ces partages de fichiers sont générés par le service et sont requis pour App Volumes.

Pour afficher les partages de fichiers, dans Horizon Universal Console, accédez à la page **Capacité**, cliquez sur Horizon Edge et faites défiler l'écran jusqu'à la section **Stockage de l'application App Volumes**.

Partage de fichiers intermédiaires

Le partage de fichiers intermédiaires est un partage de fichiers Azure utilisé pour transférer de nouveaux modules d'application à des fins de détection et d'importation dans l'inventaire d'applications. Vous pouvez copier les modules d'application à partir d'un déploiement d'App Volumes 4.x existant. Le partage de fichiers est également utilisé pour la création de modules d'application.

Un partage de fichiers unique est automatiquement provisionné lorsque Horizon Edge est déployé.

Partage de fichiers de distribution

Le partage de fichiers de distribution est un partage de fichiers Azure utilisé pour fournir des modules d'applications existants auxquels les utilisateurs ou les groupes sont autorisés à accéder. Les VM du pool de postes de travail montent les disques des modules d'application à partir de ce partage de fichiers.

Six partages de fichiers de distribution sont automatiquement provisionnés lorsque le premier pool est créé pour chaque fournisseur. Par exemple : pour une instance d'Horizon Edge avec un fournisseur principal et quatre fournisseurs secondaires, App Volumes provisionne un partage de fichiers intermédiaires et six partages de fichiers de distribution pour chaque fournisseur secondaire. Par conséquent, un total de 24 partages de fichiers est provisionné.

Note

- Si vous prévoyez d'utiliser le fournisseur principal pour créer vos pools, App Volumes provisionne un seul partage de fichiers intermédiaires et six partages de fichiers de distribution.
- Dans un dispositif Horizon Edge, le service Horizon Cloud réplique automatiquement les modules d'application du partage de fichiers intermédiaires vers les partages de fichiers de livraison.

Conditions requises de configuration

- Si vous choisissez de configurer un domaine Active Directory comme identité de machine, assurez-vous d'avoir terminé le workflow d'enregistrement du domaine Active Directory tel qu'il est décrit à la section Gestion des identités et des accès dans un environnement Horizon Cloud Service - next-gen.

  Vous pouvez également choisir Azure Active Directory comme identité de machine.

- En plus de répondre aux Conditions requises pour les ports et les protocoles pour votre déploiement d'Horizon Cloud dans Microsoft Azure pour Horizon Cloud, vous devez

également ouvrir le port 445 pour le trafic de protocole TCP. Le port 445 est le port SMB standard pour accéder à un partage de fichiers SMB sur Microsoft Windows. Les modules d'application sont stockés dans les partages de fichiers de Microsoft Azure présents dans un groupe de ressources identifié par l'instance de fournisseur principal d'Horizon Edge.

Conditions requises de l'image

Pour ajouter une application App Volumes en créant un module d'application à l'aide du workflow Ajouter un module ou Ajouter une application dans la console, l'image publiée de votre inventaire dans la console doit répondre aux critères suivants.

- Dispose d'un type de client de système d'exploitation Microsoft Windows 10 ou Windows 11. Ce type de client est parfois appelé type VDI de système d'exploitation. Le workflow de capture dans le cloud est disponible pour une utilisation uniquement avec les types VDI de systèmes d'exploitation. Le workflow de capture dans le cloud n'est pas disponible pour les types multisession ou RDS de systèmes d'exploitation.
- App Volumes Agent est installé.
- Pour utiliser le mode de distribution de modules à la demande, assurez-vous d'avoir installé Horizon Agent Installer build `23.1.0.21387799` et builds ultérieures.

Pour rechercher la version de l'agent d'une image pour un pool spécifique, procédez comme suit :

1. Accédez à **Ressources > Pools**.
2. Cliquez sur un nom de pool.
3. Sur la page Détails du pool, accédez à la section **Paramètres généraux**.
4. Dans le volet **Image**, notez la valeur `Name`.

   `Name` est le nom de l'image utilisé pour ce pool particulier.
5. Pour afficher une liste d'images, accédez à **Ressources > Images**.
6. Pour afficher le tableau **Versions** qui répertorie les versions et l'état de l'image, cliquez sur le lien du nom de l'image.
7. Cliquez sur le lien de la version de l'image souhaitée.
8. Sur la page Détails de la version de l'image, accédez au tableau **Copies d'images**.
9. Affichez la valeur `Agent Version`.

   `Agent Version` indique la build d'Horizon Agent Installer installée sur la version de l'image.

Conditions requises pour la création d'un module

- Si vous avez configuré des règles de pare-feu pour l'accès au compte de stockage provisionné par App Volumes, veillez à mettre sur liste autorisée tous les sous-réseaux associés au fournisseur pour le déploiement d'Horizon Edge utilisé pour créer le module d'applications.

- Vous devez désactiver les services de mise à jour automatique de chaque application pour laquelle vous prévoyez de créer un module, car un comportement de mise à jour automatique est problématique.
  - Si l'application dispose d'un service de mise à jour automatique, désactivez le service, par exemple avec Windows Services Manager, pendant le processus de provisionnement de l'application.
  - Si vous ne désactivez pas le service de mise à jour automatique pendant le processus de provisionnement des applications ou si vous ne pouvez pas le faire, après avoir rencontré un problème, par exemple les utilisateurs qui reçoivent une version incomplète d'une application non attribuée, modifiez l'image de base en configurant le registre. Cette configuration garantit que le service d'intérêt n'est pas démarré lorsque le module d'application est déployé sur la machine virtuelle de l'utilisateur. En particulier, configurez le registre en ajoutant le nom du service applicatif à la configuration du registre svservice **DisableAppServicesList**.

Meilleures pratiques d'utilisation d'une image Microsoft Windows 10 ou 11 Enterprise multisession avec des applications App Volumes dans des déploiements d'Horizon Edge de Microsoft Azure

Les pratiques suivantes tendent à offrir une meilleure expérience aux utilisateurs et aux administrateurs. Reportez-vous également à la section Configuration d'une image Microsoft Windows 10 ou 11 Enterprise multisession avec des applications App Volumes pour Horizon Cloud Service - next-gen.

- Installez des imprimantes matérielles avec des pilotes d'écran dans l'image de base.
- Comme indiqué dans les FAQ de la documentation Microsoft, Microsoft Windows 10 ou 11 Enterprise multisession est un type d'hôte de session Bureau à distance (RDSH) de VM permettant plusieurs sessions interactives simultanées, qui étaient auparavant uniquement fournies par les systèmes d'exploitation Microsoft Windows Server. Étant donné que Microsoft Windows 10 ou 11 Enterprise multisession est un type RDSH de système d'exploitation, les workflows applicables à RDSH d'Horizon Cloud s'appliquent à celui-ci plutôt qu'aux workflows liés à VDI. Par conséquent, pour fournir des postes de travail de session aux utilisateurs finaux en fonction de ces systèmes multisession, créez un groupe de pools à plusieurs sessions, comme décrit dans la section Créer un groupe de pools à plusieurs sessions.
- Informez les utilisateurs que lorsqu'ils installent des applications ou créent des fichiers qu'ils n'ont pas l'intention de partager entre toutes les sessions utilisateur sur la même VM, ils peuvent placer le fichier dans leur propre emplacement de profil.

Configuration d'une image Microsoft Windows 10 ou 11 Enterprise multisession avec des applications App Volumes pour Horizon Cloud Service - next-gen

Si vous utilisez une image Microsoft Windows 10 ou 11 Enterprise multisession avec App Volumes dans Horizon Cloud de Microsoft Azure, vous devez prendre des mesures spécifiques pendant le processus de configuration. Commencez par créer le système d'exploitation Microsoft Windows

Enterprise multisession sous-jacent et terminez par la distribution d'applications aux utilisateurs en créant une attribution App Volumes. La séquence générale suivante illustre ce processus.

Pour obtenir des informations générales sur les procédures qui suivent, reportez-vous à la rubrique Présentation et conditions préalables à l'utilisation d'applications App Volumes dans Horizon Cloud Service - next-gen.

Lorsque vous effectuez les procédures de la liste suivante, respectez toutes les instructions spécifiques à la configuration d'une image Microsoft Windows 10 ou 11 Enterprise multisession pour une utilisation avec les fonctionnalités d'App Volumes dans les déploiements d'Horizon Edge de Microsoft Azure.

Important

- Sur une machine multisession, le détachement du module d'application se produit après la déconnexion du dernier utilisateur auquel ce module a été attribué. L'arrêt de la VM correspondante n'est pas nécessaire au détachement des volumes.
- Le workflow de capture dans le cloud du système n'est pas disponible pour les types multisession ou RDS de systèmes d'exploitation. Ce workflow de capture dans le cloud est effectué à l'aide d'Horizon Universal Console.

  Par conséquent, pour ajouter des applications App Volumes dans l'inventaire de votre organisation à l'aide du workflow de capture dans le cloud, vous devez utiliser une image basée sur le type de client du système d'exploitation Microsoft Windows 10 ou 11 Enterprise multisession, parfois appelé type VDI du système d'exploitation, et l'utiliser pour le workflow de capture dans le cloud. Ensuite, lorsque ces applications se trouvent dans l'inventaire, vous pouvez les utiliser avec des postes de travail basés sur une session provisionnés par les pools à plusieurs sessions à l'aide d'images Microsoft Windows 10 ou 11 Enterprise multisession. Attribuez le poste de travail basé sur une session à un utilisateur final pour le poste de travail sous-jacent, puis attribuez également ces applications App Volumes capturées au même utilisateur final pour leur utilisation dans ce poste de travail basé sur une session.

Pour la prise en charge des systèmes d'exploitation invités, reportez-vous à la Matrice d'interopérabilité des produits.

1. Ajouter des applications App Volumes à l'inventaire Horizon Cloud.

Avant de pouvoir attribuer une application App Volumes à des utilisateurs finaux auxquels vous avez attribué des postes de travail basés sur une session, l'inventaire de votre locataire doit contenir l'application App Volumes. Vous pouvez utiliser le workflow Ajouter une application ou Ajouter un module, voire Importer l'application de la console pour ajouter des applications App Volumes à l'inventaire de votre organisation.

Toutefois, le workflow Créer n'est pas disponible pour un type multisession de système d'exploitation. Pour utiliser le workflow Créer afin d'ajouter une application à l'inventaire, vous devez disposer d'un type de client, parfois appelé VDI de système d'exploitation Microsoft Windows 10 ou 11 à utiliser avec ce workflow et capturer les applications à partir de ce type VDI de système d'exploitation.

- Utilisez le workflow Ajouter une application ou Ajouter un module de la console pour ajouter les applications à partie d'un type VDI de système d'exploitation Microsoft Windows 10 ou 11 dans l'inventaire. Pour obtenir la procédure, reportez-vous à la section Ajouter une application App Volumes à l'aide d'Horizon Cloud Service - next-gen.
- Utilisez le workflow Importer de la console pour ajouter des applications App Volumes à votre inventaire que vous avez capturées manuellement en dehors de votre locataire Horizon Cloud et chargées manuellement dans le partage de fichiers intermédiaires de votre dispositif Horizon Edge à l'aide du portail Microsoft Azure. Utilisation principale de ce workflow : lorsque vous disposez déjà de modules App Volumes à partir d'une installation d'App Volumes sur site et que vous souhaitez réutiliser ces modules dans votre inventaire Horizon Cloud. Reportez-vous à la section Ajouter une application App Volumes en important un module d'application existant à l'aide d'Horizon Cloud Service - next-gen.

2. Attribuer les applications App Volumes aux nouveaux utilisateurs

Créez un droit App Volumes pour les nouveaux utilisateurs, comprenant une ou plusieurs des applications App Volumes que vous venez de créer. Reportez-vous à la section Créer un droit pour une application App Volumes à l'aide d'Horizon Cloud Service - next-gen.

Important Si un service nécessitant des privilèges d'administration est capturé dans un module d'application Microsoft Windows 10 ou 11 Enterprise multisession, tous les utilisateurs auxquels ce module d'application a été attribué doivent également disposer de privilèges d'administration.

3. Créer le poste de travail sous-jacent pour le système d'exploitation Microsoft Windows 10 ou 11 Enterprise multisession et l'attribuer aux utilisateurs

Cette première partie du processus inclut les procédures qui suivent.

1 Créez une image de poste de travail du système d'exploitation Microsoft Windows 10 ou 11 Enterprise multisession.

Note Lorsque vous créez la VM de base pour l'image, installez App Volumes Agent.

Pour plus d'informations sur l'ajout d'une image à partir de Microsoft Azure Marketplace, reportez-vous à la section Ajouter une image à partir de Microsoft Azure Marketplace.

Créez un groupe de pools à plusieurs sessions en utilisant la nouvelle image du poste de travail du système d'exploitation Microsoft Windows 10 ou 11 Enterprise multisession. Reportez-vous à la section Créer un groupe de pools à plusieurs sessions.

2 Autorisez l'accès des utilisateurs finaux au groupe de pools à plusieurs sessions.

Reportez-vous à la section Lancer un poste de travail à l'aide d'Horizon HTML Access, le client Web.

Ajouter une application App Volumes à l'aide d'Horizon Cloud Service - next-gen

Le workflow Ajouter une application dans la Horizon Universal Console permet d'ajouter une application à l'inventaire de votre organisation. Vous pouvez ajouter un module immédiatement lors de la création d'une application ou utiliser le workflow Ajouter un module et ajouter ultérieurement un module à l'application existante.

Note Pour ajouter un module à une application existante, il n'est pas nécessaire de recréer l'application.

- Lorsque vous utilisez le workflow Ajouter une application pour la première fois, le même utilisateur ne doit pas essayer d'utiliser cette option une deuxième fois pour la même image tant qu'il n'a pas terminé les étapes de capture d'un module d'application dans la VM de poste de travail de capture. S'il essaie de réutiliser l'option pour la même image avant de terminer les étapes de capture d'un module d'application, un message indiquant qu'une demande de création d'un module est déjà lancée s'affiche. Un utilisateur différent dans le même locataire peut cependant initier la création d'un module pour cette image, que le premier utilisateur ait terminé ou non.

  Note Lors de la sélection de différentes images, sur le même dispositif Horizon Edge ou sur un autre dispositif Horizon Edge, le même utilisateur peut exécuter plusieurs captures simultanément. Il ne peut pas exécuter simultanément plusieurs captures pour la même image.

- La première fois que vous cliquez sur l'option Ajouter une application pour lancer le processus de capture, le système peut prendre jusqu'à 10 minutes avant que la VM de poste de travail de capture soit prête et que l'état passe à `Desktop ready for application capture`. Pour la première fois, cette durée de 20 minutes est due au fait que le système crée une attribution de poste de travail et deux machines virtuelles de poste de travail pour prendre en charge le processus de capture. Une fois que vous avez terminé la capture de votre premier module d'application, puis que vous souhaitez lancer un nouveau processus de capture, le délai entre le moment où vous cliquez sur l'option Ajouter une application et le passage de l'état à `Desktop ready for application capture` est plus court, environ 10 minutes. Les délais après la première fois sont plus courts, car le système n'a pas à créer l'attribution de poste de travail de capture comme pour la première fois. Pour la deuxième fois, le système supprime la machine virtuelle de poste de travail de capture précédemment utilisée et en utilise une nouvelle.

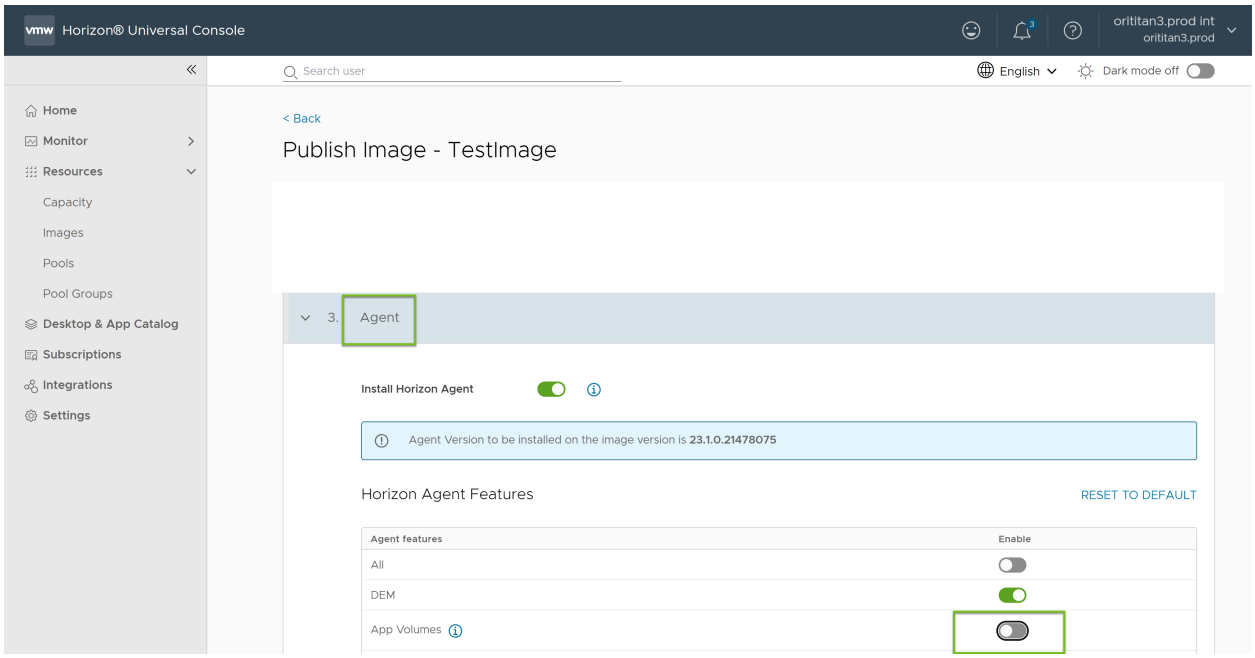
Chaque module dispose d'une option de livraison. Cette option vous permet de définir le mode de distribution de modules sur `Classic` ou `On-demand`. Avec la distribution classique, toutes les applications attribuées sont distribuées à un utilisateur final immédiatement au démarrage de l'ordinateur ou à la connexion de l'utilisateur. Avec la distribution à la demande, un raccourci s'affiche, mais l'application n'est pas distribuée tant que l'utilisateur n'ouvre pas le raccourci. Pour plus d'informations, reportez-vous à la section Présentation des modes de distribution d'un module d'application App Volumes à l'aide d'Horizon Cloud Service - next-gen.

Conditions préalables

Vérifiez que votre environnement répond à toutes les conditions préalables répertoriées dans Présentation et conditions préalables à l'utilisation d'applications App Volumes dans Horizon Cloud Service - next-gen.

Important Le workflow Ajouter n'est disponible que pour les images comportant des types d'utilisateur unique, de client ou VDI de systèmes d'exploitation Microsoft Windows, mais pas pour les types de systèmes d'exploitation multisession. Avant d'effectuer les étapes de la tâche suivante, vous devez disposer d'une image avec App Volumes Agent installé. Lors de l'ajout d'une image à partir de Microsoft Azure Marketplace et de la publication de l'image, assurez-vous que vous avez activé le bouton bascule App Volumes. Par défaut, cette option est désactivée. Ce bouton bascule est répertorié dans la section **Agent** lors de la publication d'une image.

L'option



Pour ajouter une image et la publier, reportez-vous à la section Gestion des images Horizon à l'aide du Plan de contrôle Horizon de nouvelle génération.

Procédure

1. Dans Horizon Universal Console, accédez à **Catalogue de postes de travail et d'applications > App Volumes**.
2. Cliquez sur **Ajouter > Application**.
3. Sur la page **Ajouter une application**, ajoutez **Nom d'application** et **Description**.
4. Ajoutez les **Détails du propriétaire** en sélectionnant le propriétaire dans les domaines disponibles d'Active Directory
5. Sélectionnez la bascule pour **Ajouter un module**.

   Notez que vous pouvez ajouter le module immédiatement ou ultérieurement. Pour ajouter le module ultérieurement, vous pouvez utiliser le workflow Ajouter un module.
6. Ajoutez **Nom du module** et **Description**.
7. Sélectionnez le dispositif **Horizon Edge** sur lequel cette application sera packagée.
8. Sélectionnez le **Fournisseur** dans lequel la VM de création de package est créée pour capturer le module.
9. Sélectionnez l'**Identité de machine**.

   Vous pouvez choisir `Azure Active Directory` ou un domaine Active Directory configuré enregistré dans votre environnement. Si vous choisissez le domaine Active Directory configuré, assurez-vous que le domaine est accessible à partir de l'instance d'Horizon Edge sélectionnée.

   Note Pour `Azure Active Directory`, tous les périphériques Windows 11 et Windows 10 sont pris en charge, sauf les éditions Home de Windows Server 2019 et les machines virtuelles plus récentes s'exécutant dans Microsoft Azure (Server Core n'est pas pris en charge).
10. Sélectionnez le **Gestionnaire de liaisons** ou l'utilisateur auquel la VM est allouée pour la capture de l'application.

    Le domaine de l'utilisateur doit être le même que le domaine Active Directory sélectionné.
11. Choisissez entre la livraison **Classique** et **À la demande**.

    Par défaut, la distribution des modules est définie sur `Classic`. Si vous définissez le module sur `On-demand`, celui-ci est attaché uniquement lorsque l'utilisateur final lance l'application.

    Note Pour les modules créés à l'aide des versions `23.1.0.21387799` et antérieures du programme d'installation d'Horizon Agent qui ne prennent pas en charge la distribution à la demande, un administrateur peut toujours passer de `On-demand` à `Classic` et de `Classic` à `On-demand`. Toutefois, l'agent App Volumes ne peut pas virtualiser le module existant conformément au comportement à la demande.
12. Sélectionnez l'**Image** utilisée par la VM pour capturer le module.

    Assurez-vous qu'App Volumes Agent est installé sur l'image.

13 Sélectionnez la **Version d'image** utilisée par la VM pour capturer le module.

14 Sélectionnez le **Modèle de poste de travail** utilisé pour générer la VM à des fins de création de module.

15 Cliquez sur **Enregistrer**.

Résultats

- Dès que le module est ajouté, l'état du module est `Desktop provisioning is in progress`.
- Une fois le provisionnement de poste de travail terminé et une VM attribuée au Gestionnaire de liaisons, l'état du module est `Ready for capture`.

Étape suivante

Lorsque vous créez une application, vous pouvez effectuer l'une des deux tâches suivantes :

- Pour ajouter un autre module à cette application ou créer un module ultérieurement, suivez les étapes mentionnées dans Ajouter un nouveau module d'application à une application App Volumes existante à l'aide d'Horizon Cloud Service - next-gen.
- Si vous avez déjà créé un module et que vous souhaitez capturer le module d'application, suivez les étapes mentionnées dans Capturer un module d'application App Volumes à l'aide d'Horizon Cloud Service - next-gen

Répliquer manuellement des modules d'applications App Volumes entre les déploiements d'Horizon Edge à l'aide d'Horizon Cloud Service - next-gen

Si vous disposez de plusieurs déploiements d'Horizon Edge pour répliquer un module d'application capturé ou importé d'un dispositif Horizon Edge vers un autre, vous devez copier manuellement les modules du partage du dispositif Horizon Edge source vers le partage de fichiers du dispositif Horizon Edge de destination.

Conditions préalables

Dans Horizon Cloud Service - next-gen, identifiez un module d'application capturé ou importé à répliquer.

Procédure

1 Obtenez le nom de fichier du module d'application que vous prévoyez de répliquer.

   a Dans Horizon Universal Console, accédez à **Catalogue de postes de travail et d'applications > App Volumes**.

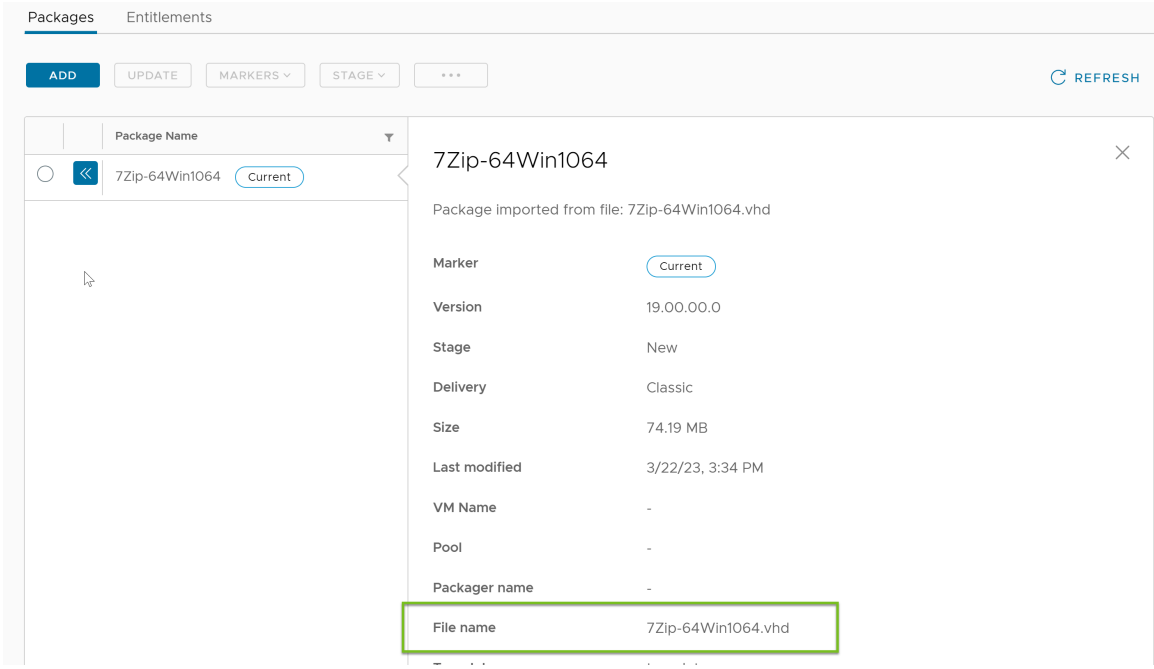
   Une liste d'applications s'affiche.

   b Cliquez sur l'application qui comporte le module à répliquer.

c Cliquez sur l'icône de double flèche gauche du module souhaité.

L'écran Détails du module s'affiche.

d Notez le nom de fichier (*filename*.vhd).



2 Accédez au portail Microsoft Azure.

3 Localisez le partage de fichiers intermédiaires qui contient les fichiers `.vhd` et `.json` du nom de fichier de l'application indiqué dans l'une des étapes précédentes.

4 Copiez les fichiers depuis `appvolumes/packages`.

5 Chargez les fichiers copiés dans le partage de fichiers intermédiaires du dispositif Horizon Edge de destination sur `appvolumes/packages`.

Point de terminaison privé Azure pour un compte de stockage d'applications App Volumes

Vous pouvez utiliser la solution de point de terminaison privé Azure pour accéder en toute sécurité aux comptes de stockage et aux partages de fichiers. La console Horizon Universal Console permet de configurer un point de terminaison privé pour un compte de stockage lors du déploiement d'un nouveau dispositif Horizon Edge ou pour un dispositif Horizon Edge existant.

Lors de la configuration d'un point de terminaison privé et de la sélection d'un sous-réseau (sous-réseau de gestion ou personnalisé de la passerelle Edge), assurez-vous que les conditions préalables suivantes sont configurées dans le portail Azure :

- Vous devez configurer les autorisations obligatoires suivantes au niveau de l'abonnement :

  Note Lorsque vous créez un principal de service, le rôle personnalisé doit disposer des autorisations répertoriées ici.

  ```
  "Microsoft.Resources/deployments/*",
  "Microsoft.Resources/subscriptions/resourceGroups/read",
  "Microsoft.Network/virtualNetworks/read",
  "Microsoft.Network/virtualNetworks/subnets/read",
  "Microsoft.Network/virtualNetworks/subnets/write",
  "Microsoft.Network/virtualNetworks/subnets/join/action",
  "Microsoft.Network/privateEndpoints/read",
  "Microsoft.Network/privateEndpoints/write",
  "Microsoft.Network/privateEndpoints/delete",
  "Microsoft.Network/locations/availablePrivateEndpointTypes/read"
  ```

  Pour plus d'informations sur ces autorisations, reportez-vous à la *documentation de Microsoft*.

- Vous devez établir l'appairage réseau entre les composants suivants :
  - Réseau virtuel personnalisé dans lequel le point de terminaison privé est configuré et réseau virtuel de la gestion de la passerelle Edge
  - Réseau virtuel personnalisé dans lequel le point de terminaison privé est configuré et réseau virtuel de chaque pool de postes de travail (existant ou nouveau).

  L'appairage réseau permet à la gestion de la passerelle Edge et au pool de postes de travail de communiquer en toute sécurité avec le compte de stockage et les partages de fichiers via le point de terminaison privé.

États d'un point de terminaison privé

Les différents états d'un point de terminaison privé sont les suivants :

Connecté

Une fois qu'un point de terminaison privé est configuré pour un déploiement d'Horizon Edge nouveau ou existant, l'état du point de terminaison privé est `Connected`.

Non configuré

Lorsqu'un compte de stockage existant n'est pas configuré avec un point de terminaison privé ou que le point de terminaison privé configuré est supprimé, l'état du point de terminaison privé est `Not Configured`.

Pour ce type de compte de stockage, vous pouvez configurer un point de terminaison privé à l'aide de l'option **Configurer le point de terminaison privé**. Cette option est disponible pour chaque dispositif Horizon Edge dans le tableau **Comptes de stockage Azure** présent dans la section **Stockage de l'application App Volumes**.

Pour configurer un point de terminaison privé lors du déploiement d'un nouveau dispositif Horizon Edge, reportez-vous à la section Déploiement d'un dispositif Microsoft Azure Edge. Pour configurer un point de terminaison privé pour un dispositif Horizon Edge existant, reportez-vous à la section Détails d'Horizon Edge.

Présentation des modes de distribution d'un module d'application App Volumes à l'aide d'Horizon Cloud Service - next-gen

Parfois, un utilisateur peut utiliser peu fréquemment des applications stratégiques pour l'entreprise. Vous pouvez désormais fournir ces applications à l'utilisateur uniquement lorsque cela est nécessaire. Cette fonctionnalité de type libre-service vous aide à définir le mode de distribution de chaque module d'application lors de la création du module et à modifier ce mode lors de la modification du module.

Les deux types de modes de distribution de modules sont : `Classic` et `On-demand`. Par défaut, le mode de distribution de modules est défini sur `Classic`.

Dans le comportement par défaut (classique), toutes les applications attribuées sont distribuées à un utilisateur final au démarrage de l'ordinateur ou lors de la connexion de l'utilisateur, même lorsque l'application n'est pas immédiatement requise par l'utilisateur final. Pour fournir une application uniquement lorsque l'utilisateur a besoin de l'application, vous pouvez utiliser le mode de distribution à la demande.

Lorsqu'un administrateur définit le mode de distribution d'un module sur `On-demand`, seuls les raccourcis de l'application s'affichent dans le menu **Démarrer** ou sur le poste de travail de l'utilisateur final. Lorsqu'un utilisateur final ouvre le raccourci, le volume d'application est distribué à l'utilisateur final, virtualisé et lancé. Pendant la virtualisation, les raccourcis App Volumes à la demande de l'application sont remplacés par les raccourcis de l'application. Si le lancement d'une application prend quelques secondes de plus, un message s'affiche à l'utilisateur final indiquant que la distribution de l'application est en cours.

Critères de livraison d'un module d'application à la demande

Pour qu'un module d'application soit distribué à la demande à l'utilisateur final, quelques critères d'éligibilité s'appliquent :

- Assurez-vous d'avoir installé la build du programme d'installation d'Horizon Agent `23.1.0.21387799` et versions ultérieures.

  Si un utilisateur final se connecte à un ordinateur agent installé avec une version antérieure du programme d'installation d'Horizon Agent et que cet utilisateur final est autorisé à utiliser une application définie sur `on-demand`, le module n'est pas distribué à l'utilisateur final.

- Les programmes d'application installés pendant le processus de création du module doivent comporter des raccourcis.

Caractéristiques d'un module d'application fourni à la demande

Voici quelques-unes des caractéristiques d'un module d'application distribué à la demande :

- Le raccourci de l'application attribuée à un utilisateur n'est visible que par cet utilisateur.
- Pour une application distribuée à la demande, le module n'est attaché qu'après que l'utilisateur final a lancé le raccourci simulé de l'application.
- Association de type de fichier

  Pour les modules existants, les administrateurs doivent mettre à jour le module pour capturer les données d'association de type de fichier dans le module.

  - Pour quelques applications qui affichent des éléments de menu contextuel, par exemple 7-Zip, l'agent App Volumes n'affiche qu'un point d'entrée pour livrer l'application. Le point d'entrée affiché pour l'utilisateur final dans le menu contextuel est le nom configuré dans la fenêtre **VMware App Volumes - Finaliser le module** lors de la création de module. Une fois l'application livrée à l'utilisateur final, le point d'entrée est remplacé par les éléments de menu propres à l'application.
  - OLE et COM, les gestionnaires d'évaluation et les bibliothèques de types qui sont dynamiques par nature ne sont pas disponibles avant que l'utilisateur ne lance le raccourci à la demande de l'application.
  - Les utilisateurs finaux peuvent utiliser les chemins d'accès aux applications pour fournir les applications à la demande.

    Par exemple : un utilisateur final peut utiliser winword.exe pour ouvrir l'application Microsoft Word, où winword.exe est un chemin d'accès à l'application. Pour plus d'informations sur les chemins d'accès aux applications, consultez la documentation Microsoft pertinente.
  - Si un administrateur configure une application en tant qu'application à la demande qui dispose de sous-menus en cascade et d'autres fonctionnalités, telles que des raccourcis, des associations de types de fichiers et des chemins d'accès à l'application, l'utilisateur final peut afficher le sous-menu en cascade uniquement lorsque le module d'application est distribué.
  - Lors de la création du module, App Volumes stocke le texte statique dans la langue du système d'exploitation utilisé dans la machine de création de module. Si le module prend en charge plusieurs langues et que la langue du système d'exploitation utilisée dans l'ordinateur agent de l'utilisateur final est différente de celle utilisée dans la machine de création du module, l'utilisateur final peut voir les noms d'application, les info-bulles, les descriptions des fichiers et d'autres éléments de texte dans la langue du système d'exploitation utilisée dans la machine de création de module.

Pour plus d'informations sur la création d'un module, reportez-vous à la section Ajouter une application App Volumes à l'aide d'Horizon Cloud Service - next-gen.

Ajouter un nouveau module d'application à une application App Volumes existante à l'aide d'Horizon Cloud Service - next-gen

Vous pouvez créer un module d'application et l'ajouter à une application App Volumes existante.

Note Pour ajouter un module à une application existante, il n'est pas nécessaire de recréer l'application. Sélectionnez plutôt l'application existante dans la liste des applications affichées dans l'onglet App Volumes et continuez à créer un module conformément aux étapes mentionnées dans cette tâche.

Lorsque vous utilisez le workflow Ajouter un module pour la première fois, le même utilisateur ne doit pas essayer d'utiliser cette option une deuxième fois pour la même image tant qu'il n'a pas terminé les étapes de capture d'un module d'application dans la VM de poste de travail de capture. S'il essaie de réutiliser l'option pour la même image avant de terminer les étapes de capture d'un module d'application, un message indiquant qu'une demande de création d'un module est déjà lancée s'affiche. Un utilisateur différent dans le même locataire peut cependant initier la création d'un module pour cette image, que le premier utilisateur ait terminé ou non.

Note Les administrateurs peuvent exécuter plusieurs captures simultanément sur la même image ou sur différentes images. L'image peut se trouver sur le même dispositif Horizon Edge ou sur un autre.

La première fois que vous cliquez sur l'option Ajouter un module pour lancer le processus de capture, le système peut prendre jusqu'à 10 minutes avant que la VM de poste de travail de capture soit prête et que l'état passe à Poste de travail prêt pour la capture d'application. Pour la première fois, cette durée de 20 minutes est due au fait que le système crée une attribution de poste de travail et deux machines virtuelles de poste de travail pour prendre en charge le processus de capture. Une fois que vous avez terminé la capture de votre premier module d'application, puis que vous souhaitez lancer un nouveau processus de capture, le délai entre le moment où vous cliquez sur l'option Ajouter un module et le passage de l'état à Poste de travail prêt pour la capture d'application est plus court, environ 10 minutes. Les délais après la première fois sont plus courts, car le système n'a pas à créer l'attribution de poste de travail de capture comme pour la première fois. Pour la deuxième fois, le système supprime la machine virtuelle de poste de travail de capture précédemment utilisée et en utilise une nouvelle.

Chaque module dispose d'une option de livraison. Cette option vous permet de définir le mode de distribution de modules sur `Classic` ou `On-demand`. Avec la livraison classique, toutes les applications attribuées sont livrées à un utilisateur final immédiatement à la connexion de l'utilisateur. Avec la distribution à la demande, un raccourci s'affiche, mais l'application n'est pas distribuée tant que l'utilisateur n'ouvre pas le raccourci. Pour plus d'informations, reportez-vous à la section Présentation des modes de distribution d'un module d'application App Volumes à l'aide d'Horizon Cloud Service - next-gen.

Procédure

1 Dans Horizon Universal Console, accédez à **Catalogue de postes de travail et d'applications > App Volumes**.

2 Cliquez sur **Ajouter > Module**.

3 Sélectionnez une application existante à laquelle ce module doit être ajouté.

4 Entrez le **Nom du module** et la **Description**.

5 Sélectionnez le dispositif **Horizon Edge** sur lequel cette application sera packagée.

6 Sélectionnez le **Fournisseur** dans lequel la VM de création de package est créée pour capturer le module.

7 Sélectionnez l'**Image** utilisée par la VM pour capturer le module.

Assurez-vous qu'App Volumes Agent est installé sur l'image.

8 Sélectionnez la **Version d'image** utilisée par la VM pour capturer le module.

9 Sélectionnez le **Modèle de poste de travail** utilisé pour générer la VM à des fins de création de module.

10 Sélectionnez l'**Identité de machine**.

Vous pouvez choisir `Azure Active Directory` ou un domaine Active Directory configuré enregistré dans votre environnement. Si vous choisissez le domaine Active Directory configuré, assurez-vous que le domaine est accessible à partir de l'instance d'Horizon Edge sélectionnée.

Note Pour `Azure Active Directory`, tous les périphériques Windows 11 et Windows 10 sont pris en charge, sauf les éditions Home de Windows Server 2019 et les machines virtuelles plus récentes s'exécutant dans Azure (le noyau du serveur n'est pas pris en charge).

11 Sélectionnez le **Gestionnaire de liaisons** ou l'utilisateur auquel la VM est allouée pour la capture de l'application.

Le domaine de l'utilisateur doit être le même que le domaine Active Directory sélectionné.

12 Choisissez entre la livraison **Classique** et **À la demande**.

Par défaut, la distribution des modules est définie sur `Classic`. Si vous définissez le module sur `On-demand`, celui-ci est attaché uniquement lorsque l'utilisateur final lance l'application.

Note Pour les modules créés à l'aide des versions `23.1.0.21387799` et antérieures du programme d'installation d'Horizon Agent qui ne prennent pas en charge la distribution à la demande, un administrateur peut toujours passer de `On-demand` à `Classic` et de `Classic` à `On-demand`. Toutefois, l'agent App Volumes ne peut pas virtualiser le module existant conformément au comportement à la demande.

13 Cliquez sur **Enregistrer**.

Résultats

- Dès que le module est ajouté, l'état du module est `Desktop provisioning is in progress`.

- Une fois le provisionnement de poste de travail terminé et une VM attribuée au Gestionnaire de liaisons, l'état du module est `Ready for capture`.

Étape suivante

Pour capturer le module d'application, suivez les étapes mentionnées dans Capturer un module d'application App Volumes à l'aide d'Horizon Cloud Service - next-gen.

Supprimer une application App Volumes à l'aide d'Horizon Cloud Service - next-gen

En fonction de vos besoins, vous pouvez supprimer une application. Lorsque vous supprimez une application, les modules associés sont également supprimés.

Si une application dispose de droits, vous ne pouvez pas la supprimer. Vous devez annuler l'autorisation d'accès à l'application, puis effectuer l'opération de suppression. Pour plus d'informations sur la suppression d'un droit d'une application, reportez-vous à la section Supprimer un droit App Volumes à l'aide d'Horizon Cloud Service - next-gen.

Conditions préalables

Assurez-vous que l'application ne dispose d'aucun droit.

Procédure

1. Dans Horizon Universal Console, accédez à **Catalogue de postes de travail et d'applications > App Volumes**.
2. Sélectionnez l'application souhaitée, puis cliquez sur **SUPPRIMER**.
3. Dans la fenêtre **Supprimer l'application**, cliquez sur **SUPPRIMER**.

Ajouter une application App Volumes en important un module d'application existant à l'aide d'Horizon Cloud Service - next-gen

Les modules d'application App Volumes créés dans un autre déploiement d'Horizon Edge peuvent être utilisés dans le déploiement actuel à l'aide de la fonctionnalité d'importation. Vous pouvez également utiliser cette fonctionnalité pour réimporter les modules dont les attributs d'application sont manquants ou lorsque les modules sont absents de l'inventaire.

Pour plus d'informations sur l'utilisation de l'Explorateur de stockage Microsoft Azure, reportez-vous à la documentation de l'Explorateur de stockage.

Conditions préalables

Assurez-vous que vous connaissez les points suivants :

- Vérifiez que votre environnement répond à toutes les conditions préalables répertoriées dans Présentation et conditions préalables à l'utilisation d'applications App Volumes dans Horizon Cloud Service - next-gen.

- Ajoutez l'adresse IP du client à la liste autorisée d'adresses qui peuvent accéder au partage de fichiers intermédiaires au moyen du pare-feu. Dans le portail Microsoft Azure, accédez à la page qui contient les paramètres de sécurité réseau de votre compte de stockage. Sous la section Pare-feu, activez l'option pour ajouter l'adresse IP du client.

  Vous pouvez confirmer l'emplacement de ce partage de fichiers en accédant au partage de fichiers approprié dans l'Explorateur de stockage Microsoft Azure. Pour identifier le partage de fichiers intermédiaires pour le dispositif Horizon Edge, accédez à **Ressources > Capacité**, cliquez sur le nom du dispositif Horizon Edge, puis accédez à la section **Stockage de l'application App Volumes**.
- Les fichiers JSON et VHD pour le module d'application que vous prévoyez d'importer doivent se trouver dans le partage de fichiers intermédiaires de votre dispositif Horizon Edge sous `appvolumes/packages`.

  Info-bulle Les fichiers JSON et VHD requis pour l'importation du module d'application sont semblables aux suivants : `7Zip.json` et `7Zip.vhd`. Certaines des sources des fichiers JSON et VHD sont la capture autonome et le partage de fichiers d'un autre dispositif Horizon Edge.

Note Vous devrez peut-être mettre à jour les règles de pare-feu pour le compte de stockage dans le portail Microsoft Azure pour accéder aux fichiers dans le partage de fichiers.

Procédure

1. Dans la Horizon Universal Console, accédez à **Catalogue de postes de travail et d'applications**.
2. Sur la page **Catalogue de postes de travail et d'applications**, cliquez sur **App Volumes**.
3. Cliquez sur **Ajouter > Importer l'application**.
4. Sur la page **Importer**, sélectionnez le site et le dispositif Horizon Edge à partir duquel vous souhaitez importer les modules d'application dans la Horizon Universal Console.
5. En fonction de votre cas d'utilisation, utilisez l'option **Importer** correspondante :

Option	Cas d'utilisation
Nouveaux modules	Utilisez cette option lorsque vous souhaitez importer un nouveau module d'application dans l'inventaire App Volumes à partir du partage de fichiers intermédiaire du dispositif Edge sélectionné.
Tous les modules	Réimportez un module d'application à l'aide de cette option s'il manque des attributs d'application, tels que propriétaire, raccourci, etc., ou si le module est déjà importé, mais manquant dans l'inventaire.

6. Cliquez sur **Importer**.

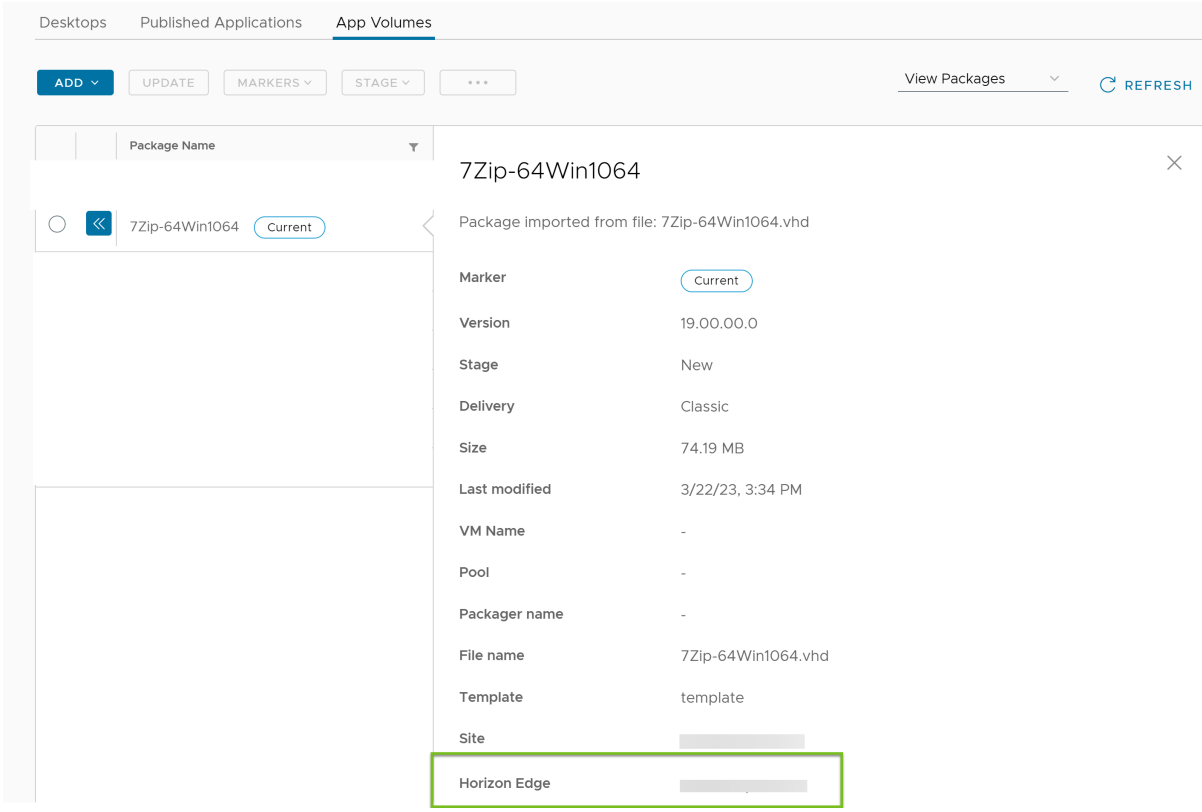
   Une fois l'importation réussie, les modules d'application s'affichent dans l'onglet App Volumes de la Horizon Universal Console. Vous devrez peut-être actualiser la page pour afficher la nouvelle application.

Résultats

- Une fois importées, les données JSON sont mises à jour dans la Horizon Universal Console.

  Important Ne tentez pas de supprimer les fichiers JSON ou VHD directement depuis les partages de fichiers intermédiaires et de livraison. Utilisez toujours la Horizon Universal Console pour supprimer les modules d'application.

- Pour afficher le dispositif Horizon Edge dans lequel le module d'application est importé, accédez au module, développez les détails de celui-ci et recherchez les informations sur Horizon Edge.



  Si vous effectuez à nouveau l'importation pour des déploiements d'Horizon Edge supplémentaires (après la copie ou le transfert des fichiers VHD et JSON vers chaque dispositif Horizon Edge à partir duquel vous devez effectuer l'importation), l'application devient disponible pour plusieurs déploiements d'Horizon Edge. Dans ce cas, les informations sur Horizon Edge dans la fenêtre Détails du module affichent le nombre de déploiements d'Horizon Edge. Pour afficher tous les déploiements, vous pouvez cliquer sur **Afficher** et la page affiche un tableau qui répertorie les détails de déploiements d'Horizon Edge.

Gestion des modules d'applications dans une application App Volumes à l'aide d'Horizon Cloud Service - next-gen

Vous pouvez gérer un module d'application App Volumes dans Horizon Cloud Service - next-gen.

Modifier l'étape du cycle de vie d'un module d'application App Volumes à l'aide d'Horizon Cloud Service - next-gen

Un module d'application App Volumes présente différentes étapes. Ces étapes fournissent des informations sur l'état de livraison du module. En tant qu'administrateur, vous pouvez modifier l'étape d'un module lors de la capture d'un module d'application.

Lorsque la capture de module réussit, l'état du module est `Ready` et l'étape du module est automatiquement définie sur `New`. Vous pouvez désormais modifier les étapes du module.

Note Vous ne pouvez pas modifier le cycle de vie d'un module lorsque l'étape du module est `Unpackaged`.

L'étape d'un module est automatiquement définie sur `Unpackaged` lorsque le module est ajouté à une application, mais pas encore capturé. L'état du module est `Ready for capture`.

Les étapes de cycle de vie d'un module sont les suivantes :

Nouveau

Le module est prêt à être testé.

Testé

Le test du module est terminé et le module est prêt à être publié.

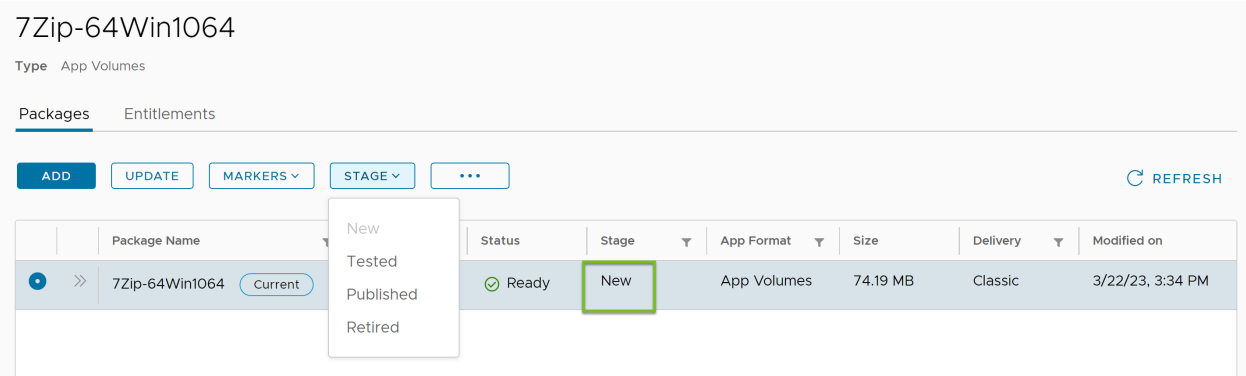
Publié

Le module est publié pour les utilisateurs auxquels il est attribué.

Retiré

Les modules ne sont plus requis ou mis à jour.

Les entités peuvent toujours être attribuées à des applications avec des modules retirés.



Conditions préalables

Assurez-vous que le module est capturé et que l'état du module est `Ready`.

Pour capturer un module d'application, reportez-vous à la section Capturer un module d'application App Volumes à l'aide d'Horizon Cloud Service - next-gen.

Procédure

1. Dans Horizon Universal Console, accédez à **Catalogue de postes de travail et d'applications > App Volumes**.
2. Cliquez sur **Afficher les modules**.
3. Sélectionnez le module souhaité.
4. Cliquez sur **ÉTAPE**, puis sur l'étape de cycle de vie souhaitée.

   L'étape de module mise à jour s'affiche dans la colonne **Étape** sur la page qui contient la liste des modules.

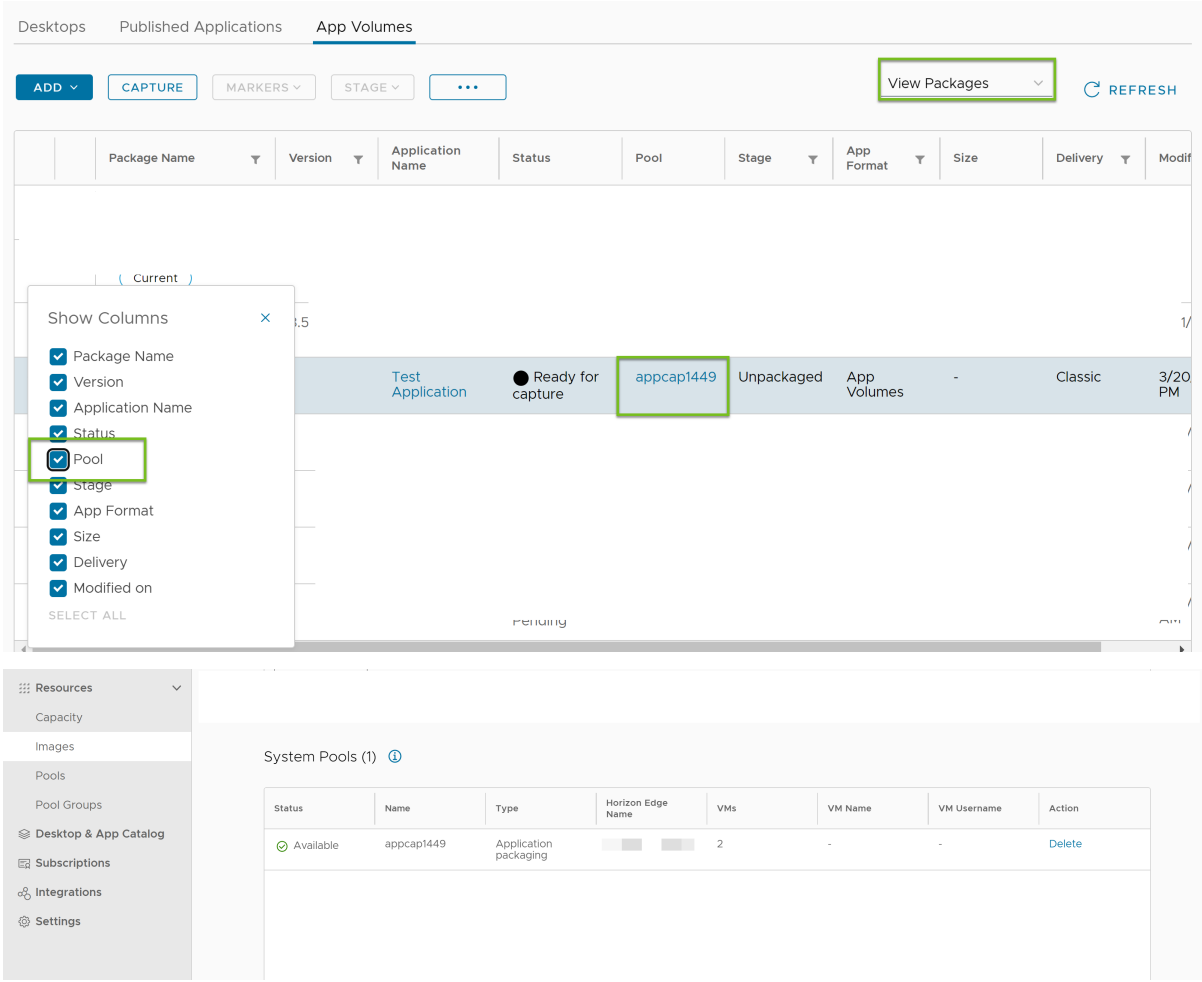
Capturer un module d'application App Volumes à l'aide d'Horizon Cloud Service - next-gen

Chaque module App Volumes stocke un ou plusieurs programmes requis pour l'exécution de l'application. Un seul module peut être fourni à plusieurs utilisateurs et groupes d'utilisateurs. Pour capturer un module d'application, utilisez le workflow suivant.

La première fois que vous lancez le processus de capture, le système prend jusqu'à 10 minutes avant que la machine virtuelle du poste de travail de capture soit prête à l'emploi pour capturer une application. Pendant ces 20 minutes, le système crée un pool système de postes de travail VDI du processus de capture et deux VM de poste de travail à utiliser pour les VM de poste de travail de capture. Le système peut mettre jusqu'à 20 minutes pour créer ce pool système sous-jacent et les VM.

- Le système crée un pool par utilisateur, par image et par dispositif Horizon Edge. Pour cette raison, il peut créer un ou plusieurs pools.
- Il existe deux postes de travail dans chaque pool système afin que vous puissiez démarrer une deuxième capture rapidement après la fin de la première.
- Ces pools sont nommés en fonction du modèle `appcaptureXXX`, où `XXX` est un numéro généré de manière aléatoire.
- Pour mettre à jour l'image utilisée pour le processus de création de module, vous devez supprimer ces pools avant de le faire.

  L'image utilisée sur la VM de poste de travail de capture est présente sur la page **Ressources > Image**. Pour identifier facilement l'image utilisée par la VM de poste de travail de capture pour un module particulier, accédez à la liste des modules (page **Afficher les modules**). Cliquez sur le bouton **Gérer les colonnes** et sélectionnez `Pool`. Dans la colonne Pool, cliquez sur le nom du pool correspondant au module souhaité. La page d'image correspondante s'affiche. Cette page indique l'image utilisée sur la VM de poste de travail de capture pour ce module et les informations sur le pool sont présentes dans la section **Pools système** sur la page d'image.



- Si vous ne prévoyez pas d'effectuer une capture supplémentaire dans un proche avenir, vous pouvez supprimer les pools système afin qu'ils ne figurent pas dans votre environnement sans raison. Cependant, si vous les supprimez, la prochaine fois que vous effectuez une capture, le système mettra jusqu'à 20 minutes pour en créer de nouvelles.

  Note À l'aide des informations de navigation de la page d'image décrites précédemment, accédez à l'image du module souhaité. Accédez à la section **Pools système** et supprimez le pool souhaité.

Note Si une capture échoue, vous pouvez accéder à **Surveiller > Journaux d'activité** pour afficher les événements d'activité système.

Il existe désormais une entrée pour le module d'application dans la liste de la page Applications. Si vous passez votre curseur sur État pour cette entrée de la liste, l'état de la machine virtuelle de capture est indiqué. Lorsque l'état est `Desktop ready for application capture`, vous pouvez poursuivre les étapes de connexion à la machine virtuelle de poste de travail de capture et commencer à installer une application pour votre module d'application.

Note Si vous ne démarrez pas la capture dans l'heure, la VM de poste de travail de capture est automatiquement mise hors tension par le service App Volumes. Cette mise hors tension garantit des économies de coût dans la gestion de l'alimentation pour votre organisation. Toutefois, l'expérience utilisateur ne change pas pour l'administrateur. Lorsque vous êtes prêt pour la capture, vous pouvez continuer à utiliser la VM de poste de travail de capture et passer aux étapes suivantes.

Conditions préalables

Assurez-vous que l'état du module à capturer se trouve dans `Ready for capture`.

Procédure

1. Dans Horizon Universal Console, accédez à **Catalogue de postes de travail et d'applications > App Volumes**.
2. Cliquez sur **Afficher les modules**.
3. Sélectionnez le module que vous prévoyez de capturer.
4. Cliquez sur **CAPTURER**.
5. Pour vous connecter à la VM de création de module, sélectionnez VMware Horizon® Client™ ou le navigateur.
6. Suivez les invites jusqu'à ce que vous lanciez la VM du Gestionnaire de liaisons.

   Cette VM s'ouvre et les informations sur `Création de module App Volumes en cours` s'affichent.

   Dans Horizon Universal Console, l'état du module est `Capture in progress`.
7. Dans la VM du Gestionnaire de liaisons, téléchargez l'application et installez-la.
8. Lorsque vous installez l'application, dans la boîte de dialogue **Création de module App Volumes en cours**, cliquez sur **OK**.
9. Dans la boîte de dialogue **Confirmation d'installation terminée**, cliquez sur **Oui**.
10. (Facultatif) Dans la fenêtre **VMware App Volumes - Finaliser le module**, ajoutez des remarques relatives au Gestionnaire de liaisons.
11. Cliquez sur **Finaliser**.
12. Dans la boîte de dialogue **Redémarrage requis**, cliquez sur **OK**.

    La VM de création de module redémarre.

13 Reconnectez-vous avec les informations d'identification du Gestionnaire de liaisons utilisées précédemment.

14 Dans la boîte de dialogue **La création de module a réussi**, cliquez sur **OK**.

Résultats

Une fois la capture terminée, l'attribution de la VM de création de module est annulée pour le Gestionnaire de liaisons et la VM est supprimée. La taille du modèle de pool est `1`.

L'état du module est désormais `Ready`. L'étape de cycle de vie du module est `New`.

Étape suivante

Vous pouvez effectuer des opérations de gestion de modules, telles que la modification du cycle de vie d'un module, la définition du marqueur `Current` sur le module ou la création de droits pour le module.

Pour plus d'informations sur l'une de ces opérations de gestion des modules, reportez-vous à la section Gestion des modules d'applications dans une application App Volumes à l'aide d'Horizon Cloud Service - next-gen.

Déplacer un module d'application App Volumes à l'aide d'Horizon Cloud Service - next-gen

Vous pouvez transférer des modules d'une application vers une autre. Lorsqu'il existe des conditions requises de modules similaires dans les applications, vous pouvez utiliser la fonctionnalité de transfert.

Conditions préalables

- Assurez-vous que le module à transférer ne dispose d'aucun droit ni d'un marqueur `CURRENT`.

  Vous ne pouvez pas transférer un module disposant d'un droit ou d'un marqueur `CURRENT`. Si un module dispose d'un droit ou d'un marqueur `CURRENT`, supprimez le droit ou le marqueur, puis effectuez de nouveau l'opération de transfert du module.

- Assurez-vous que le module est capturé et que l'état est `Ready`.

  Vous ne pouvez transférer un module qu'après sa capture. Pour plus d'informations sur la capture d'un module d'application, reportez-vous à la section Capturer un module d'application App Volumes à l'aide d'Horizon Cloud Service - next-gen.

Procédure

1 Dans Horizon Universal Console, accédez à **Catalogue de postes de travail et d'applications > App Volumes**.

2 Cliquez sur **Afficher les modules**.

3 Sélectionnez le module pour l'opération de transfert.

4 Cliquez sur l'icône de points de suspension horizontaux et cliquez sur **Déplacer**.

5 Dans la fenêtre **Transférer le module**, sélectionnez l'application de destination dans la zone déroulante **Application**.

6 Cliquez sur **Enregistrer**.

Le module est déplacé vers l'application de destination.

7 Pour vérifier le transfert du module, accédez à l'application de destination et affichez la liste des modules pour cette application.

Modifier un module d'application App Volumes à l'aide d'Horizon Cloud Service - next-gen

Pour modifier les propriétés telles que le nom, la description et le mode de distribution d'un module, vous pouvez modifier celui-ci à l'aide de la fonctionnalité Modifier le module.

Seul un module dans l'état `Ready` contient le champ **Notes**.

Lors de la modification d'un module, le champ **Notes** est utilisé pour afficher les notes ajoutées à la machine virtuelle de création de module. Les informations ajoutées dans ce champ de texte remplacent toutes les informations présentes dans ce champ avant la capture de l'application. La modification de ce champ de texte dans App Volumes Manager met uniquement à jour les métadonnées et ne met pas à jour le fichier de disque virtuel du module d'origine ou le fichier `JSON` du module.

Procédure

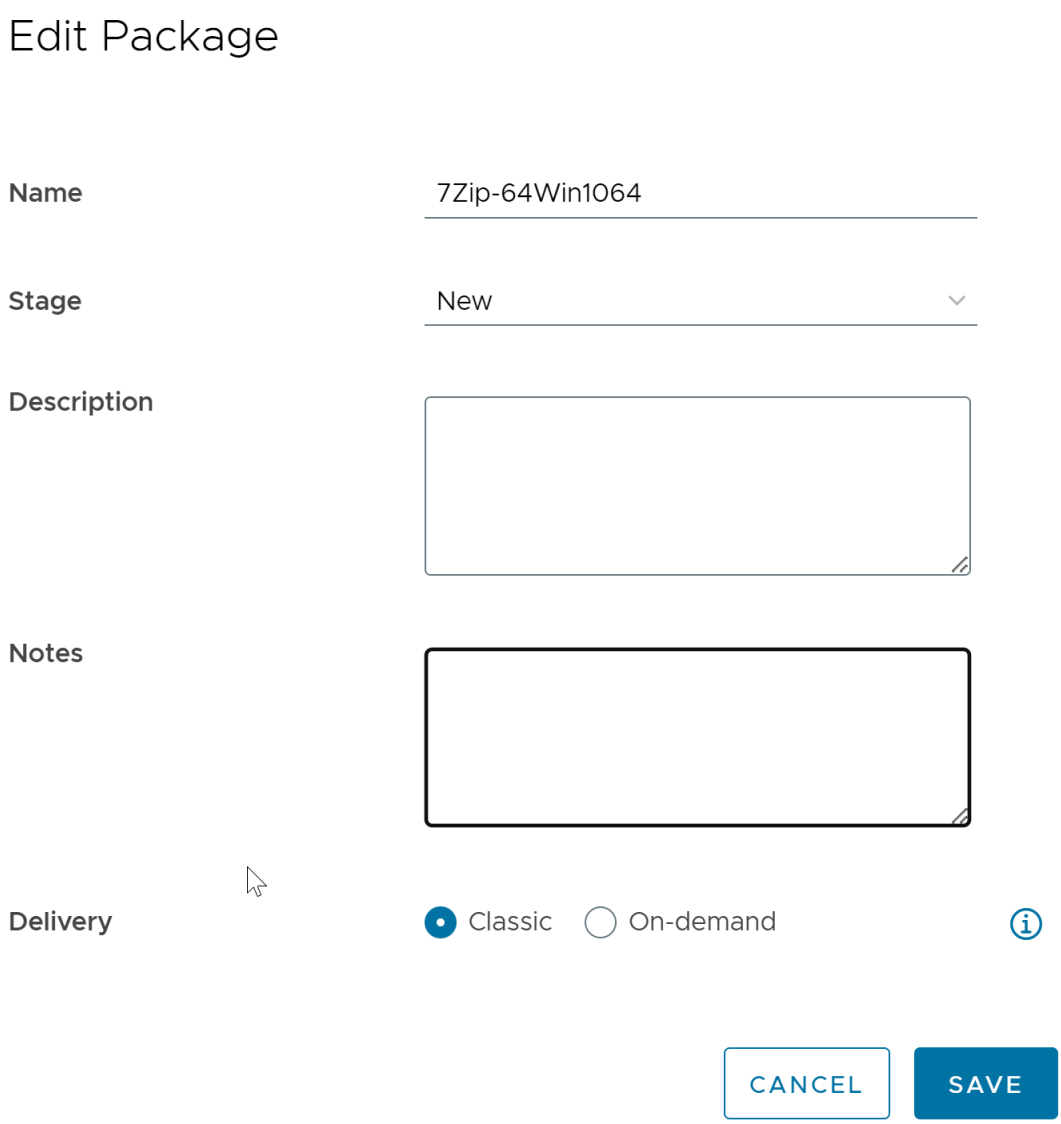
1 Dans Horizon Universal Console, accédez à **Catalogue de postes de travail et d'applications > App Volumes**.

2 Cliquez sur **Afficher les modules**.

3 Sélectionnez le module que vous souhaitez modifier.

4 Cliquez sur le bouton de sélection , puis sur **Modifier**.

5 Dans la fenêtre **Modifier le module**, modifiez les propriétés souhaitées.



6 Cliquez sur **Enregistrer**.

Le module est modifié.

Présentation des scénarios de droits d'accès à l'application App Volumes

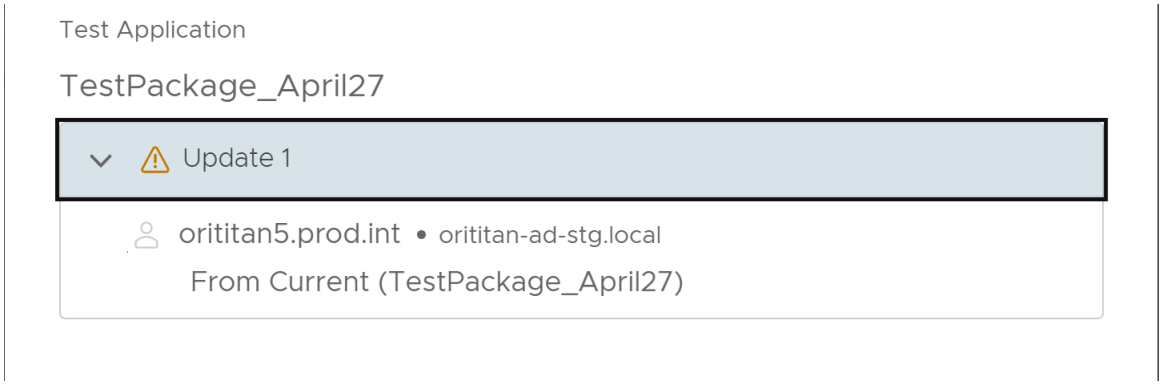
Lors de la création d'un droit, le module d'application récemment sélectionné peut être une mise à jour d'un droit existant ou d'un nouveau droit. Si le module d'application récemment sélectionné est le même que l'actuel, le droit n'est pas modifié pour l'utilisateur ou le groupe d'utilisateurs.

Scénarios de droit

Mettre à jour

Le module sélectionné remplace le droit existant de l'utilisateur ou du groupe d'utilisateurs. Par conséquent, le droit est considéré comme une mise à jour de l'actuel.

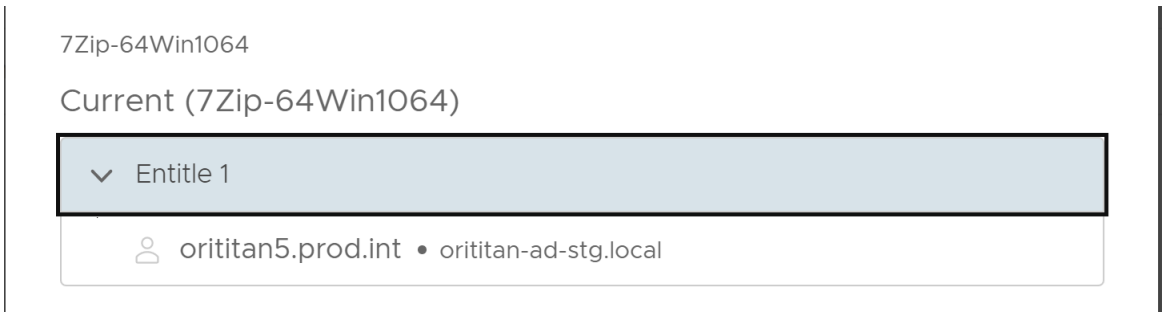
Sur l'image suivante, orititan5.prod.int est un utilisateur autorisé avec `Current (Testpackage_April27)`. Lorsque `TestPackage_April27` est sélectionné, ce droit remplace `Current (Testpackage_April27)`. Par conséquent, ce scénario est considéré comme une mise à jour.



Nouveau (autoriser l'accès)

Le module sélectionné est un nouveau droit d'accès de l'utilisateur ou du groupe d'utilisateurs.

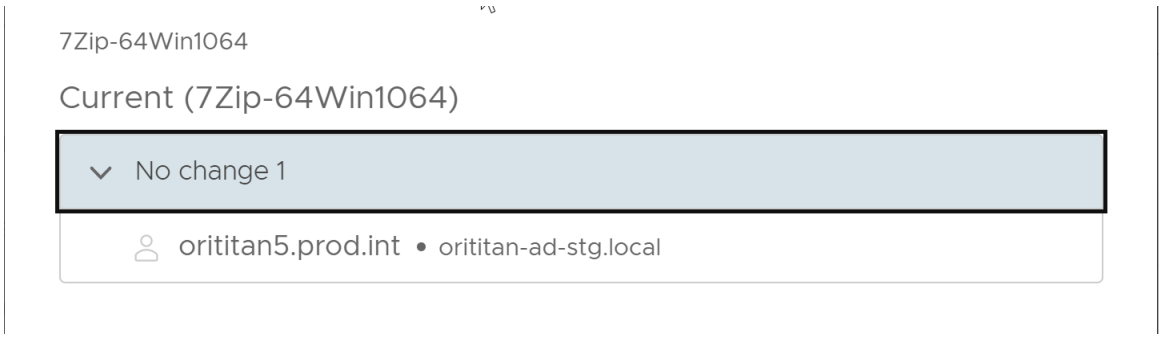
Sur l'image suivante, `Current (7Zip-64Win1064)` est un nouveau droit d'accès de l'utilisateur, orititan5.prod.int.



Aucune modification

L'utilisateur ou le groupe d'utilisateurs est déjà autorisé à accéder au module sélectionné, le droit n'est donc pas modifié.

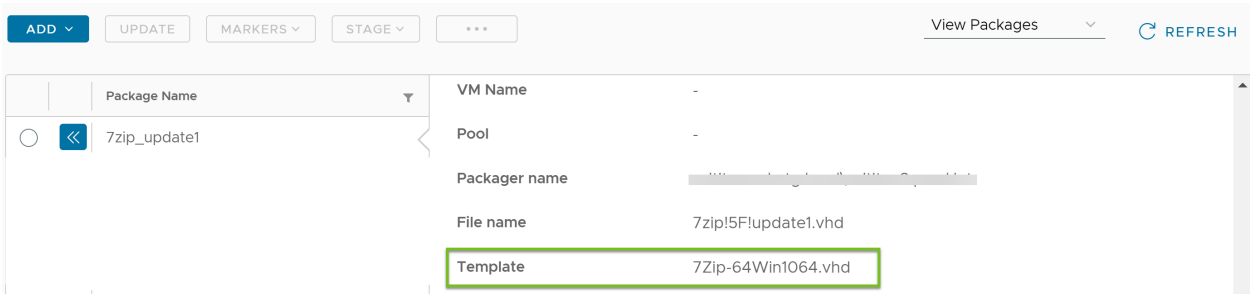
Sur l'image suivante, `Current (7Zip-64Win1064)` est de nouveau sélectionné pour le droit, mais l'utilisateur, orititan5.prod.int, est déjà autorisé à accéder au même module. Par conséquent, le droit d'accès n'est pas modifié.



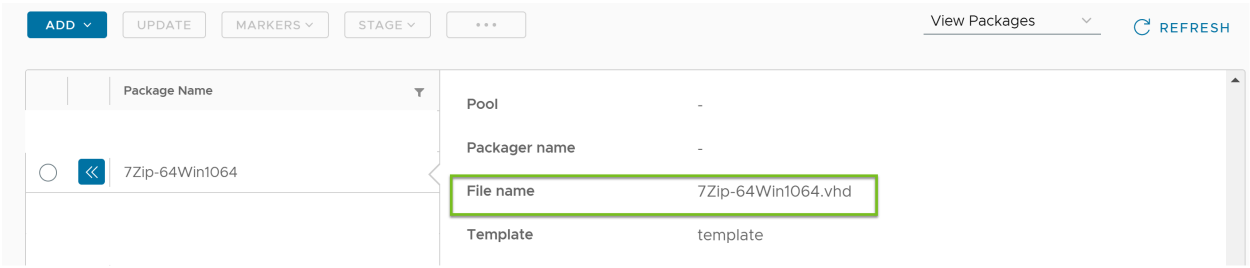
Mettre à jour un module d'application App Volumes à l'aide d'Horizon Cloud Service - next-gen

Vous pouvez créer une version d'un module existant en mettant à jour le module existant. Le module existant est le modèle ou il agit comme module de base pour la nouvelle version du module.

Dans la capture d'écran suivante, `7zip_update1` est le module mis à jour et `7Zip-64Win1064.vhd` est le modèle, qui est le nom de fichier du module existant.



Dans la capture d'écran suivante, `7Zip-64Win1064` est le module existant et le nom de fichier est `7Zip-64Win1064.vhd`.



Conditions préalables

Assurez-vous que le module que vous souhaitez mettre à jour a terminé le processus de création du module et que l'état du module est `Ready`.

Procédure

1. Dans Horizon Universal Console, accédez à **Catalogue de postes de travail et d'applications > App Volumes**.
2. Cliquez sur **Afficher les modules**.

3 Sélectionnez le module que vous souhaitez mettre à jour.

4 Cliquez sur **METTRE À JOUR**.

5 Dans la fenêtre **Mettre à jour le module**, ajoutez les informations requises.

6 Cliquez sur **Enregistrer**.

Résultats

Le module mis à jour s'affiche dans la liste des modules.

Supprimer un module d'application App Volumes à l'aide d'Horizon Cloud Service - next-gen

Si vous ne souhaitez plus de module, vous pouvez le supprimer.

Conditions préalables

Assurez-vous de supprimer le marqueur ou le droit d'accès au module avant de supprimer ce dernier.

Procédure

1 Dans Horizon Universal Console, accédez à **Catalogue de postes de travail et d'applications > App Volumes**.

2 Cliquez sur **Afficher les modules**.

3 Sélectionnez le module que vous souhaitez supprimer.

4 Cliquez sur le bouton de sélection, puis sur **SUPPRIMER**.

5 Dans la fenêtre **Supprimer le module**, cliquez sur **SUPPRIMER**.

Le module est supprimé de la liste des modules.

> **Note** Si le module est dans l'état `Delete Failed`, réessayez de le supprimer.
>
> Le module peut être dans cet état notamment si un ou plusieurs utilisateurs ont ouvert une session sur leur poste de travail et utilisent actuellement ce module d'application.

Définir le marqueur CURRENT sur un module d'application App Volumes à l'aide d'Horizon Cloud Service - next-gen

Si une application dispose de plusieurs modules et que vous souhaitez fournir la dernière version de l'application à un utilisateur ou à un groupe d'utilisateurs, vous pouvez définir le marqueur `CURRENT` sur le module. Vous pouvez configurer l'utilisateur ou le groupe d'utilisateurs pour recevoir toujours la version du module qui contient le marqueur, même si ce dernier est supprimé d'un module et défini sur l'autre module.

Voici quelques éléments à prendre en compte lors de la définition d'un marqueur `CURRENT` sur un module :

- Vous ne pouvez pas effectuer les opérations de transfert et de suppression sur un module défini avec un marqueur `CURRENT`.

Pour effectuer l'une des deux opérations, vous devez supprimer le marqueur du module.

- Un seul module d'application peut être défini comme `CURRENT`.

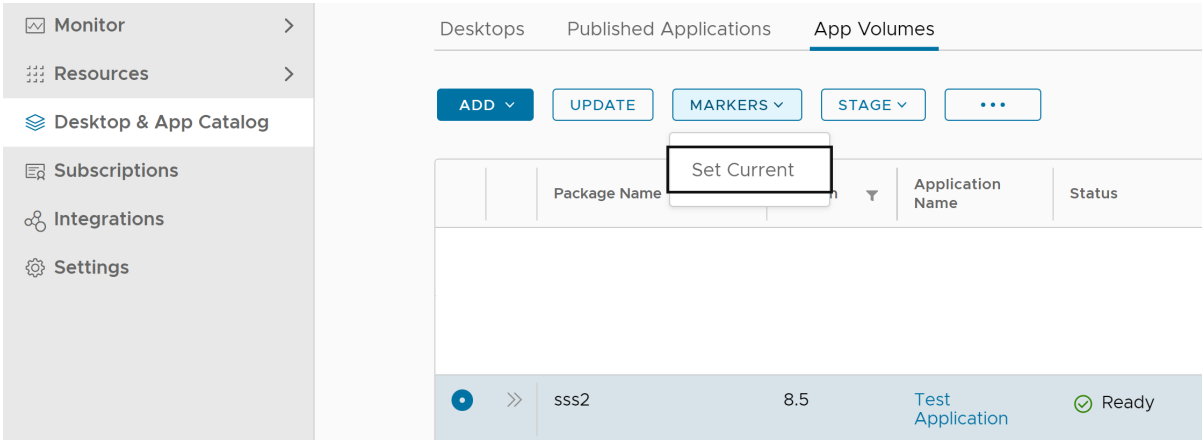
Conditions préalables

Assurez-vous que le module à marquer comme `CURRENT` a terminé le processus de création du module et que l'état du module est `Ready`.

Procédure

1. Dans Horizon Universal Console, accédez à **Catalogue de postes de travail et d'applications > App Volumes**.
2. Cliquez sur l'application qui dispose du module sur lequel vous souhaitez définir le marqueur `CURRENT`.

   La liste des modules pour cette application s'affiche.
3. Sélectionnez le module.
4. Cliquez sur **MARQUEURS > Définir l'élément actuel**.



5. Dans la boîte de dialogue **Définir l'élément actuel**, cliquez sur **DÉFINIR**.

   Le nom du module s'affiche avec le marqueur `CURRENT`.

Étape suivante

Vous pouvez désormais attribuer ce module à des utilisateurs ou des groupes d'utilisateurs. Pour plus d'informations sur la création d'un droit, reportez-vous à la section Créer un droit pour une application App Volumes à l'aide d'Horizon Cloud Service - next-gen.

VMware Horizon® Cloud Service™ - next-gen : annuler la définition du marqueur CURRENT sur un module d'application App Volumes

Si un module d'application marqué comme `Current` n'est plus la dernière version, vous pouvez supprimer le marqueur `Current` sur le module. Si vous définissez le marqueur sur un autre module pour la même application, cette action annule automatiquement la définition du marqueur sur le module précédent.

Une application ne peut avoir qu'un seul module marqué comme `Current`.

Lorsqu'un marqueur est supprimé d'un module, les droits cessent de recevoir le module `Current`. Si le marqueur est déplacé vers un autre module, les droits commencent automatiquement à recevoir le module qui est défini sur `Current`.

Procédure

1. Dans Horizon Universal Console, accédez à **Catalogue de postes de travail et d'applications > App Volumes**.
2. Cliquez sur **Afficher les modules**.

3. Sélectionnez le module avec le marqueur `Current`.
4. Cliquez sur **MARQUEURS > Supprimer Current**.
5. Dans la fenêtre de confirmation **Supprimer Current**, cliquez sur **SUPPRIMER**.

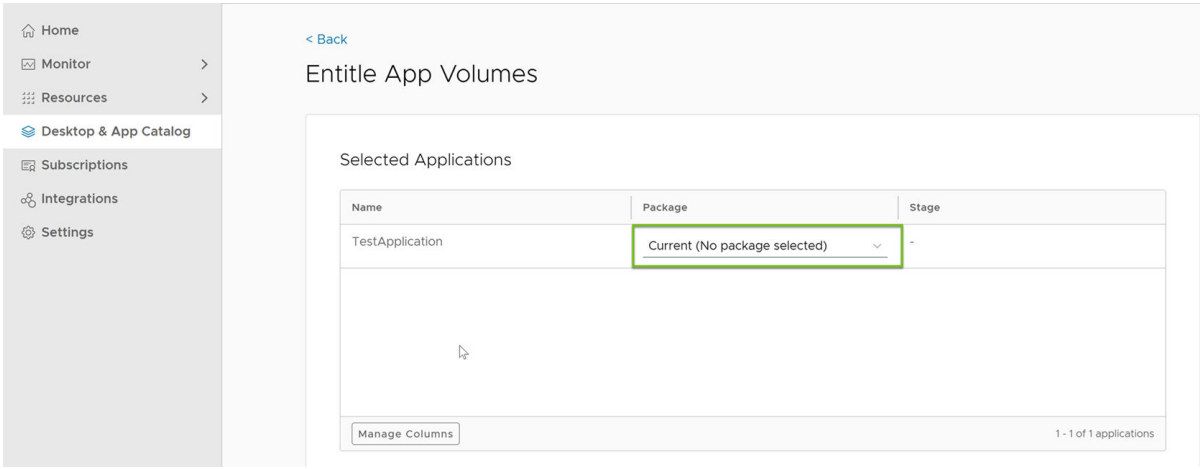
   Le module ne dispose plus du marqueur `Current`.

Créer un droit pour une application App Volumes à l'aide d'Horizon Cloud Service - next-gen

Pour fournir un module d'application App Volumes à un utilisateur final, vous devez autoriser l'accès d'un utilisateur ou d'un groupe d'utilisateurs à une application.

Voici quelques éléments à prendre en compte lors de la création de droits d'accès à une application :

- Le droit d'accès à une application peut être attribué à un ou plusieurs utilisateurs ou groupes d'utilisateurs.
- Un droit peut être créé en fonction d'une version de module spécifique ou d'un marqueur `CURRENT` qui n'est pas encore défini sur un module. Si vous choisissez le marqueur `CURRENT`, l'application est attribuée à l'utilisateur ou au groupe d'utilisateurs. Plus tard, lorsqu'un module pour cette application est créé et marqué `CURRENT`, l'utilisateur ou le groupe d'utilisateurs reçoit ce module.



- Pour un droit basé sur des marqueurs, l'utilisateur ou le groupe d'utilisateurs reçoit toujours le module avec la version `CURRENT`. Si l'administrateur définit le marqueur `CURRENT` sur un autre module, l'utilisateur ou le groupe d'utilisateurs reçoit le nouveau module ayant le marqueur `CURRENT` lors de la connexion suivante.
- Une application peut être attribuée à un utilisateur ou à un groupe d'utilisateurs même si elle ne dispose d'aucun module.

Pour que le module d'application soit distribué à l'utilisateur ou au groupe d'utilisateurs, l'état du module doit être `Ready`.

Vous pouvez également attribuer plusieurs applications à un utilisateur ou à un groupe d'utilisateurs en même temps.

Conditions préalables

Un module se trouve dans l'état `Ready` après la capture d'une application. Pour plus d'informations, reportez-vous à la section Capturer un module d'application App Volumes à l'aide d'Horizon Cloud Service - next-gen.

Avant de créer un droit App Volumes, vous devez d'abord créer une attribution de postes de travail VDI flottants. En raison des besoins de traitement des systèmes d'exploitation Microsoft Windows 10 et Windows 11, cette attribution doit disposer d'un modèle de poste de travail VMware recommandé qui fournit au moins 2 vCPU et 4 Go de RAM.

Procédure

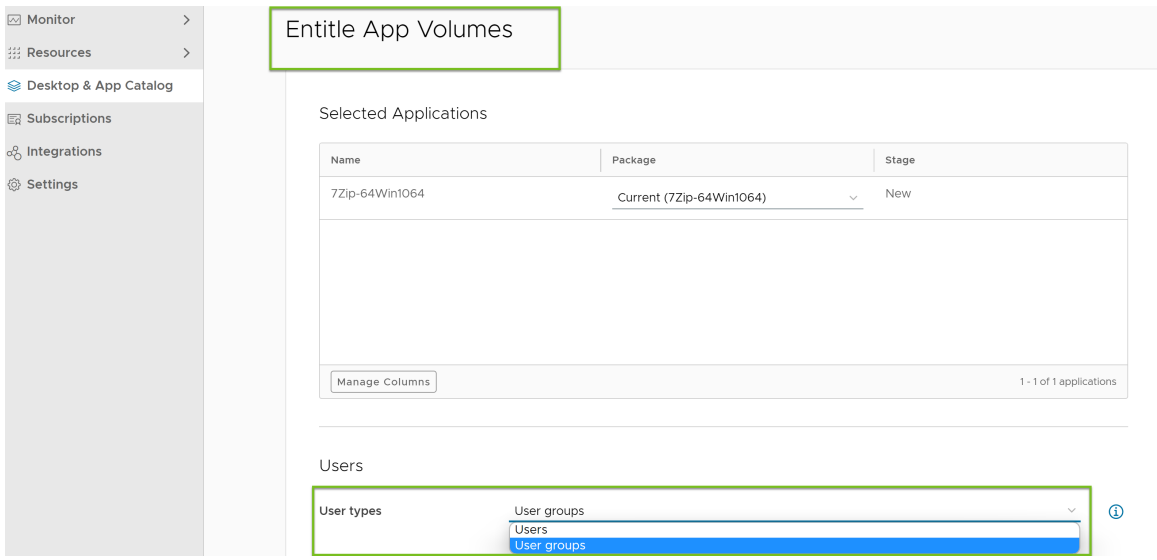
1. Dans Horizon Universal Console, accédez à **Catalogue de postes de travail et d'applications > App Volumes**.
2. Sélectionnez l'application à laquelle vous souhaitez attribuer l'accès par un utilisateur ou un groupe d'utilisateurs.
3. Cliquez sur **Droit > AUTORISER L'ACCÈS**.

4 Sur la page **Autoriser App Volumes**, procédez comme suit :

a Sélectionnez le module souhaité.

b Sélectionnez les **Types d'utilisateurs**.

c En fonction du type d'utilisateur sélectionné à l'étape précédente, ajoutez les utilisateurs ou les groupes d'utilisateurs.



5 Cliquez sur **Enregistrer**.

Tous les droits d'accès d'une application s'affichent dans l'onglet **Droits**.

a Accédez à **Catalogue de postes de travail et d'applications > App Volumes**.

b Cliquez sur une application.

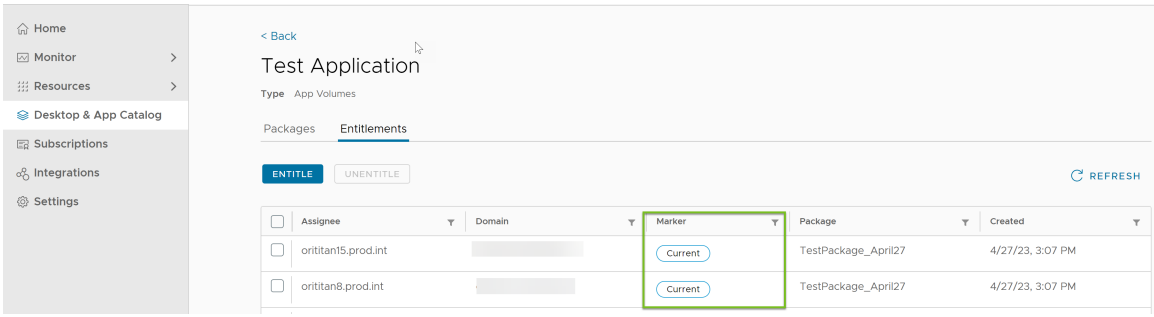
c Sur la page Détails de l'application, cliquez sur l'onglet **Droits**.

Tous les droits associés à l'application s'affichent sur la page.

Note Dans Horizon Cloud Service first-gen, chaque attribution peut disposer de plusieurs applications qui peuvent être attribuées à plusieurs utilisateurs ou groupes d'utilisateurs. Par conséquent, la page Attribution affiche toutes les applications et leurs utilisateurs ou groupes d'utilisateurs correspondants.

Toutefois, dans VMware Horizon® Cloud Service™ - next-gen, la page des droits d'accès à l'application affiche uniquement l'utilisateur ou les groupes d'utilisateurs associés aux modules d'application spécifiques pour cette application spécifique uniquement.

Si un module ayant un marqueur `CURRENT` est choisi pour un utilisateur ou un groupe d'utilisateurs spécifique, la colonne **Marqueur** sur cette page affiche `CURRENT` pour ce droit d'utilisateur ou de groupe d'utilisateurs.



Supprimer un droit App Volumes à l'aide d'Horizon Cloud Service - next-gen

Vous pouvez modifier le droit d'accès à une application en supprimant les droits de l'application. Pour supprimer des droits, vous pouvez utiliser le bouton **Annuler l'autorisation d'accès**.

Procédure

1. Dans Horizon Universal Console, accédez à **Catalogue de postes de travail et d'applications > App Volumes**.
2. Sélectionnez l'application souhaitée.
3. Cliquez sur **DROITS > Annuler l'autorisation d'accès > ..**
4. Dans la fenêtre **Annuler l'autorisation d'accès à l'application**, sélectionnez les destinataires.
5. Cliquez sur **ANNULER L'AUTORISATION D'ACCÈS**.

Résultats

Sur la page **Catalogue de postes de travail et d'applications**, vous pouvez constater que la colonne Droits de l'application affiche `0` en raison de la suppression de tous les droits pour cette application.

Intégrer Horizon Cloud Service - next-gen à Workspace ONE Intelligent Hub

Vous pouvez accéder à vos postes de travail et applications depuis Workspace ONE Intelligent Hub sans devoir entrer vos informations d'identification.

Conditions préalables

- Le locataire d'accès est créé hors ligne ou à l'aide du workflow d'accès actuel.
- Workspace ONE Access est sélectionné comme fournisseur d'identité lorsque vous connectez votre fournisseur d'identité. Pour plus d'informations, reportez-vous à la section Connexion de votre fournisseur d'identité.
- Les versions 8.10 et ultérieures d'Horizon Client sont utilisées.

Procédure

1 Connectez-vous à Horizon Universal Console.

2 Sur la page **Accueil**, cliquez sur **Intégrations** .

3 Sur la page **Intégrations**, cliquez sur **Gérer** sur la vignette **Workspace ONE Intelligent Hub**.

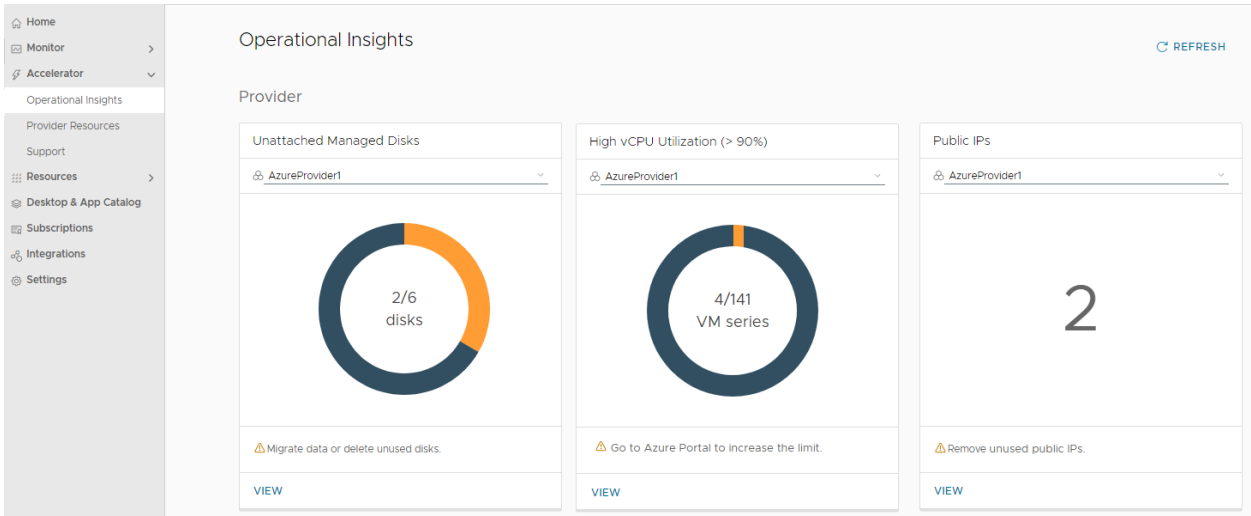
4 Sur la page **Workspace ONE Intelligent Hub**, sélectionnez l'option pour activer **Intelligent Hub**.

Les droits sont désormais visibles par l'utilisateur final sur Workspace ONE Intelligent Hub.

Note Pour cette fonctionnalité, seuls les clients Windows, Mac, Linux et HTML Access sont pris en charge.

Horizon Accelerator - Mise en route

Cette page de documentation explique comment démarrer avec l'offre SaaS VMware Horizon Accelerator (VHA). Les liens en bas permettent d'accéder à des pages contenant des informations plus détaillées.



Brève introduction

Horizon Accelerator est une SKU de module complémentaire pour les abonnements de la licence universelle Horizon.

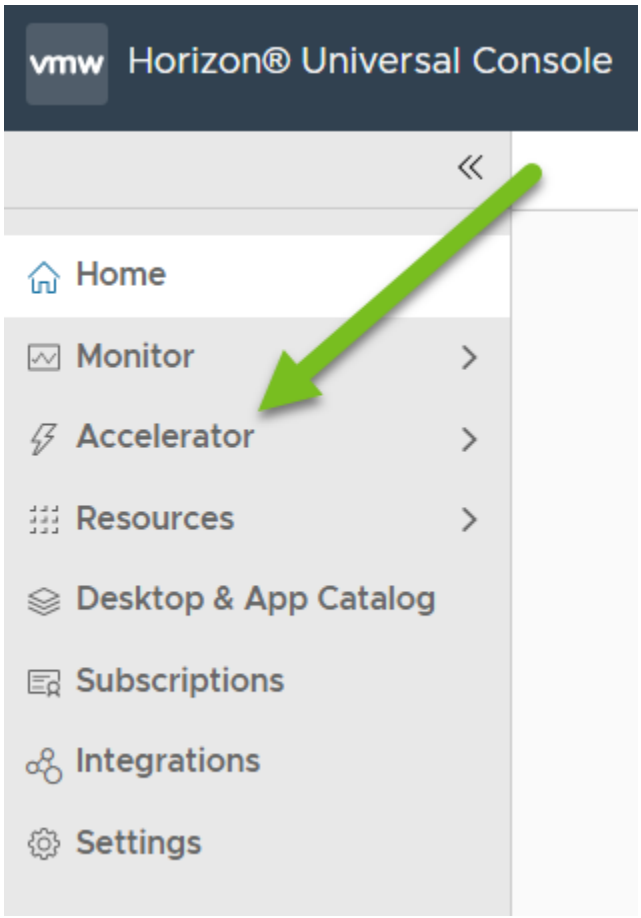
Horizon Accelerator vous fournit une prise en charge continue du jour 0 au jour 2 de votre environnement Horizon Cloud Service - next-gen et la possibilité d'obtenir des informations sur votre environnement et une visibilité de celui-ci.

Grâce à Horizon Accelerator, vous obtenez un retour sur investissement plus rapide et évitez la complexité et la courbe d'apprentissage de votre environnement VDI. L'expertise VDI dédiée augmente votre personnel informatique et réduit la charge de travail des opérations du jour 0 au jour 2.

Accédez aux fonctionnalités d'Horizon Accelerator dans le Centre de contrôle VHA d'Horizon Universal Console.

Exigences

Lorsque la licence associée à votre environnement de nouvelle génération vous autorise à utiliser Horizon Accelerator. Horizon Universal Console affiche automatiquement **Accelerator** dans le volet de navigation de la console, comme illustré dans la capture d'écran suivante.



À mesure que les nouvelles fonctionnalités sont publiées dans le plan de contrôle du cloud, elles deviennent automatiquement disponibles pour votre utilisation.

Pour vérifier les licences associées à votre environnement, utilisez la page Abonnements de la console. Reportez-vous à la section Utiliser Horizon Universal Console pour suivre vos licences Horizon. Pour utiliser Horizon Accelerator, votre environnement nécessite les éléments suivants :

- Abonnement Horizon qui fournit des SKU complémentaires. Les abonnements Horizon sont décrits dans la Matrice de comparaison des abonnements VMware Horizon.
- Licence d'Horizon Accelerator.
- Vous avez effectué l'intégration à Horizon Cloud Service - next-gen Chapitre 4 Intégration pour les administrateurs Horizon Cloud Service - next-gen.

Centre de contrôle VMware Horizon Accelerator (VHA)

Avec ce centre de contrôle, vous obtenez une analyse et une visibilité des ressources des fournisseurs configurés avec votre environnement de nouvelle génération sans devoir vous connecter à l'interface utilisateur ou au portail de chaque fournisseur et examiner chaque ressource individuelle.

Analyses opérationnelles

La vue **Analyses opérationnelles** fournit des analyses exploitables et des conseils à l'écran dans les ressources du fournisseur que vous pouvez ajuster afin de réduire les coûts opérationnels.

Chaque zone liée aux ressources met en évidence les problèmes qui peuvent exister et révèle des opportunités d'optimisation.

Analyses des ressources de l'infrastructure

La vue **Ressources de fournisseur** fonctionne conjointement avec la vue **Analyses opérationnelles** pour fournir une visibilité des ressources du fournisseur.

Cette possibilité d'obtenir une visibilité de l'état des ressources du fournisseur peut être particulièrement utile pour les administrateurs de votre environnement de nouvelle génération qui peuvent ne pas avoir accès au portail du fournisseur.

La vue **Ressources du fournisseur** comporte une fonctionnalité d'exportation des données de ressources dans un format de fichier téléchargeable. Une fonctionnalité d'actualisation permet d'obtenir les données au moment où vous souhaitez les consulter.

Service d'assistance Horizon Pros

Le Service d'assistance Horizon Pros est composé d'une équipe d'experts, Horizon Pros, dédiés à la livraison Horizon. Les experts Horizon Pros fournissent les services suivants :

- Prise en charge 24h/24, 7 j/7
- Expertise VDI dédiée
- Prise en charge complète du cycle de vie, y compris l'optimisation du jour 0 au jour 2, et des conseils tels que les architectures standard, les meilleures pratiques, etc.
- Conseils d'experts sur les types de déploiement d'Horizon

Note Les fonctionnalités du Service d'assistance Horizon Pros sont fournies pour les déploiements de Microsoft Azure et sur site.

Pour obtenir une description du support 24 h/24 par VMware pour les déploiements cloud, reportez-vous à la section PDF de support de production VMware pour les produits cloud sur le site vmware.com.

En savoir plus

Pour obtenir des descriptions plus détaillées des fonctionnalités ci-dessus, utilisez les liens suivants.

Horizon Accelerator - Analyses opérationnelles

Cette page de documentation décrit la fonctionnalité Centre de contrôle d'Horizon Accelerator qui fournit des analyses opérationnelles sur les fournisseurs de ressources utilisées pour votre environnement Horizon Cloud Service - next-gen.

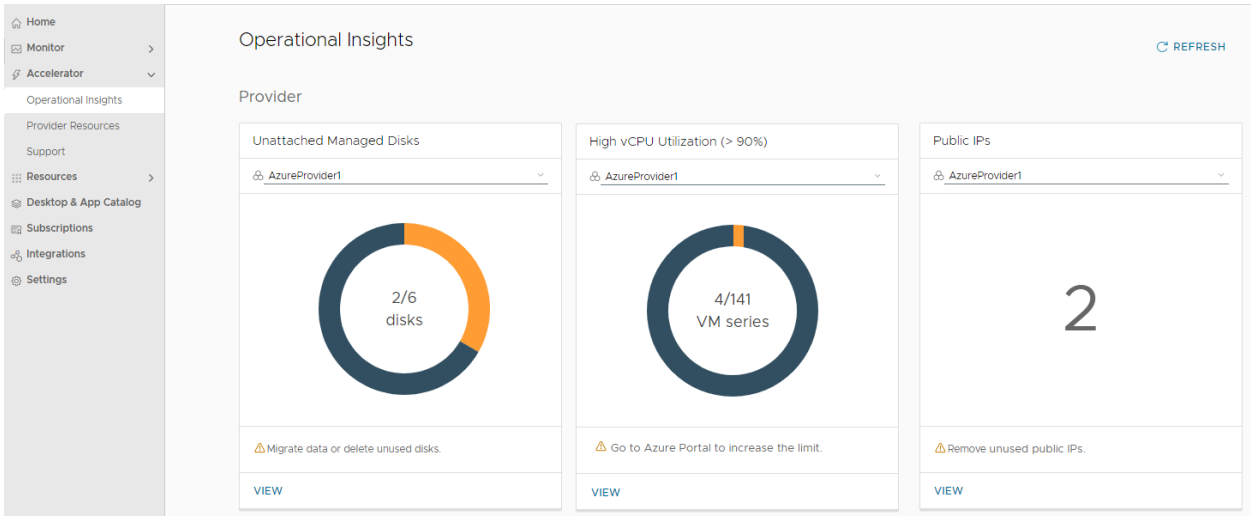
Cette fonctionnalité peut être utilisée dans Horizon Universal Console lorsque vous disposez de la licence de module complémentaire Horizon Accelerator.

Actuellement, cette fonctionnalité peut être utilisée avec le fournisseur de capacité Microsoft Azure.

Introduction

La vue **Analyses opérationnelles** fournit des analyses exploitables et des conseils à l'écran dans les ressources du fournisseur que vous pouvez ajuster afin de réduire les coûts opérationnels.

La capture d'écran suivante illustre l'emplacement de l'interface utilisateur, **Accelerator > Analyses opérationnelles**. Cette capture d'écran illustre également cette vue lorsqu'un fournisseur Microsoft Azure est sélectionné pour chacun des indicateurs.



Chaque zone liée aux ressources met en évidence les problèmes qui peuvent exister et révèle des opportunités d'optimisation.

Dans chaque vue détaillée, vous pouvez examiner les détails de la ressource de fournisseur et voir des instructions pour corriger les problèmes.

Informations sur les ressources - Fournisseur Microsoft Azure

Dans la version actuelle, l'option **Analyses opérationnelles** fournit des analyses pour les ressources suivantes que votre environnement de nouvelle génération utilise à partir des fournisseurs Microsoft Azure configurés pour elle.

Chaque indicateur affiché fournit des données qui correspondent au fournisseur de ressources spécifique sélectionné en haut de l'indicateur et au type de ressource spécifique.

Info-bulle Pour Microsoft Azure, le fournisseur est basé sur un abonnement Azure. Les données affichées sont spécifiques aux ressources situées dans l'abonnement associé au fournisseur sélectionné.

Pour chaque indicateur et vue détaillée, le système obtient des informations en fonction des caractéristiques que l'API Azure fournit pour ce type de ressource spécifique.

Disques gérés non attachés

Cet indicateur fournit des informations sur le nombre de disques gérés non attachés qui existent dans le fournisseur sélectionné.

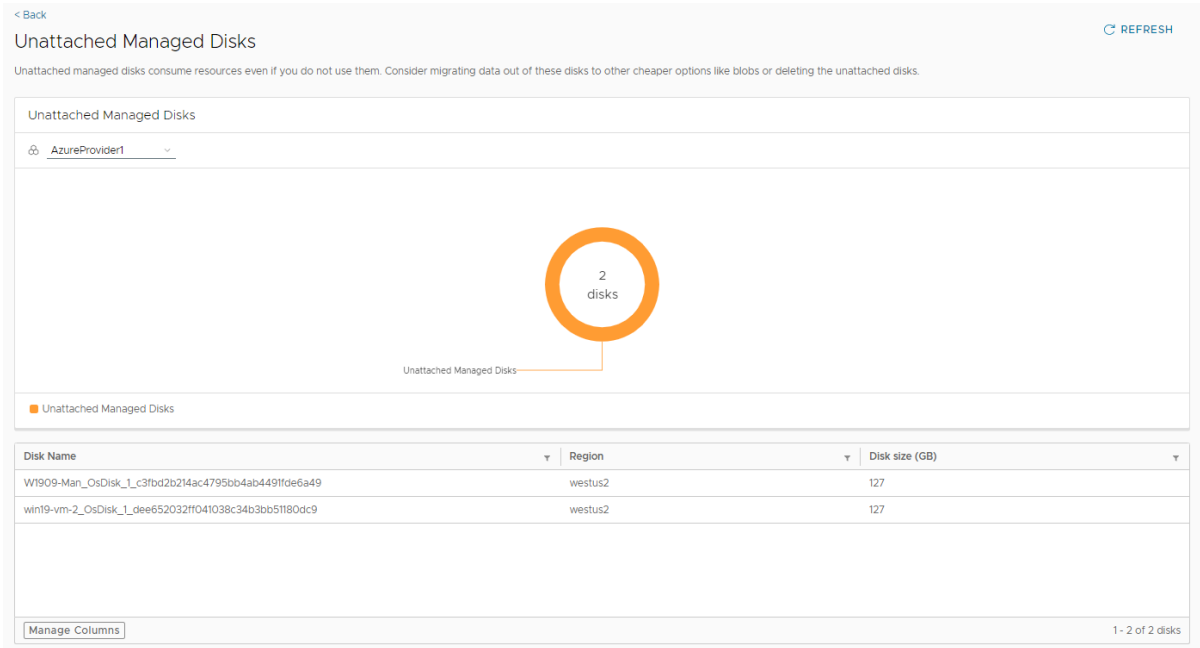
L'indicateur reflète la liste globale des disques gérés dans le fournisseur sélectionné et indique quels sous-ensembles de ces disques sont attachés à des machines virtuelles et lesquels ne sont pas attachés à des machines virtuelles.

Comme décrit dans la documentation de Microsoft Azure, les disques gérés Azure sont un stockage haute performance conçu pour être utilisé avec des machines virtuelles Azure.

Étant donné qu'un abonnement Azure entraîne un coût pour chaque disque géré, la présence de disques non attachés est une analyse exploitable.

- **Solution recommandée** : les disques gérés non attachés consomment des ressources, même si le disque n'est pas utilisé. Envisagez de migrer toutes les données sur disque dont vous avez besoin à partir de ces disques non attachés pour réduire les coûts, par exemple les fichiers blob. Lorsque vous avez terminé la migration des données, supprimez les disques inutilisés.
- **Afficher** : affichez la liste des disques gérés non attachés par nom, région et taille de disque.

La capture d'écran suivante illustre la vue détaillée.



Utilisation élevée du vCPU (> 90 %)

Cet indicateur fournit des informations sur les séries de machines virtuelles qui peuvent nécessiter une augmentation du quota de calcul du fournisseur.

L'indicateur reflète l'utilisation actuelle du quota Azure Compute dans le fournisseur sélectionné et quelle série de machines virtuelles a une utilisation de vCPU de 90 % ou plus.

Une utilisation supérieure à 90 % est une analyse exploitable vous permettant de demander un quota supplémentaire pour cette série de machines virtuelles dans la région Azure indiquée afin de vous assurer que le quota existe dans le fournisseur avant qu'il ne soit nécessaire.

- **Solution recommandée** : envisagez d'augmenter le quota pour les séries de machines virtuelles dont l'utilisation de vCPU est égale ou supérieure à 90 %. L'augmentation du quota d'une série de machines virtuelles s'effectue dans le portail Azure à l'aide de la lame **Quotas** et du filtrage sur **Calcul** et la région Azure concernée.
- **Afficher** : affichez la liste des séries de machines virtuelles Azure qui ont une utilisation de vCPU de 90 % ou plus. À partir de cette vue, vous pouvez déterminer les séries de machines virtuelles spécifiques pour lesquelles demander une augmentation de quota.

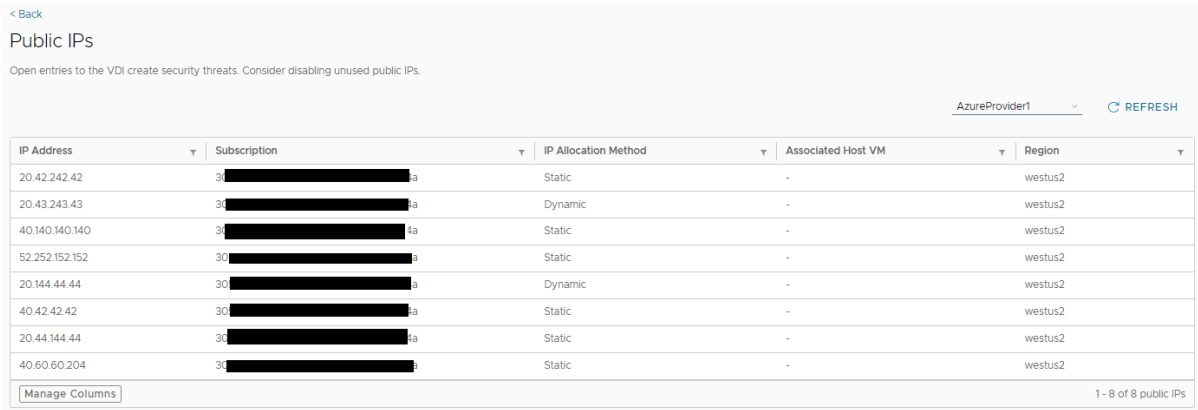
Adresses IP publiques

Du point de vue de la sécurité, la meilleure pratique consiste à limiter le nombre d'entrées ouvertes à Virtual Desktop Infrastructure (VDI) à partir du monde externe.

Bien que les instances d'Unified Access Gateway et de passerelle Horizon Edge de VDI nécessitent des adresses IP publiques, cette analyse opérationnelle détecte toutes les autres adresses IP publiques activées dans le réseau du fournisseur et fournit une liste pour votre examen.

- **Solution recommandée** : vérifiez et désactivez les adresses IP publiques non souhaitées ou inutilisées.
- **Afficher** : affichez la liste des adresses IP publiques et les informations associées, telles que leur adresse IP et la machine virtuelle associée.

La capture d'écran suivante illustre la vue détaillée. Certaines valeurs sont modifiées à des fins de confidentialité.



Actions de l'interface utilisateur : Filtrer, Gérer les colonnes, Actualiser

Chaque section fournit ces actions standard.

Filtres

Chaque en-tête de colonne fournit une icône de filtrage.

Actualiser

Lorsque vous accédez à une vue détaillée à partir de la vue des indicateurs, le système extrait les données du fournisseur de ressources sélectionné et affiche les données. Les données que vous voyez sont les données à jour.

Si vous affichez les données depuis un certain temps et que vous souhaitez extraire les dernières données, cliquez sur **Actualiser** pour remplir cette section avec les données les plus récentes.

Gérer les colonnes

Utilisez cette fonctionnalité pour afficher et masquer les colonnes de l'affichage.

Horizon Accelerator - Ressources du fournisseur

Cette page de documentation décrit la fonctionnalité Centre de contrôle d'Horizon Accelerator pour afficher les ressources du fournisseur utilisées pour votre environnement Horizon Cloud Service - next-gen.

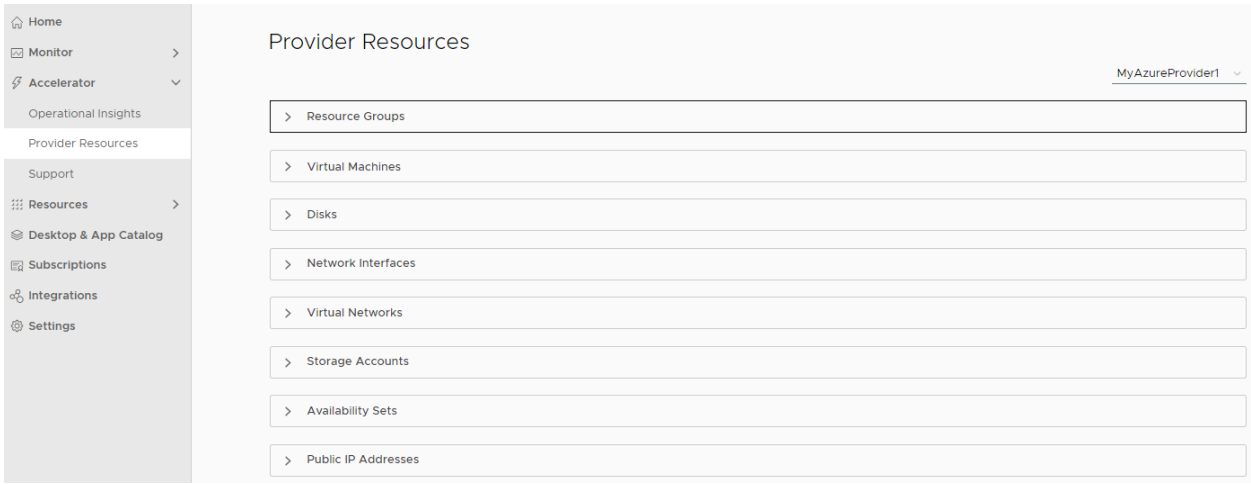
Cette fonctionnalité peut être utilisée dans Horizon Universal Console lorsque vous disposez de la licence de module complémentaire Horizon Accelerator.

Actuellement, cette fonctionnalité peut être utilisée avec le fournisseur de capacité Microsoft Azure.

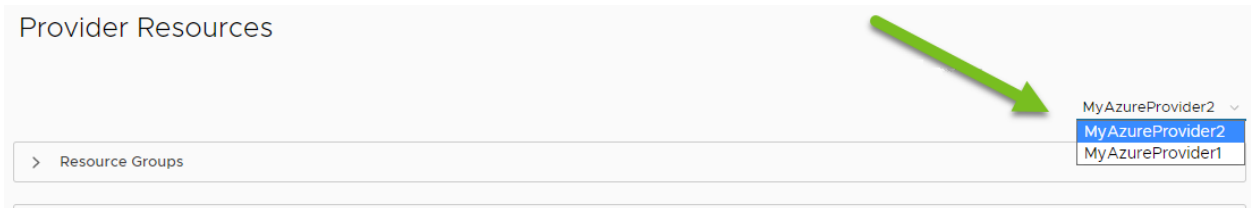
Introduction

Avec le Centre de contrôle d'Horizon Accelerator, vous obtenez une visibilité des ressources du fournisseur utilisées par votre environnement de nouvelle génération sans devoir vous connecter à l'interface utilisateur ou au portail de chaque fournisseur et examiner chaque ressource individuelle.

La capture d'écran suivante illustre l'emplacement de cette vue **Ressources du fournisseur** dans la console, **Accelerator > Ressources du fournisseur** et comment cette vue s'affiche pour un fournisseur Microsoft Azure.



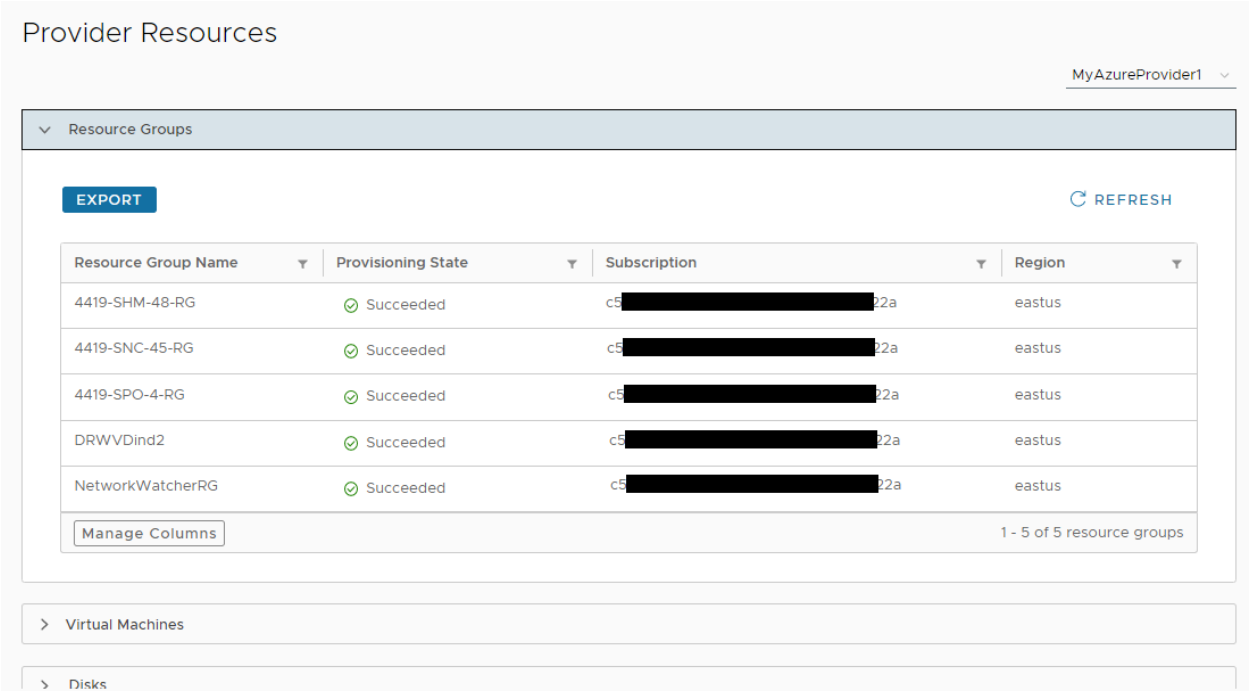
La liste de sélection de fournisseurs située dans le coin supérieur droit de cette vue illustre chaque fournisseur configuré dans votre environnement de nouvelle génération. Cette liste facilite la sélection des ressources d'un fournisseur particulier à afficher.



Pour afficher les informations sur chaque type de ressource, développez sa section.

Lorsque vous développez une section, le système récupère les données, afin que vous disposiez des informations les plus récentes.

La capture d'écran suivante illustre un exemple de section développée. Les informations d'abonnement sont modifiées à des fins de confidentialité.



Fournisseur Microsoft Azure : types de ressources

Dans la version actuelle, la vue **Ressources du fournisseur** fournit des données pour les ressources suivantes que votre environnement de nouvelle génération utilise à partir des fournisseurs Microsoft Azure configurés pour elle.

Pour chacun de ces types de ressources, lorsque vous développez une catégorie dans l'interface utilisateur, le système appelle une API Azure pour récupérer les données les plus récentes de Microsoft Azure et l'abonnement dans lequel résident les ressources.

Pour chaque type de ressource affiché, le système fournit les données qui correspondent au fournisseur de ressources spécifique sélectionné dans la liste supérieure droite en haut de la vue **Ressources du fournisseur**.

Info-bulle Pour Microsoft Azure, le fournisseur est basé sur un abonnement Azure. Les données affichées sont propres aux ressources situées dans un abonnement associé au fournisseur que vous sélectionnez dans la liste de sélection en haut à droite.

Pour chaque type de ressource, le système obtient des informations en fonction des caractéristiques que l'API Azure fournit pour ce type de ressource spécifique. Par exemple, même si Azure fournit une caractéristique de l'`état du provisionnement` pour les groupes de ressources, Azure ne fournit pas cette caractéristique pour les interfaces réseau.

Par conséquent, la section de l'interface utilisateur de chaque type de ressource contient des colonnes et des filtres en fonction de ce que l'appel d'API du système vers Azure renvoie pour ce type de ressource.

Les colonnes affichées représentent les caractéristiques qu'Azure associe au type de ressource.

Lorsqu'Azure définit et prend en charge des valeurs spécifiques pour une caractéristique particulière, vous pouvez effectuer un filtrage sur ces valeurs connues à l'aide de l'icône de filtre dans l'en-tête de colonne.

Note Pour les caractéristiques liées à l'état, les valeurs affichées dans ces colonnes sont basées sur les valeurs qu'Azure renvoie vers l'appel d'API du système. La documentation Azure fait référence à ces valeurs en tant que valeurs connues prises en charge par le service. Au fil du temps, Azure peut ajouter de nouvelles valeurs connues ou mettre à jour les noms spécifiques qu'il utilise pour ses valeurs connues. Les valeurs liées à l'état indiquées dans les listes suivantes sont à jour au moment de la rédaction du présent document.

Groupes de ressources

Répertorie les groupes de ressources dans ce fournisseur et affiche des informations sur chacun d'entre eux, comme sa région Azure. La colonne **État du provisionnement** indique l'état du déploiement de chaque groupe de ressources.

- **Nom du groupe de ressources** : nom du groupe de ressources.
- **État du provisionnement** : pour cette caractéristique liée à l'état, Azure signale les valeurs `Réussi`, `Échec`, `Suppression` et `Mise à jour`.
- **ID d'abonnement** : ID de l'abonnement Azure associé.
- **Région** : nom de la région Azure dans laquelle réside la ressource.

Machines virtuelles

Répertorie les machines virtuelles dans ce fournisseur et affiche des informations sur chacune d'elles, telles que sa carte réseau et son adresse IP.

- **Nom de la machine virtuelle** : nom de la machine virtuelle (VM).
- **ID d'abonnement** : ID de l'abonnement Azure associé.
- **Groupe de ressources** : nom du groupe de ressources.
- **Nom de l'interface réseau** : nom de l'interface réseau (NIC) associé à la VM.
- **Nom du réseau virtuel** : nom du réseau virtuel associé à la carte réseau.
- **Adresse IP** : adresse IP définie sur la carte réseau.
- **Taille de la machine virtuelle** : modèle de VM Azure utilisé pour la VM.

Disques

Répertorie les disques de ce fournisseur et affiche des informations sur chacun d'eux, telles que l'état et la taille du disque.

- **Nom du disque** : nom attribué au disque.
- **État du disque** : pour cette caractéristique liée à l'état, Azure signale les valeurs `Non attaché`, `Attaché`, `SAS actif`, `SAS actif bloqué`, `Bloqué`, `Chargement actif`, `Prêt à charger` et `Réservé`.

  Pour obtenir des définitions précises de toutes ces valeurs Azure connues, reportez-vous à la page Type d'état de disque dans la documentation d'Azure.

  Les états de disque qui s'affichent généralement pour un environnement de nouvelle génération sont `Attaché`, `Réservé` et `Non attaché`. Les disques attachés sont attachés aux VM en cours d'exécution. Les disques réservés sont attachés à des VM arrêtées et désallouées. Les disques non attachés ne sont utilisés par aucune VM.
- **ID d'abonnement** : ID de l'abonnement Azure associé.
- **Groupe de ressources** : nom du groupe de ressources.
- **Région** : nom de la région Azure dans laquelle réside la ressource.
- **Taille du disque (Go)** : taille du disque.

Note Comme décrit dans la documentation d'Azure, un état de disque non attaché signifie que le disque est utilisé dans cet abonnement. Autrement dit, le disque était précédemment attaché à un poste de travail, et même si ce dernier est supprimé, le disque existe toujours côté Azure.

Info-bulle Lorsque vous disposez de pools de postes de travail flottants, si vous constatez que cette vue **Disques** répertorie plusieurs disques `Non attachés` pour le groupe de ressources de ce pool, il est recommandé de supprimer ces disques non attachés afin d'éviter les coûts dans Microsoft Azure. Un état non attaché indique généralement que le disque ne fournit aucune utilisation et qu'il peut avoir été orphelin à partir d'un poste de travail flottant supprimé.

Interfaces réseau

Répertorie les interfaces réseau de ce fournisseur et affiche des informations sur chacune d'entre elles, par exemple dans quel groupe de ressources elles résident.

- **Nom de l'interface réseau** : nom de l'interface réseau (NIC).
- **ID d'abonnement** : ID de l'abonnement Azure associé.
- **Nom du groupe de ressources** : nom du groupe de ressources.
- **Région** : nom de la région Azure dans laquelle réside la ressource.

Réseaux virtuels

Répertorie les réseaux virtuels (VNet) de ce fournisseur et affiche des informations sur chacun d'entre eux, par exemple son état d'appairage. Pour chaque réseau virtuel, cette vue répertorie ses préfixes d'adresses définis.

- **Nom du réseau virtuel** : nom du réseau virtuel.
- **État du provisionnement** : pour cette caractéristique liée à l'état, Azure signale les valeurs `Réussi`, `Échec`, `Suppression` et `Mise à jour`.
- **ID d'abonnement** : ID de l'abonnement Azure associé.
- **Nom du groupe de ressources** : nom du groupe de ressources.
- **Préfixe d'adresse** : préfixe d'adresse dans ce réseau virtuel.
- **État d'appairage** : pour cette caractéristique liée à l'état, Azure signale les valeurs `Connecté`, `Déconnecté` et `Lancé`.

Comptes de stockage

Répertorie les comptes de stockage de ce fournisseur et affiche des informations sur chacune d'entre elles, par exemple dans quel groupe de ressources elles résident.

- **Nom du compte de stockage** : nom du compte de stockage.
- **ID d'abonnement** : ID de l'abonnement Azure associé.
- **Nom du groupe de ressources** : nom du groupe de ressources.
- **Région** : nom de la région Azure dans laquelle réside la ressource.

Groupes à haute disponibilité

Répertorie les groupes à haute disponibilité de ce fournisseur et affiche des informations sur chacun d'eux, par exemple dans quel groupe de ressources ils résident.

- **Groupes à haute disponibilité** : nom du groupe à haute disponibilité.
- **ID d'abonnement** : ID de l'abonnement Azure associé.
- **Nom du groupe de ressources** : nom du groupe de ressources.

Adresses IP publiques

Répertorie les adresses IP publiques de ce fournisseur et affiche des informations sur chacune d'entre elles, par exemple leur méthode d'allocation (`statique`, `dynamique`).

- **Nom d'adresse IP publique** : nom de l'adresse IP publique.
- **État du provisionnement** : pour cette caractéristique liée à l'état, Azure signale les valeurs `Réussi`, `Échec`, `Suppression` et `Mise à jour`.
- **Adresse IP publique** : adresse IP de cette adresse IP publique.
- **Version de l'adresse IP publique** : IPv4 ou IPv6.
- **Méthode d'allocation IP** : Azure renvoie la valeur `Dynamique` ou `Statique`.

- **Délai d'expiration (minutes)** : valeur du délai d'expiration pour l'adresse IP publique.
- **ID d'abonnement** : ID de l'abonnement Azure associé.
- **Région** : nom de la région Azure dans laquelle réside la ressource.

Actions de l'interface utilisateur : Filtrer, Gérer les colonnes, Actualiser et Exporter

Chaque section fournit ces actions standard.

Filtres

Chaque en-tête de colonne fournit une icône de filtrage. Si vous définissez des filtres sur une colonne, puis exportez les données, seules les données filtrées sont exportées dans le fichier CSV.

Gérer les colonnes

Utilisez cette fonctionnalité pour afficher et masquer les colonnes de l'affichage.

Actualiser

Lorsque vous développez une section, le système extrait les données du fournisseur de ressources et affiche les données. Au moment où vous développez une section, les données affichées sont celles qui sont les plus récentes de cette ressource, par exemple qu'elle se trouve dans le fournisseur sélectionné dans la liste du coin supérieur droit.

Dans chaque section, si vous affichez les données depuis un certain temps et que vous souhaitez extraire les dernières données, cliquez sur **Actualiser** dans cette section pour remplir cette section avec les données les plus récentes.

Exporter

Dans chaque section se trouve un bouton **Exporter** pour exporter les données au format CSV et rendre le fichier CSV disponible sur la page **Téléchargements** de la console.

Si vous avez défini l'un des filtres de colonne, ces filtres sont appliqués aux données exportées.

Lorsque vous cliquez sur **Exporter**, une boîte de dialogue s'affiche et fournit un champ vous permettant de personnaliser le nom du fichier. Vous pouvez entrer un nouveau nom ou accepter la valeur par défaut affichée.

Lorsque vous êtes prêt, le système permet le téléchargement du fichier sur la page **Téléchargements** de la console (**Surveiller > Téléchargements**.

Note Par défaut, le système dispose d'un délai d'expiration de 30 jours pour les fichiers sur la page **Téléchargements**. Au bout de 30 jours, les fichiers sont supprimés du système.

Horizon Accelerator - Horizon Pros - Support dédié

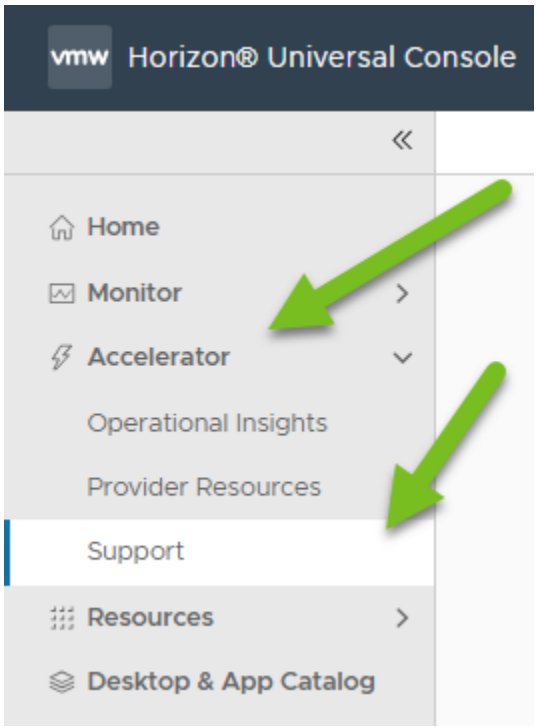
L'équipe du support Horizon Accelerator fournit une assistance dédiée et continue du jour 0 au jour 2 dans votre environnement Horizon Cloud Service - next-gen.

Note L'équipe Horizon Pros est également appelée équipe du support VMware Horizon Accelerator. Le nom de l'équipe apparaît en abrégé `Support VHA Accelerator` dans les e-mails et d'autres méthodes de contact.

Cette fonctionnalité peut être utilisée dans Horizon Universal Console lorsque vous disposez de la licence de module complémentaire Horizon Accelerator.

Fonctionnement

Pour demander de l'aide à l'équipe du support, cliquez sur **Accelerator > Support**.

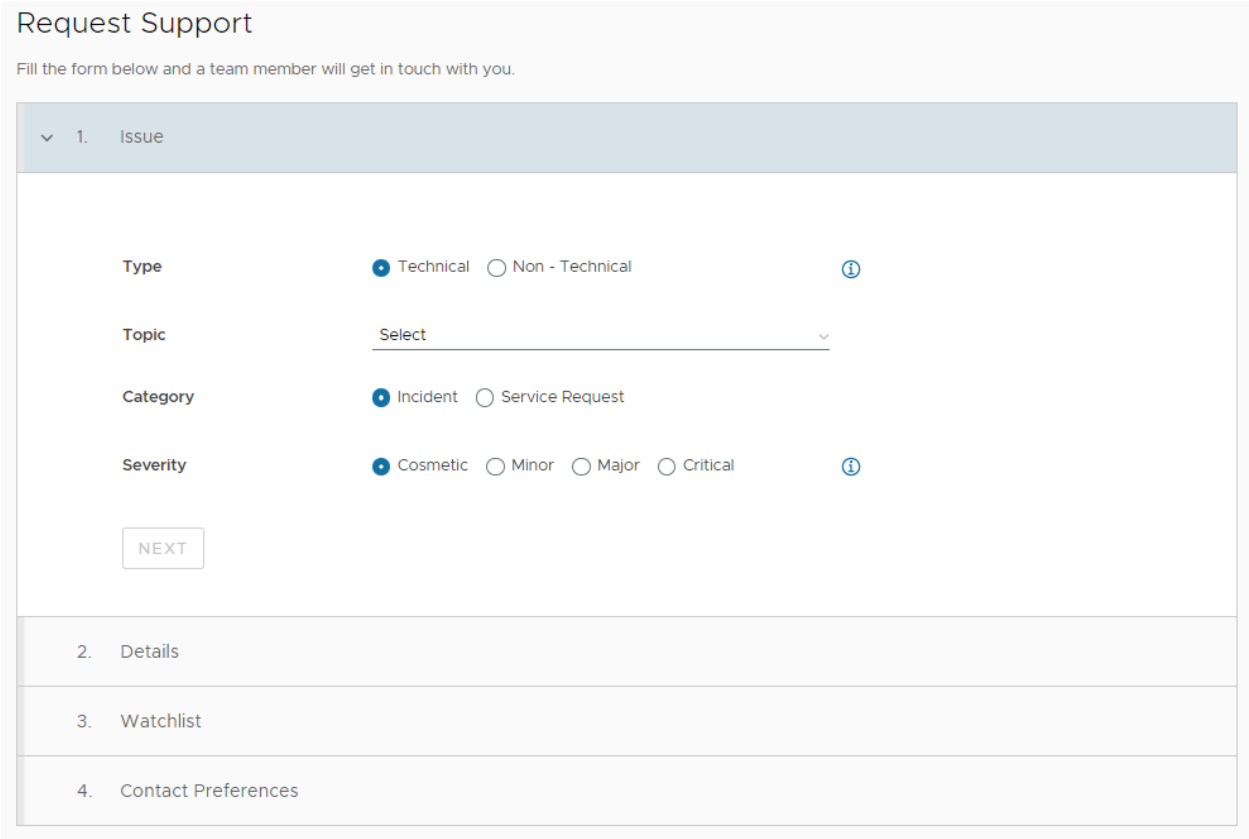


Une fois l'assistant terminé, l'un des agents de support est alerté et vous contactera à propos de votre demande.

Demander une assistance

Lorsque vous cliquez sur **Accelerator > Support**, la console démarre l'assistant **Demander une assistance**.

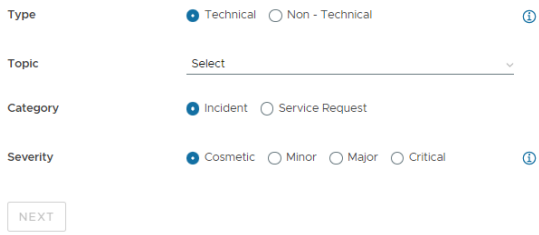
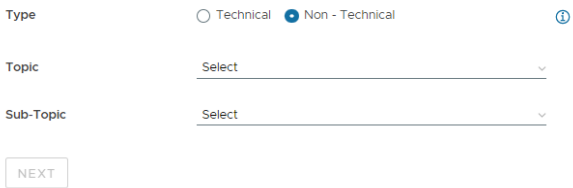
La capture d'écran suivante illustre l'apparence initiale de l'assistant.



Dans cet assistant, vous effectuez les sélections appropriées pour le type de support que vous demandez. Les sections suivantes décrivent chaque étape.

Étape 1 - Type de support

Déterminez d'abord si le type de demande est de nature technique ou non technique. Une catégorie de problème et une balise de gravité sont associées aux demandes d'ordre technique.

Type technique	Type non technique
	

Une fois le type choisi, suivez l'interface utilisateur pour mieux associer la demande à une rubrique à laquelle elle s'applique le mieux selon vous. (La rubrique ne comporte ni réponse juste ni réponse fausse.)

Sélectionnez la rubrique dans une liste définie par le système. Cette dernière inclut une rubrique `Autre` au cas où votre demande ne correspond pas vraiment aux autres demandes de la liste.

Étant donné que la console est dynamique et répertorie les choix disponibles les plus récents dans le système, cette documentation présente n'énumère pas les listes de rubriques ou de sous-rubriques. Si une tentative d'énumération était effectuée dans la documentation présente, celle-ci serait rapidement obsolète. Au lieu d'une liste énumérée, voici quelques exemples :

- Pour une demande d'ordre technique, les rubriques incluent les zones associées aux fonctions techniques telles que `Connectivité`, `Déploiement du dispositif Edge`, `Maintenance` et des concepts associés aux fonctions techniques semblables.
- Pour une demande d'ordre non technique, les rubriques incluent des domaines commerciaux et orientés licence, tels que `Compte avec droits`, `Utilisateurs et autorisations` et des concepts commerciaux semblables. Pour une demande d'ordre non technique, vous pouvez inclure une sous-rubrique pour une rubrique sélectionnée.

Pour type **Technique**, vous pouvez sélectionner une catégorie de problème :

Incident

Lorsque vous êtes confronté à un problème, tel qu'un service opérationnel interrompu, des problèmes de latence ou de performances et des faits semblables.

Les incidents sont balisés avec une balise de gravité, dans l'ordre de gravité décroissant **Critique**, **Majeure**, **Mineure**, **Superficielle**. Chaque gravité est associée à des temps de réponse initiaux cibles du Support VMware Horizon Accelerator.

Le tableau suivant fournit des instructions générales pour la sélection d'une gravité.

Gravité	Description	Temps de réponse initiale cible de Horizon Accelerator
Critique	Le problème a arrêté les opérations commerciales sans solution de procédure.	Dans un délai de 30 minutes
Majeur	Ce problème a une forte incidence sur certaines parties des opérations commerciales.	Dans un délai de 4 heures ouvrées
Mineur	Ce problème entraîne une perte de service partielle et non critique avec une faible incidence sur les opérations commerciales.	Dans un délai de 8 heures ouvrées
Cosmétique	Le problème est lié à l'apparence de l'application.	Dans un délai de 12 heures ouvrées

Note Au moment de la rédaction du présent document, les temps indiqués dans le tableau sont à jour avec les temps cibles de l'équipe du support VMware Horizon Accelerator. Vous pouvez utiliser l'assistant **Demander une assistance** si vous avez des questions sur vos propres temps.

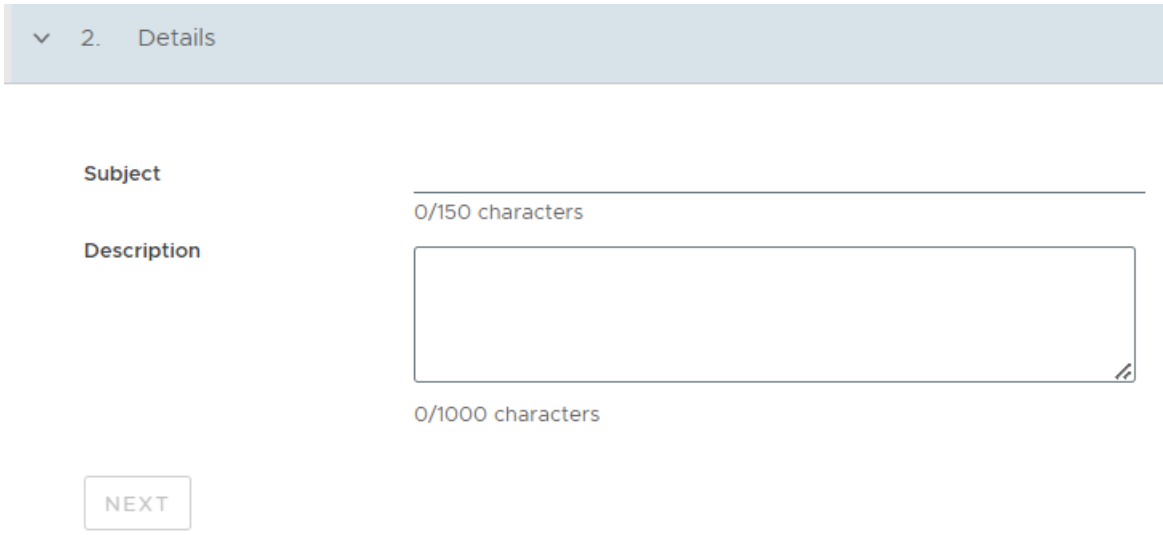
Demande de service

Lors de la demande d'informations ou d'une demande de tâche à effectuer par l'équipe de support dédiée.

Continuez à effectuer les choix d'interface utilisateur souhaités jusqu'à ce que cette dernière rende le bouton **Suivant** disponible. Cliquez sur **Suivant** pour enregistrer vos choix et passer à l'étape suivante.

Étape 2 - Détails

Cette étape commence par :

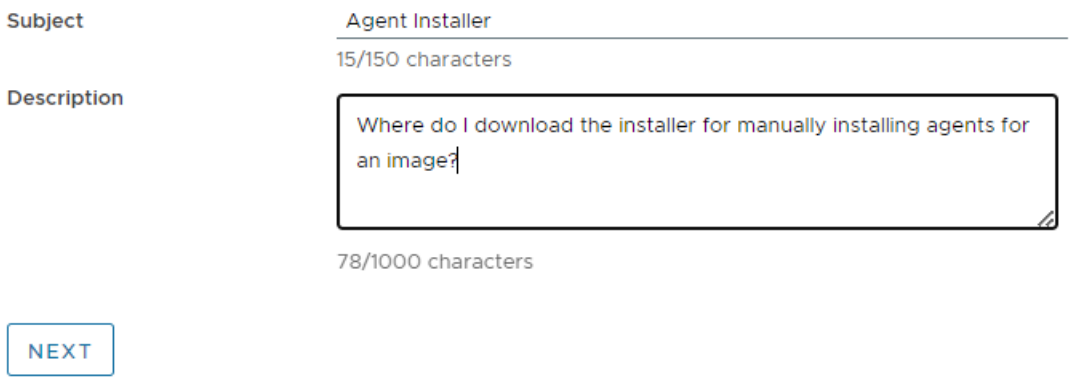


Utilisez le champ **Objet** pour fournir une brève description du problème ou la raison de cette demande d'aide.

Utilisez le champ plus grand pour fournir une description plus longue sur ce que vous attendez de l'assistance.

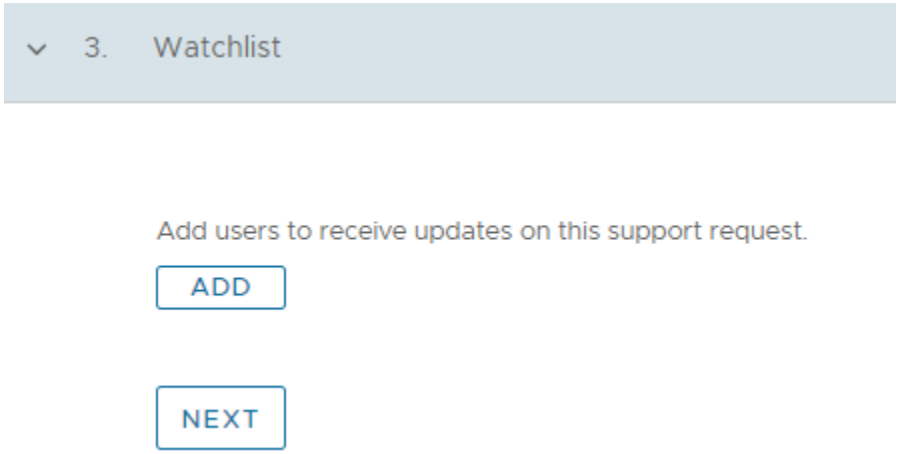
Lorsque la console rend l'option **Suivant** disponible, cliquez sur **Suivant** pour passer à l'étape suivante.

Exemple de capture d'écran :



Étape 3 - Liste de surveillance

Cette étape commence par :



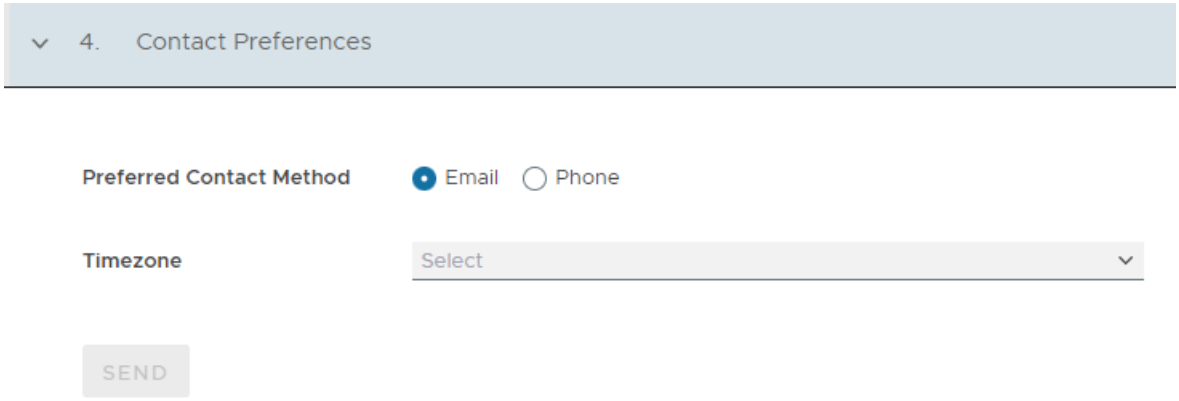
Utilisez le bouton **Ajouter** pour fournir les adresses e-mail des personnes dont vous souhaitez recevoir des mises à jour concernant cette demande. Pour ajouter le nom suivant, cliquez de nouveau sur **Ajouter**.

Note Par défaut, le système inclut automatiquement l'adresse e-mail de l'expéditeur de la demande (votre adresse e-mail). Le système utilise l'e-mail associé à la connexion que vous avez utilisée pour vous connecter à Horizon Universal Console.

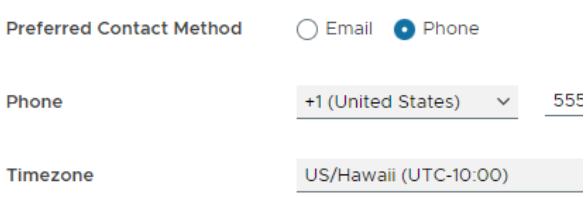
Lorsque la console rend l'option **Suivant** disponible et que vous avez ajouté les personnes souhaitées à la liste de surveillance, cliquez sur **Suivant** pour passer à l'étape suivante.

Étape 4 - Préférences de contact

Cette étape commence par :



Spécifiez la méthode que vous préférez que l'agent de support attribué utilise pour vous contacter à propos de cette demande. Lorsque vous sélectionnez **Téléphone**, fournissez un numéro de téléphone de contact.

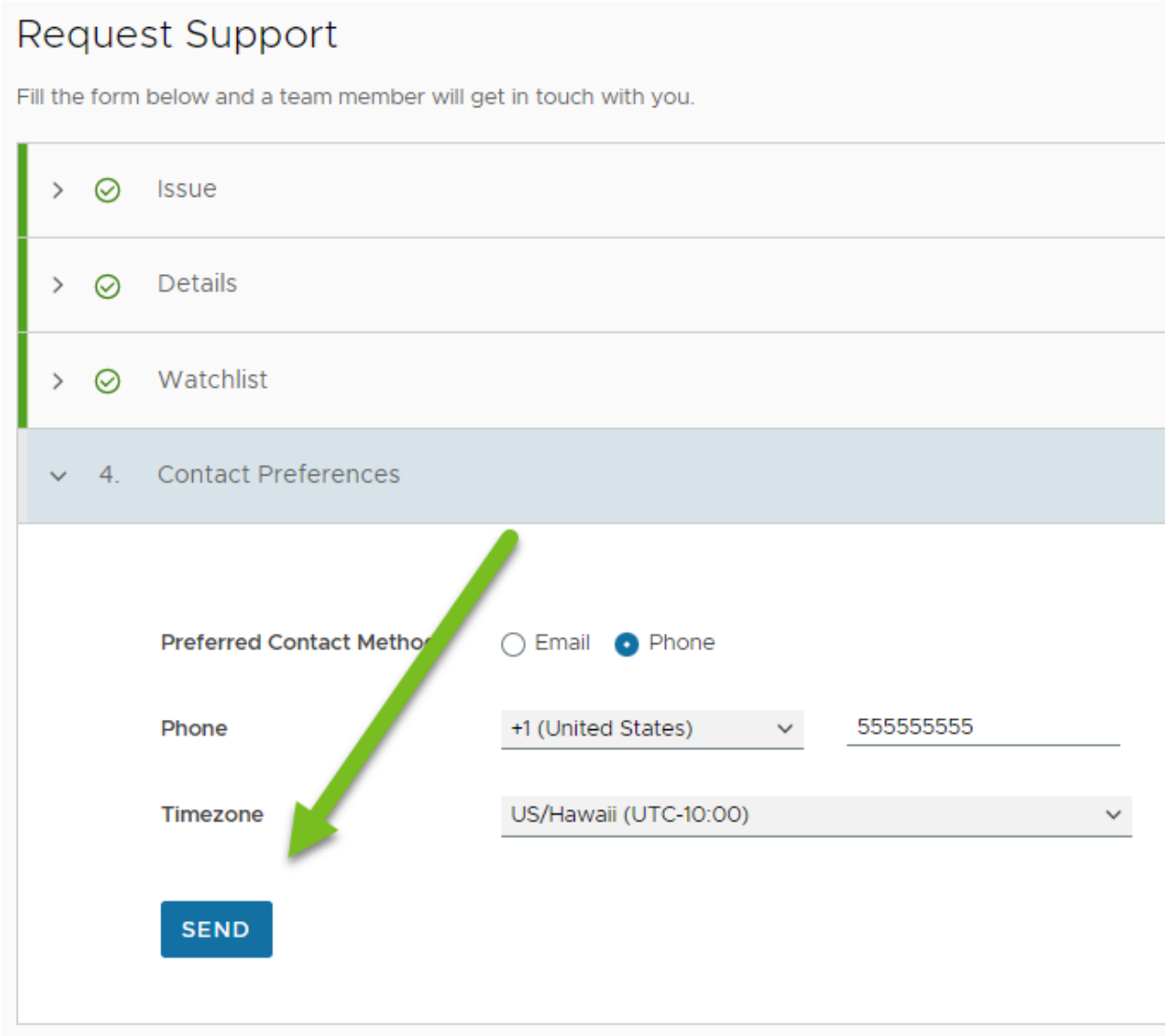
Méthode de contact par e-mail	Méthode de contact par téléphone
	

L'un des objectifs de l'équipe de support est que vous receviez une assistance pendant vos heures ouvrées. Pour atteindre cet objectif, l'agent de support déduit les heures ouvrées typiques de votre fuseau horaire sélectionné. Ce choix de fuseau horaire facilite une communication plus efficace entre l'équipe de support et votre équipe.

Lorsque la console rend l'option **Envoyer** disponible, vous pouvez cliquer sur **Envoyer** pour envoyer la demande de support.

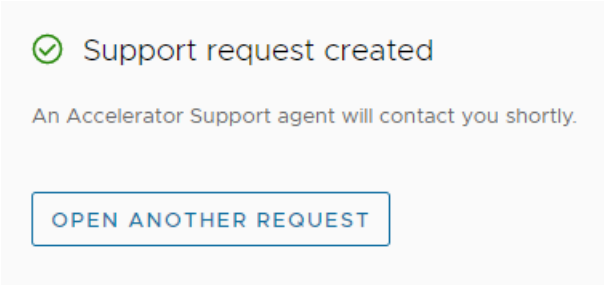
Envoyer la demande

Lorsque les étapes sont terminées dans l'interface utilisateur et que vous êtes prêt à envoyer la demande, cliquez sur **Envoyer**.



Lorsque vous cliquez sur **Envoyer**, la demande de support est acheminée vers l'équipe du support.

La console affiche un message de confirmation pour vous informer que la demande a été créée et est passée dans le pipeline de support.



Étape suivante

Le système informe l'équipe de Support VMware Horizon Accelerator de votre demande de support.

En même temps, le système envoie un e-mail à l'adresse de l'équipe de Support VMware Horizon Accelerator et met en Cc votre adresse e-mail et les adresses que vous avez entrées à l'étape **Liste de surveillance**.

Dès que l'équipe aura reçu la notification système de votre demande de support envoyée, elle vous contactera et commencera à traiter votre demande.

La notification qui s'affiche en premier est un e-mail de confirmation contenant l'adresse de l'équipe du support VHA Accelerator dans la ligne **À** et votre adresse e-mail et les e-mails que vous avez entrés dans l'étape **Liste de surveillance** de la ligne **Cc**.

Note Si vous ne recevez pas cet e-mail de confirmation dans les 15 minutes, vous pouvez renvoyer la demande.

L'expéditeur de l'e-mail sera l'équipe du support Horizon Cloud (adresse de l'expéditeur `do-not-reply-horizon@vmware.com`)

La ligne d'objet de l'e-mail inclut la chaîne `Ticket de support créé` et le corps inclut les informations que vous avez sélectionnées et saisies dans l'assistant.

Gestion et surveillance des ressources et des mises à niveau dans le plan de contrôle Horizon et Horizon Cloud Service - next-gen

6

Utilisez le plan de contrôle Horizon et la console d'administration d'Horizon Cloud Service - next-gen pour gérer les images, les pools, les postes de travail et les applications, les rôles et les licences. Utilisez également la console pour surveiller les ressources et les mesures, générer et afficher des journaux, et installer des correctifs et des mises à niveau de produits.

Lisez les sections suivantes :

- Gestion de votre environnement à l'aide de la console Horizon Universal Console
- Surveillance de votre environnement Horizon Cloud Service - next-gen
- Gestion du logiciel Horizon Agent
- Maintenance et mises à jour d'Horizon Edge dans Horizon Cloud Service - next-gen

Gestion de votre environnement à l'aide de la console Horizon Universal Console

Utilisez la console Horizon Universal Console pour gérer les images, les pools et les groupes de pools, les postes de travail et les applications, les rôles et les licences de l'utilisateur de votre environnement Plan de contrôle Horizon de nouvelle génération.

Une fois vos déploiements et configurations initiaux terminés, utilisez la console Horizon Universal Console pour une gestion continue. Pour plus d'informations, reportez-vous aux pages liées.

- Gestion des images - Gestion des images Horizon à l'aide du Plan de contrôle Horizon de nouvelle génération
- Gestion des pools et des groupes de pools - Gestion de provisionnement du pool
- Droits d'accès utilisateur - Autorisation de l'accès des utilisateurs finaux aux postes de travail et applications
- Gestion des rôles - Attribution de rôles administratifs aux utilisateurs Horizon Universal Console
- Licences - Utiliser Horizon Universal Console pour suivre vos licences Horizon

Notifications dans Horizon Cloud Service - next-gen

Horizon Cloud Service - next-gen utilise des notifications pour vous informer d'un événement important.

Affichage des notifications

Note

- Cette rubrique décrit la vérification des notifications d'Horizon Cloud à l'aide d'Horizon Universal Console. Vous avez également la possibilité de vérifier les notifications à l'aide de Cloud Services Console, également appelée plate-forme d'engagement de Cloud Services. Cependant, lorsque vous agissez sur les notifications, utilisez Horizon Universal Console.
- Si vous cliquez sur **Afficher toutes les notifications** dans l'icône en forme de cloche () située dans le coin supérieur droit de n'importe quelle page, vous êtes redirigé vers la page Mes notifications de Cloud Services Console.

  La page Mes notifications affiche toutes vos notifications, y compris celles générées à partir d'autres services.

  Pour afficher uniquement les notifications d'Horizon Cloud, cliquez sur **Afficher les notifications Horizon Cloud** et accédez à la page **Notifications** dans Horizon Universal Console.

Les options suivantes sont disponibles sur la page **Notifications**.

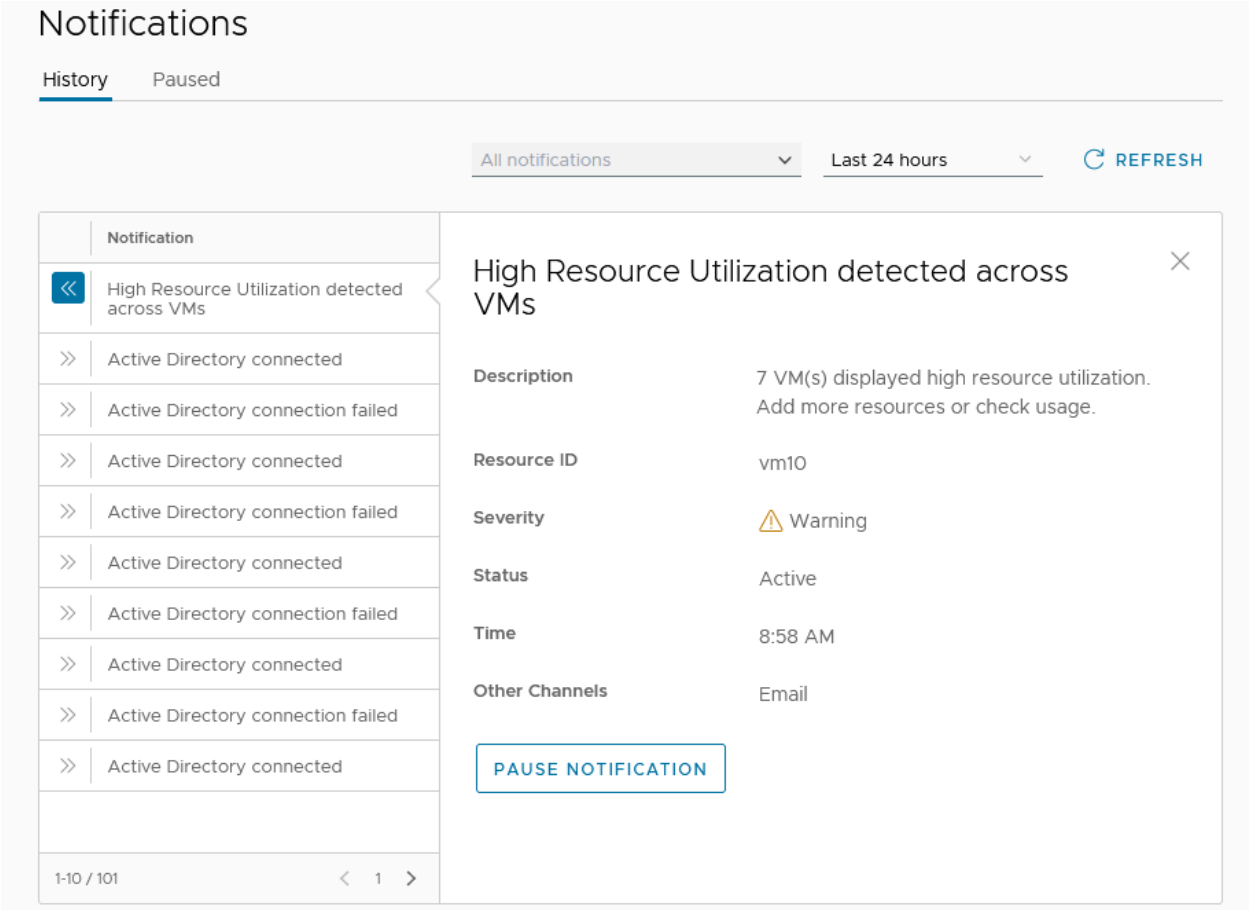
- L'onglet **Historique** affiche une liste de notifications basée sur les filtres de notification. Les paramètres de filtre se trouvent au-dessus de la liste de notifications. Vous pouvez filtrer les notifications par type et par période (jusqu'à 90 jours).

  Vous pouvez afficher les détails d'une notification en cliquant sur l'icône en forme de double flèche gauche pour cette notification. Les informations suivantes s'appliquent au volet Détails de la notification.

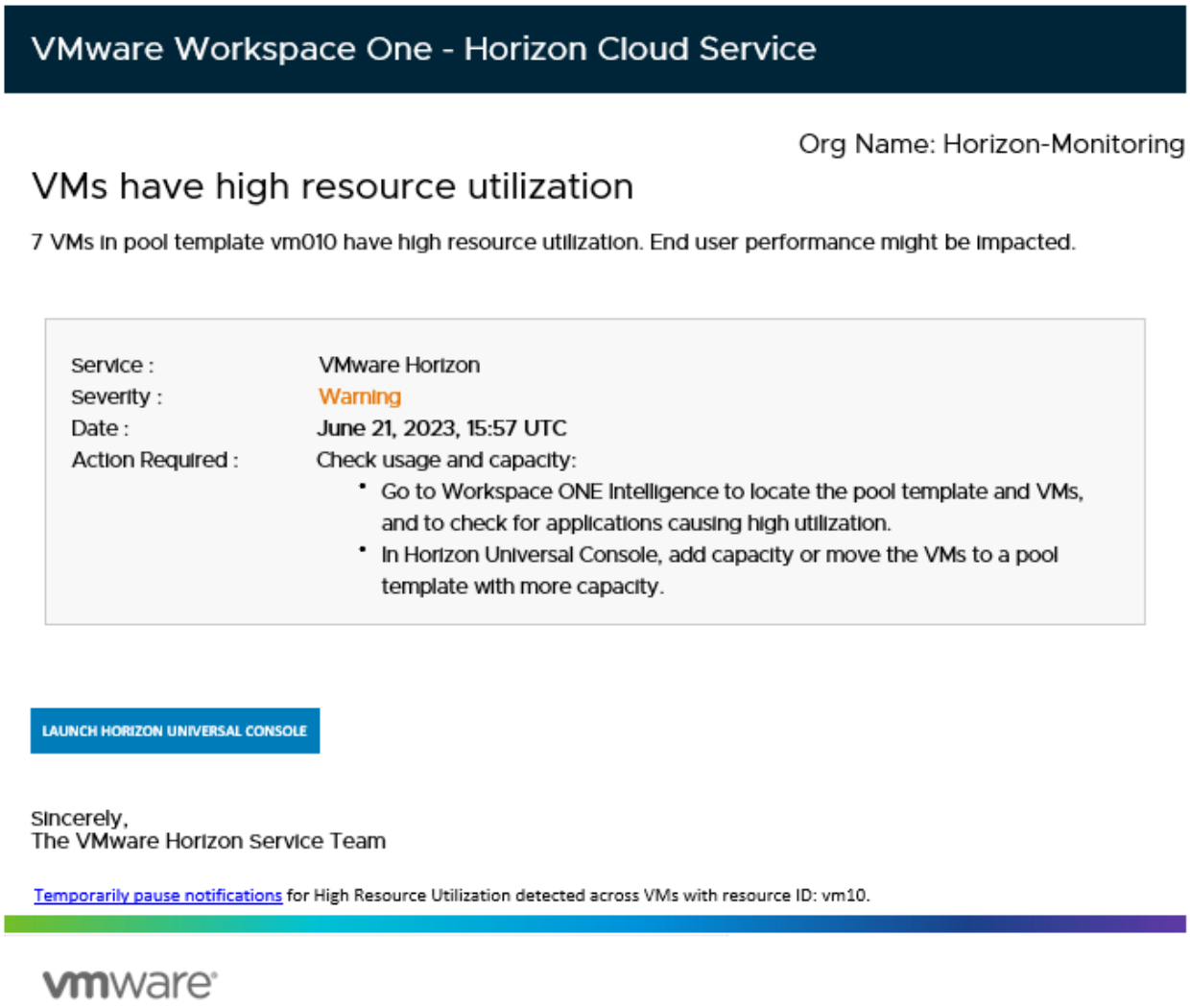
  - Les détails incluent **Description**, **ID de ressource**, **Gravité**, **État**, **Heure** et **Autres canaux** (comportant actuellement les notifications par e-mail).
  - Les états suivants s'appliquent.

Type de notification	Description
Actif	Notifications qu'un administrateur n'a pas encore traitées
Ignoré	Les notifications qu'un administrateur a indiquées ne nécessitent aucune attention particulière

Pour certains types de notifications à fréquence élevée, comme *Utilisation élevée des ressources détectée sur les VM*, une option **Suspendre la notification** est disponible, qui vous permet de suspendre ce type de notification pendant 72 heures maximum sur tous les canaux. L'option **Suspendre la notification** permet de résoudre la cause sans avertissements répétés.



Pour ces types de notification, vous recevez un e-mail, comme illustré par la capture d'écran de l'e-mail qui suit.



Vous pouvez suspendre ces types de notifications de deux manières :

- À partir de l'e-mail et en cliquant sur **Suspendre temporairement les notifications**, ce qui vous permet d'accéder directement à la notification sur la page Horizon Universal Console – Historique des notifications, sur laquelle vous pouvez cliquer sur **Suspendre la notification**.
- À partir d'Horizon Universal Console directement et en accédant à la page Historique des notifications, sur laquelle vous pouvez cliquer sur **Suspendre la notification**.

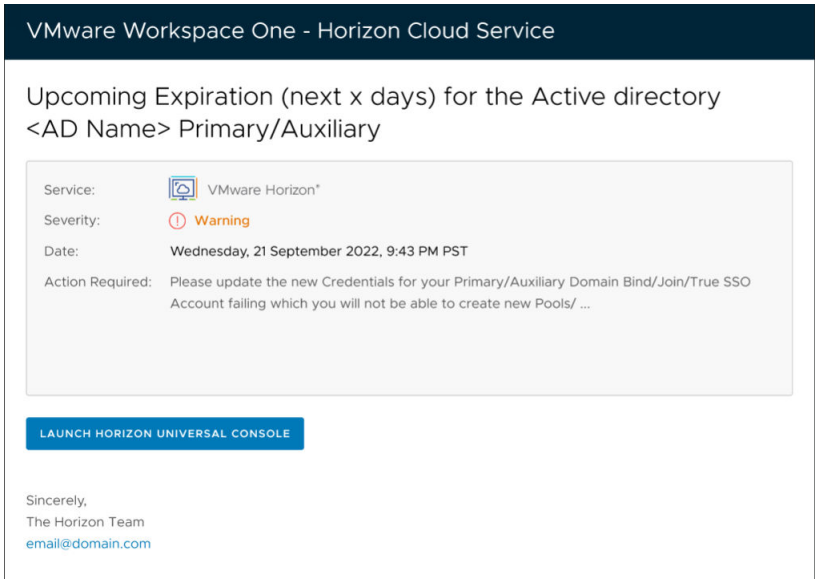
Expiration des informations d'identification du compte de domaine Active Directory : notifications

En plus d'une notification dans l'application de la console, le système envoie une notification par e-mail si les informations d'identification de compte de service répertoriées suivantes sont sur le point d'expirer ou ont déjà expiré.

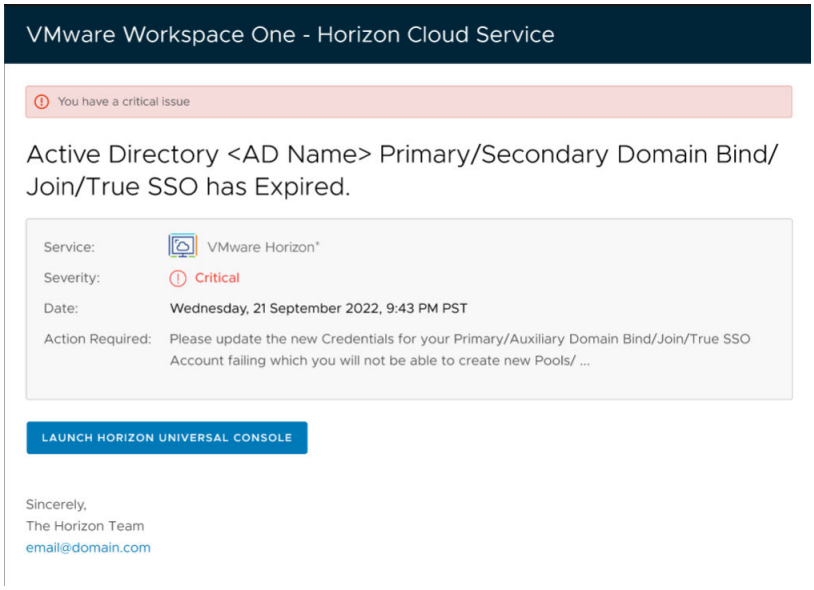
Ces e-mails vous indiquent que vous devez prendre les mesures nécessaires pour vous assurer que les opérations de votre environnement Horizon Cloud qui reposent sur les comptes de service peuvent se poursuivre sans interruption.

- Liaison de domaine
- Jonction de domaine
- Comptes du service d'inscription de True SSO : principaux et auxiliaires

La capture d'écran suivante illustre la notification par e-mail lorsque les informations d'identification d'un compte sont sur le point d'expirer.



La capture d'écran suivante illustre la notification par e-mail lorsque les informations d'identification d'un compte ont expiré.



Gestion des images Horizon à l'aide du Plan de contrôle Horizon de nouvelle génération

La gestion des images est essentielle à l'environnement Plan de contrôle Horizon de nouvelle génération. Cette page de documentation présente Horizon Image Management Service (IMS). Cette page décrit également certaines conditions requises propres à l'utilisation des fonctionnalités IMS dans votre environnement.

Brève introduction

IMS permet de créer, personnaliser et publier des versions d'images pour les droits d'accès à un poste de travail et à un serveur dans les déploiements d'Horizon Edge.

Les processus du service dépendent de l'administration rapide des images système. Celles-ci permettent de démarrer les machines virtuelles qui provisionnent des droits d'accès pour les utilisateurs finaux. Pour gérer les images système, chaque personnalisation d'image nécessite que l'administrateur ajoute et publie de nouvelles versions d'une image, et mette à jour les droits associés individuellement.

IMS simplifie et rationalise ce processus en offrant les fonctionnalités et avantages suivants dans vos déploiements d'Horizon Edge.

- Catalogues d'images centralisés, répertoriant les images avec leurs versions et copies sur les dispositifs Edge.
- Étapes guidées faciles à utiliser pour publier une image.
- Droits d'accès différents aux sites et dispositifs Edge connectés au cloud, qui peuvent facilement et régulièrement utiliser la même version de l'image gérée par le service d'image.
- Gestion simplifiée des versions de l'image pour contrôler et suivre les personnalisations.

Terminologie importante

Pour comprendre la gestion des images, vous devez connaître des termes tels que `image`, `version` et `copy`. De façon générale, une `image` classe par catégories le système d'exploitation et le modèle de machine virtuelle. Chaque `version` sous cette `image` est une `version` numérotée conçue pour différents ensembles de logiciels sur l'image et au format `major.minor.patch`. Une copie de chaque `image version` est une instance concrète de chaque dispositif Edge. Par exemple, une image nommée `Game` peut avoir une version `1.1.0` au format `major.minor.patch` et une copie d'image `Game 1.1.0` sur divers dispositifs Edge tels que `Edge-1`, `Edge-2`, `Edge-3`, etc.

Une fois qu'une version d'image et ses copies sont créées, elles sont traitées comme étant non modifiables. Si d'autres modifications sont nécessaires, elles doivent être effectuées sur les versions mineures ou majeures, si le contenu est différent de l'image source.

Déploiements de Microsoft Azure et IMS

Cette section décrit les conditions requises et les éléments à prendre en compte lors de l'utilisation d'IMS avec des déploiements d'Horizon Edge dans Microsoft Azure.

Tout d'abord, votre déploiement d'Horizon Edge dans Microsoft Azure doit respecter les informations de ces pages liées :

Microsoft Azure : configuration requise globale d'Horizon Edge

- Liste de vérification des conditions requises pour le déploiement d'un dispositif Microsoft Azure Edge
- Déploiements de Microsoft Azure Edge

Outre les détails sur les pages liées précédentes, pour que les opérations IMS fonctionnent et soient prises en charge avec vos déploiements, ces derniers doivent également respecter les conditions requises suivantes.

Si vos déploiements ne répondent toujours pas à ces conditions requises, des résultats inattendus peuvent se produire et les opérations de gestion d'images risquent d'échouer. L'opération de publication est particulièrement sensible à ces conditions requises.

Conditions requises du quota Microsoft Azure

Vos abonnements Microsoft Azure doivent disposer d'un quota suffisant pour les modèles de VM que vous prévoyez de sélectionner pour les opérations de gestion d'images. Pour connaître les types de modèles recommandés à utiliser pour la VM de base de l'image, reportez-vous à la section Image Management System Requirements de la liste de vérification des conditions requises.

Configuration requise du principal de service

Comme décrit dans la section Créer un principal de service pour l'abonnement Microsoft Azure, le service utilise des appels d'API pour utiliser des ressources dans vos abonnements Microsoft Azure. Pour que les opérations réussissent, tant que les principaux de service sont enregistrés pour être utilisés avec vos déploiements d'Horizon Edge dans Microsoft Azure, vous devez vérifier qu'elles :

- Continuent à répondre aux conditions requises décrites sur cette page.
- Ne sont pas expirées et n'atteignent pas leur date d'expiration.
- Demeurent dans le portail Azure et ne sont pas supprimées.

Limitations connues et problèmes connus propres à IMS

Limitations connues d'IMS

Les limitations connues du service sont décrites dans la section Limitations connues des Notes de mise à jour d'Horizon Cloud Service - next-gen. Recherchez la section Images à cet emplacement.

Par exemple, ces limitations peuvent inclure des scénarios et des cas d'utilisation qui ne sont actuellement pas pris en charge.

Problèmes connus d'IMS

Les problèmes connus du service sont décrits dans la section Problèmes connus des Notes de mise à jour d'Horizon Cloud Service - next-gen.

Ajouter une image dans Horizon Cloud Service - next-gen

Vous pouvez ajouter et gérer des images provenant de Microsoft Azure Marketplace et de la galerie de calcul Microsoft Azure, à l'aide d'Horizon Image Management Service.

Avant d'effectuer l'une des étapes suivantes, vérifiez également les informations clés dans Déploiements de Microsoft Azure et IMS.

Conditions préalables

- Décidez du modèle de VM à utiliser pour l'image. Pour connaître la configuration requise du modèle de VM, reportez-vous à la section Image Management System Requirements.
- Les dispositifs Unified Access Gateway et Passerelle Horizon Edge sont dans un état **Prêt**.
- Vérifiez que vos abonnements fournissent un quota de cœurs de CPU adéquat pour le modèle que vous prévoyez de sélectionner pour la VM de base. Pour connaître les types de modèles pris en charge, reportez-vous à la section Image Management System Requirements.
- Vérifiez que les sous-réseaux de locataire (poste de travail) autorisent un nombre suffisant d'adresses IP.
- Pour l'accès du protocole RDP (Remote Desktop Protocol) Microsoft pour la personnalisation de la VM de base, vérifiez que vous disposez d'un nombre requis d'adresses IP publiques provisionnées.
- Vérifiez que `softwareupdate.vmware.com` peut être résolu et est accessible depuis les sous-réseaux de gestion et de locataire (poste de travail) à l'aide du port `443` sur le protocole TCP pour télécharger les logiciels liés à l'agent utilisés dans les opérations de création d'images système. Pour plus d'informations, reportez-vous à la section Conditions requises pour les ports et les protocoles pour votre déploiement d'Horizon Cloud dans Microsoft Azure.
- Vérifiez qu'au moins un réseau virtuel et un sous-réseau de locataire (poste de travail) sont sélectionnés pour le fournisseur.
- Déterminez si le système d'exploitation invité de l'image que vous prévoyez d'ajouter est pris en charge.

  Pour la prise en charge des systèmes d'exploitation invités, reportez-vous à la section Matrice d'interopérabilité des produits. La recherche préconfigurée de la requête Matrice d'interopérabilité des produits VMware dans la matrice d'interopérabilité des produits répertorie les systèmes d'exploitation pris en charge par Horizon Cloud Service - next-gen.

Procédure

1. Sur la page **Accueil**, cliquez sur **Images** sur la vignette **Images** pour accéder à la page **Images**.
2. Sur la page **Images**, cliquez sur **Ajouter** pour accéder à la page **Ajouter une image**.

3 Dans la section **Informations générales**, ajoutez le **Nom de l'image** unique, puis cliquez sur **Suivant**.

   La version de l'image est automatiquement ajoutée au nom avec des tirets pour créer le nom de la copie de l'image (Image-1-0, Image-1-100).

4 Vous pouvez ajouter une **Description** de l'image.

5 Dans le champ **Marqueurs**, vous pouvez ajouter de nouveaux marqueurs. Donnez des noms uniques aux marqueurs. Les nouveaux marqueurs sont enregistrés lorsque l'image est enregistrée.

   Bien que les marqueurs soient facultatifs, vous ne pouvez pas utiliser une image pour la création de pools si aucun marqueur n'est associé.

6 Dans la section **Source de l'image**, sélectionnez une option de source.

Ajouter une image à partir de Microsoft Azure Marketplace

À l'aide d'Horizon Cloud Service next-gen, vous pouvez ajouter et gérer des images provenant de Microsoft Azure Marketplace.

Avant d'effectuer l'une des étapes suivantes, vérifiez également les informations clés dans Déploiements de Microsoft Azure et IMS.

Procédure

1 Sur la page **Accueil**, cliquez sur **Images** sur la vignette **Images** pour accéder à la page **Images**.

2 Sur la page **Images**, cliquez sur **Ajouter** pour accéder à la page **Ajouter une image**.

3 Dans **Informations générales**, ajoutez un **Nom d'image** unique, puis cliquez sur **Suivant**.

   La version de l'image est automatiquement ajoutée au nom avec des tirets pour créer le nom de la copie de l'image (Image-1-0, Image-1-100).

4 Vous pouvez ajouter une **Description** de l'image.

5 Dans le champ **Marqueurs**, vous pouvez ajouter de nouveaux marqueurs. Donnez des noms uniques aux marqueurs. Les nouveaux marqueurs sont enregistrés lorsque l'image est enregistrée.

6 Dans la section **Source de l'image**, sélectionnez **Microsoft Azure Marketplace**, puis cliquez sur **Suivant**.

7 Dans la sous-section **Destination**, sélectionnez **Site**, **Horizon Edge** et **Fournisseur**.

8 Dans la sous-section **Détails de la VM**, sélectionnez **SE**, **Type de génération Type de modèle de VM** et **Modèle de VM**.

9 Sélectionnez **Type de génération** entre **V1** et **V2**.

   Le système d'exploitation ne prend en charge qu'un **Type de génération** spécifique.

10 Le système d'exploitation ne prend en charge qu'un **Type de sécurité** spécifique. Une option **Type de sécurité** est automatiquement sélectionnée et désactivée entre **Standard** et **Lancement approuvé**.

   Si vous sélectionnez **V1**, seule l'option **Standard Type de sécurité** est activée. **Standard** fournit un niveau de sécurité de base aux machines virtuelles.

   Si vous sélectionnez **V2**, l'option **Lancement approuvé Type de sécurité** est activée par défaut. Le démarrage sécurisé est activé par défaut, ce qui fournit une protection contre les kits de démarrage, les rootkits et les logiciels malveillants au niveau du noyau. Le vTPM (Virtual Trusted Platform Module) est également activé par défaut, ce qui permet de stocker en toute sécurité les clés, les secrets et valide l'intégrité de démarrage des VM. L'option **Lancement approuvé** permet d'améliorer la sécurité et empêche les attaques avancées sur les machines virtuelles de génération 2.

   Vous pouvez également sélectionner **Standard Type de sécurité** pour **V2**.

11 Sélectionnez un **Type de modèle de VM** entre **Sans GPU** et **Avec GPU**.

12 Sélectionnez un **Modèle de VM** pris en charge parmi les options disponibles.

   Les options de **Modèle de VM** s'affichent en fonction du type de modèle de VM et du type de génération.

13 Dans la sous-section **Réseau**, vous pouvez activer **Adresse IP publique** en faisant glisser la bascule pour accéder à l'image via une connexion au protocole RDP (Remote Desktop Protocol), puis **Sélectionner un réseau**.

   Pour personnaliser et optimiser des images, vous avez besoin d'une VM créée à partir de l'image s'exécutant sur un réseau approprié pour vous connecter. Par conséquent, vous devez fournir un réseau virtuel, un sous-réseau et une adresse IP publique appropriés ayant un quota suffisant de ressources.

14 Dans la sous-section **Informations d'identification de l'administrateur de la VM**, ajoutez un **Nom d'utilisateur** et un **Mot de passe** pour que le compte d'administrateur local accède au système d'exploitation de l'image et l'utilise lors du processus de personnalisation de l'image.

15 Cochez la **case** correspondant à Licence Windows avec Software Assurance, puis cliquez sur **Ajouter**.

   L'ajout d'une image à partir de **Microsoft Azure Marketplace** la fait passer à un état Non publiée et prête à être personnalisée. L'image peut être utilisée par les pools uniquement après la publication.

Ajouter une image avec une VM Microsoft Azure personnalisée

Vous pouvez ajouter et gérer des images à partir d'une VM personnalisée facilement disponible à partir de Microsoft Azure Marketplace.

Avant d'effectuer l'une des étapes suivantes, vérifiez également les informations clés dans Déploiements de Microsoft Azure et IMS.

Conditions préalables

- La VM personnalisée créée dans Microsoft Azure doit être d'un type de modèle de VM de génération 1 ou 2.
- Pour le groupe de ressources dans lequel la VM personnalisée est créée, vous devez d'abord configurer le contrôle d'accès basé sur les rôles (RBAC).
- La région du fournisseur cible et la région dans laquelle réside la VM personnalisée doivent être identiques.

Note La VM personnalisée sélectionnée est convertie en image généralisée et ne peut pas être réutilisée comme VM lors du workflow de publication de l'image. Il est recommandé de conserver une sauvegarde de la VM.

Procédure

1. Sur la page **Accueil**, cliquez sur **Images** sur la vignette **Images** pour accéder à la page **Images**.
2. Sur la page **Images**, cliquez sur **Ajouter** pour accéder à la page **Ajouter une image**.
3. Dans **Informations générales**, ajoutez un **Nom d'image** unique, puis cliquez sur **Suivant**.

   La version de l'image est automatiquement ajoutée au nom avec des tirets pour créer le nom de la copie de l'image (Image-1-0, Image-1-100).
4. Vous pouvez ajouter une **Description** de l'image.
5. Dans le champ **Marqueurs**, vous pouvez ajouter de nouveaux marqueurs.

   Donnez des noms uniques aux marqueurs. Les nouveaux marqueurs sont enregistrés lorsque l'image est enregistrée.
6. Dans la section **Source de l'image**, sélectionnez **VM Microsoft Azure personnalisée**, puis cliquez sur **Suivant**.
7. Dans la sous-section **Destination**, sélectionnez **Site**, **Horizon Edge** et **Fournisseur**.
8. Dans **Détails de la VM**, sélectionnez une **VM**.

   Toutes les VM personnalisées doivent faire partie du **Groupe de ressources Azure** renseigné `vmw-hcs-<ProviderInstance_Id>-base-vms`. Vous pouvez obtenir le nom du groupe de ressources dans le portail Microsoft Azure sur la page Détails de la VM.

   Note Les pools ne peuvent être provisionnés qu'avec le type de génération de la VM sélectionnée.
9. Sélectionnez le type de **SE** de cette VM personnalisée.

   Sélectionnez le type de **SE** de **VM personnalisée** précisément, car vous ne pouvez pas le vérifier.

10 Dans la sous-section **Informations d'identification de l'administrateur de la VM**, ajoutez un **Nom d'utilisateur** et un **Mot de passe** pour que le compte d'administrateur local accède au système d'exploitation de l'image et l'utilise lors du processus de personnalisation de l'image.

   Le nom d'utilisateur ne peut pas dépasser 19 caractères et ne peut pas se terminer par un point (.). Les noms d'utilisateur interdits par Microsoft Azure, comme « invité » ou « administrateur », ne peuvent pas être utilisés.

   Les mots de passe doivent comporter entre 12 et 123 caractères et répondre à 3 des conditions requises suivantes : lettre minuscule [a-z], lettre majuscule [A-Z], chiffre et caractère spécial (!@#$%/^&*).

11 Cochez la **case** correspondant à Licence Windows avec Software Assurance, puis cliquez sur **Ajouter**.

Ajouter une image à partir de la galerie de calcul Microsoft Azure

Vous pouvez ajouter et gérer des images provenant de la galerie de calcul Microsoft Azure.

Conditions préalables

- Vous devez respecter les conditions préalables générales décrites dans la section Ajouter une image dans Horizon Cloud Service - next-gen.
- Avant d'effectuer la procédure d'ajout d'une image à partir de la galerie de calcul Microsoft Azure, assurez-vous que le système d'exploitation que vous prévoyez d'utiliser est pris en charge.

  Les conditions préalables générales font référence à la Matrice d'interopérabilité des produits VMware. Seules les images répertoriées dans la requête fournie sont prises en charge lorsque vous importez des images à partir de la galerie de calcul Microsoft Azure.

  Plus spécifiquement, utilisez la liste de référence des systèmes d'exploitation qui suit pour déterminer si la définition d'image est correctement définie.

Systèmes d'exploitation pris en charge lors de l'ajout d'une image à partir de la galerie de calcul Microsoft Azure

Les informations qui suivent incluent des détails de l'offre et de la SKU pour chaque système d'exploitation Microsoft Windows pris en charge par Horizon Cloud Service - next-gen. Les valeurs Offre et SKU répertoriées doivent être définies dans la définition d'image de votre galerie de calcul Microsoft Azure. Par exemple, pour utiliser le système d'exploitation Microsoft - Windows Server 2022 pour votre image, assurez-vous que la valeur Offre est `windowsserver` et la valeur SKU est `2022-datacenter`.

Système d'exploitation	Images de VM Azure Marketplace – Gen 1	Images de VM Azure Marketplace – Gen 2
Microsoft Windows Server 2022	Éditeur : microsoftwindowsserver Offre : windowsserver SKU : 2022-datacenter	Éditeur : microsoftwindowsserver Offre : windowsserver SKU : 2022-datacenter-g2
Microsoft - Windows Server 2019	Éditeur : microsoftwindowsserver Offre : windowsserver SKU : 2019-datacenter	Éditeur : microsoftwindowsserver Offre : windowsserver SKU : 2019-datacenter-gensecond
Microsoft - Windows Server 2016	Éditeur : microsoftwindowsserver Offre : windowsserver SKU : 2016-datacenter	Éditeur : microsoftwindowsserver Offre : windowsserver SKU : 2016-datacenter-gensecond
Microsoft - Windows 11 Enterprise multisession 23H2	Non pris en charge	Éditeur : microsoftwindowsdesktop Offre : windows-11 SKU : win11-23h2-avd
Microsoft - Windows 11 Enterprise 23H2	Non pris en charge	Éditeur : microsoftwindowsdesktop Offre : windows-11 SKU : win11-23h2-ent
Microsoft - Windows 11 Enterprise multisession 22H2	Non pris en charge	Éditeur : microsoftwindowsdesktop Offre : windows-11 SKU : win11-22h2-avd
Microsoft - Windows 11 Enterprise 22H2	Non pris en charge	Éditeur : microsoftwindowsdesktop Offre : windows-11 SKU : win11-22h2-ent
Microsoft - Windows 11 Enterprise multisession, 21H2	Non pris en charge	Éditeur : microsoftwindowsdesktop Offre : windows-11 SKU : win11-21h2-avd
Microsoft - Windows 11 21H2 Enterprise	Non pris en charge	Éditeur : microsoftwindowsdesktop Offre : windows-11 SKU : win11-21h2-ent
Microsoft - Windows 10 Enterprise multisession, 22H2	Éditeur : microsoftwindowsdesktop Offre : windows-10 SKU : win10-22h2-avd	Éditeur : microsoftwindowsdesktop Offre : windows-10 SKU : win10-22h2-avd-g2
Microsoft - Windows 10 Enterprise 22H2	Éditeur : microsoftwindowsdesktop Offre : windows-10 SKU : win10-22h2-ent	Éditeur : microsoftwindowsdesktop Offre : windows-10 SKU : win10-22h2-ent-g2
Microsoft - Windows 10 Enterprise multisession, 21H2	Éditeur : microsoftwindowsdesktop Offre : windows-10 SKU : win10-21h2-avd	Éditeur : microsoftwindowsdesktop Offre : windows-10 SKU : win10-21h2-avd-g2
Microsoft - Windows 10 Enterprise, 21H2	Éditeur : microsoftwindowsdesktop Offre : windows-10 SKU : win10-21h2-ent	Éditeur : microsoftwindowsdesktop Offre : windows-10 SKU : win10-21h2-ent-g2

Système d'exploitation	Images de VM Azure Marketplace – Gen 1	Images de VM Azure Marketplace – Gen 2
Microsoft - Windows 10 Pro, 21H2	Éditeur : microsoftwindowsdesktop Offre : windows-10 SKU : win10-21h2-pro	Éditeur : microsoftwindowsdesktop Offre : windows-10 SKU : win10-21h2-pro-g2
Microsoft - Windows 10 Enterprise multisession, 20H2	Éditeur : microsoftwindowsdesktop Offre : windows-10 SKU : 20h2-evd	Éditeur : microsoftwindowsdesktop Offre : windows-10 SKU : 20h2-evd-g2
Microsoft - Windows 10 Enterprise, 20H2	Éditeur : microsoftwindowsdesktop Offre : windows-10 SKU : 20h2-ent	Éditeur : microsoftwindowsdesktop Offre : windows-10 SKU : 20h2-ent-g2

Étapes de l'ajout d'une image à partir de la galerie de calcul Microsoft Azure

Utilisez Horizon Image Management Service pour ajouter une image personnalisée avec un système d'exploitation pris en charge à partir de la galerie de calcul Microsoft Azure.

Avant d'effectuer l'une des étapes suivantes, vérifiez également les informations clés dans Déploiements de Microsoft Azure et IMS.

Conditions préalables

Cliquez ou faites défiler l'écran vers le haut si nécessaire pour afficher les conditions préalables répertoriées au début de la section Ajouter une image à partir de la galerie de calcul Microsoft Azure. Assurez-vous que ces conditions préalables sont remplies.

Procédure

1. Sur la page **Accueil**, cliquez sur **Images** sur la vignette **Images** pour accéder à la page **Images**.
2. Sur la page **Images**, cliquez sur **Ajouter** pour accéder à la page **Ajouter une image**.
3. Dans **Informations générales**, ajoutez un **Nom d'image** unique, puis cliquez sur **Suivant**.

   La version de l'image est automatiquement ajoutée au nom avec des tirets pour créer le nom de la copie de l'image (Image-1-0, Image-1-100).
4. Vous pouvez ajouter une **Description** de l'image.
5. Dans le champ **Marqueurs**, vous pouvez ajouter de nouveaux marqueurs. Donnez des noms uniques aux marqueurs. Les nouveaux marqueurs sont enregistrés lorsque l'image est enregistrée.
6. Dans la section **Source de l'image**, sélectionnez **Galerie de calcul Microsoft Azure**, puis cliquez sur **Suivant**.
7. Dans la sous-section **Destination**, sélectionnez **Site** et **Horizon Edge**.

8 Dans la sous-section **Détails de la version de l'image source**, ajoutez l'**ID de locataire Microsoft Entra ID** à partir du portail Microsoft Azure. Ajoutez l'**ID de ressource** obtenu à partir du portail Microsoft Azure en cliquant sur le lien Vue JSON situé sur la version de l'image de la définition de l'image. Si l'image a été publiée à l'aide d'Horizon Universal Console, cet ID peut être obtenu dans la console à partir de la colonne Chemin d'emplacement de la grille Copies d'images sur la page Détails de la version de l'image.

   Assurez-vous que le fournisseur du dispositif Horizon Edge de destination sélectionné dispose d'un accès en lecture Microsoft Azure RBAC à l'image source ou au groupe de ressources contenant l'image. Assurez-vous également que l'image source est déjà publiée avec Horizon Agent.

9 Sélectionnez **Copier à partir de la source de l'image** pour **Attributs de l'image** pour utiliser les attributs de la version de l'image source.

   Si vous êtes pris en charge par un `VMware Managed Services Provider` (MSP), vous pouvez copier l'image du fournisseur d'organisation MSP vers votre fournisseur. Ce processus exploite une image source publiée dans le catalogue Horizon correspondant à une organisation externe (MSP) autre que la vôtre. Le MSP fournit une image complète incluant les détails de l'application résidant dans le serveur ou l'image multisession.

   Lorsque vous sélectionnez l'option **Copier à partir de la source de l'image**, spécifiez l'**ID d'organisation** qui a partagé ou publié initialement l'image.

   L'option **Remplacer** permet de configurer les attributs. L'option Remplacer s'applique lorsque vous souhaitez copier une image source qui ne se trouve pas dans votre catalogue Horizon. Par exemple, une image d'un abonnement externe lisible par l'abonnement du fournisseur Horizon.

   Lorsque vous importez une image externe, assurez-vous que la dernière version d'Horizon Agent est installée sur l'image source ou que les VM créées dans le cadre de pools de postes de travail/serveurs sur cette image peuvent rencontrer une erreur.

   L'image source est une image déjà publiée qui est généralisée avec l'agent et le logiciel nécessaires. Par conséquent, une copie de la même image dans l'organisation du client peut être utilisée directement par les pools. Elle peut également être republiée dans d'autres abonnements ou régions. Votre fournisseur doit disposer d'un accès RBAC approprié à l'image source.

   Lorsque vous sélectionnez **Remplacer**, spécifiez le **SE** de l'image source. Si le SE ne prend pas en charge un type de génération spécifique, un type de génération pris en charge est sélectionné par défaut.

10 Si vous pouvez le sélectionner, choisissez une option **Type de génération**.

   Note Les VM Microsoft Azure de génération 1 et 2 sont prises en charge. Si vous sélectionnez **V1**, les pools ne peuvent être provisionnés qu'avec des modèles de génération V1.

11 Dans la sous-section **Détails de la VM**, sélectionnez **Type de modèle de VM** et **Modèle de VM**.

Note Vos sélections pour le **Type de génération** et le **Type de modèle de VM** servent de filtre et déterminent quels modèles de VM sont disponibles dans le menu déroulant **Modèle de VM**.

12 Dans la sous-section **Informations d'identification de l'administrateur de la VM**, ajoutez un **Nom d'utilisateur** et un **Mot de passe** pour que le compte d'administrateur local accède au système d'exploitation de l'image et l'utilise lors du processus de conversion de l'image.

13 Cochez la **case** correspondant à Licence Windows avec Software Assurance, puis cliquez sur **Ajouter**.

Ajouter une version à une image de la galerie de calcul Microsoft Azure existante

Vous pouvez ajouter de nouvelles versions à vos images de la galerie de calcul Microsoft Azure existantes, sans avoir à cloner une version. Seul un type similaire d'image peut être ajouté comme version de l'image existante.

Procédure

1 Cliquez sur la vignette **Images** sur la page Horizon Universal Console **Accueil**.

2 Sur la page **Images**, cliquez sur le **Nom de l'image** qui a été ajouté à partir de la **Galerie de calcul Microsoft Azure** pour accéder à la page **Image**.

3 Cliquez sur **Ajouter** pour accéder à la page **Ajouter une version de l'image**.

4 Dans la section **Source**, cliquez sur **Suivant** après **Galerie de calcul Microsoft Azure**.

5 Dans la section **Détails de la source**, sélectionnez les options **Site**, **Horizon Edge** et **Fournisseur** dans la sous-section **Destination**.

6 Dans la sous-section **Détails de la version de l'image source**, ajoutez l'**ID de locataire Microsoft Entra ID** à partir du portail Microsoft Azure. Ajoutez l'**ID de ressource** obtenu à partir des propriétés Active Directory du portail Microsoft Azure en cliquant sur le lien Vue JSON situé sur la version de l'image de la définition de l'image. Si l'image a été publiée à l'aide d'Horizon Universal Console, cet ID peut être obtenu dans la console à partir de la colonne **Chemin d'emplacement** de la grille **Copies d'images** sur la page **Détails de la version de l'image**.

   Assurez-vous que le fournisseur principal de l'instance d'**Horizon Edge** de destination sélectionnée dispose d'un accès en lecture Microsoft Azure RBAC à l'image source ou au groupe de ressources contenant l'image. Assurez-vous également que l'image source est déjà publiée avec Horizon Agent.

7 Dans Attributs de l'image, sélectionnez **Copier à partir de l'image source** et **Remplacer**.

a Si vous sélectionnez **Copier à partir de la source de l'image**, ajoutez l'**ID d'organisation** du compte qui a publié l'image à l'aide d'Horizon Universal Console. Vous pouvez obtenir cet ID dans les paramètres de l'utilisateur/de l'organisation de ce compte. Pour l'option **Copier à partir de la source de l'image**, les attributs de la version de l'image source sont utilisés

Les options **Nom du SE**, **Type de système d'exploitation** et **Type de session** sont copiées automatiquement à partir de l'image source.

Si vous êtes pris en charge par un `VMware Managed Services Provider` (MSP), vous pouvez copier l'image du fournisseur d'organisation MSP vers votre fournisseur. Ce processus exploite une image source publiée dans le catalogue Horizon correspondant à une organisation externe (MSP) autre que la vôtre. Le MSP fournit une image complète incluant les détails de l'application résidant dans le serveur ou l'image multisession.

L'option **Copier à partir de la source de l'image** s'applique lorsque vous souhaitez ajouter une version à l'aide de la version existante de l'image Horizon disponible dans le catalogue de l'organisation MSP.

b Si vous sélectionnez Remplacer, vous devez sélectionner les options **SE**, **Type de système d'exploitation** et **Type de session**.

L'option **Remplacer** s'applique lorsque vous souhaitez copier une image source qui ne se trouve pas dans votre catalogue Horizon. Par exemple, une image d'un abonnement externe lisible par l'abonnement du fournisseur Horizon.

Lorsque vous ajoutez une image externe, assurez-vous que la dernière version d'Horizon Agent est installée sur l'image source, sinon les VM créées dans le cadre de pools de postes de travail/serveurs sur cette image risquent de rencontrer une erreur.

Assurez-vous que l'éditeur, l'offre et la SKU de l'image Microsoft Azure Marketplace utilisée pour la création de l'image source sont configurés dans la définition de l'image sous la galerie de calcul Azure source. Les valeurs d'éditeur, d'offre et de SKU doivent correspondre à la liste existante d'images prises en charge répertoriées lors de l'importation d'une nouvelle image Azure Marketplace.

L'image source est une image déjà publiée qui est généralisée avec l'agent et le logiciel nécessaires. Par conséquent, une copie de la même image dans l'organisation du client peut être utilisée directement par les pools. Elle peut également être republiée dans d'autres abonnements ou régions. Votre fournisseur doit disposer d'un accès RBAC approprié à l'image source.

8 Dans la sous-section **Détails de la VM**, sélectionnez **Type de modèle de VM** et **Modèle de VM**.

Note Dans la liste de **Modèles de VM**, seuls les modèles de VM ayant le même type de génération que l'image sont répertoriés.

9 Dans la sous-section **Informations d'identification de l'administrateur de la VM**, ajoutez un **Nom d'utilisateur** et un **Mot de passe** pour que le compte d'administrateur local accède au système d'exploitation de l'image et l'utilise lors du processus de conversion de l'image.

10 Cochez la **case** correspondant à **Licence Windows avec Software Assurance**.

11 Dans la section **Version cible**, sélectionnez le **Type de version, Majeure** ou **Mineure**.

   a Si vous sélectionnez **Majeure**, le **Numéro de version attendu** est renseigné automatiquement, en fonction de votre sélection et des versions préexistantes de l'image.

   b Si vous sélectionnez **Mineure**, ajoutez le numéro de version majeure dans **Ajouter une version sous**, au-dessous duquel vous souhaitez ajouter la version **Mineure** pour renseigner automatiquement le **Numéro de version attendu**.

12 Dans le champ **Marqueurs**, vous pouvez ajouter de nouveaux marqueurs. Donnez des noms uniques aux marqueurs. Les nouveaux marqueurs sont enregistrés lorsque l'image est enregistrée.

Ajouter une version à une image existante avec une VM personnalisée Microsoft Azure

Vous pouvez ajouter de nouvelles versions à vos images de la galerie de calcul Microsoft Azure existantes, sans avoir à cloner une version. Seul un type similaire d'image peut être ajouté comme version de l'image existante.

Procédure

1 Cliquez sur la vignette **Images** sur la page Horizon Universal Console **Accueil**.

2 Sur la page **Images**, cliquez sur un **Nom d'image** pour accéder à la page **Image**.

3 Cliquez sur **Ajouter** pour accéder à la page **Ajouter une version de l'image**.

4 Dans la section **Source**, cliquez sur **Suivant** après **VM Microsoft Azure personnalisée**.

5 Dans la section **Détails de la source**, sélectionnez les options **Site**, **Horizon Edge** et **Fournisseur** dans la sous-section **Destination**.

6 Dans **Informations générales**, ajoutez un **Nom d'image** unique, puis cliquez sur **Suivant**.

   La version de l'image est automatiquement ajoutée au nom avec des tirets pour créer le nom de la copie de l'image (Image-1-0, Image-1-100).

7 Vous pouvez ajouter une **Description** de l'image.

8 Dans le champ **Marqueurs**, vous pouvez ajouter de nouveaux marqueurs.

   Donnez des noms uniques aux marqueurs. Les nouveaux marqueurs sont enregistrés lorsque l'image est enregistrée.

9 Dans la section **Source de l'image**, sélectionnez **VM Microsoft Azure personnalisée**, puis cliquez sur **Suivant**.

10 Dans la sous-section **Destination**, sélectionnez **Site**, **Horizon Edge** et **Fournisseur**.

11 Dans **Détails de la VM**, sélectionnez une **VM**.

Toutes les VM personnalisées doivent faire partie du **Groupe de ressources Azure** renseigné `vmw-hcs-<ProviderInstance_Id>-base-vms`. Vous pouvez obtenir le nom du groupe de ressources dans le portail Microsoft Azure sur la page Détails de la VM.

Note Dans la liste **Sélectionner une VM**, seules les VM personnalisées ayant le même type de génération que l'image sont répertoriées.

12 Sélectionnez le type de **SE** de cette VM personnalisée.

Sélectionnez le type de **SE** de **VM personnalisée** précisément, car vous ne pouvez pas le vérifier. Lorsque vous importez une image externe, assurez-vous que la dernière version d'Horizon Agent est installée sur l'image source ou que les VM créées dans le cadre de pools de postes de travail/serveurs sur cette image peuvent rencontrer une erreur.

13 Dans la sous-section **Informations d'identification de l'administrateur de la VM**, ajoutez un **Nom d'utilisateur** et un **Mot de passe** pour que le compte d'administrateur local accède au système d'exploitation de l'image et l'utilise lors du processus de personnalisation de l'image.

Le nom d'utilisateur ne peut pas dépasser 19 caractères et ne peut pas se terminer par un point (.). Les noms d'utilisateur interdits par Microsoft Azure, comme « invité » ou « administrateur », ne peuvent pas être utilisés.

Les mots de passe doivent comporter entre 12 et 123 caractères et répondre à 3 des conditions requises suivantes : lettre minuscule [a-z], lettre majuscule [A-Z], chiffre et caractère spécial (!@#$%/^&*). Mots de passe interdits par Microsoft Azure, tels que « Password1 ».

14 Cochez la **case** correspondant à **Licence Windows avec Software Assurance**.

15 Dans la section **Version cible**, sélectionnez le **Type de version, Majeure** ou **Mineure**.

a Si vous sélectionnez **Majeure**, le **Numéro de version attendu** est renseigné automatiquement, en fonction de votre sélection et des versions préexistantes de l'image.

b Si vous sélectionnez **Mineure**, ajoutez le numéro de version majeure dans **Ajouter une version sous**, au-dessous duquel vous souhaitez ajouter la version **Mineure** pour renseigner automatiquement le **Numéro de version attendu**.

16 Dans le champ **Marqueurs**, vous pouvez ajouter de nouveaux marqueurs. Donnez des noms uniques aux marqueurs. Les nouveaux marqueurs sont enregistrés lorsque l'image est enregistrée.

Supprimer une image

Vous pouvez supprimer une image, si nécessaire, pendant votre processus de gestion des images.

Conditions préalables

- Unified Access Gateway et la passerelle Edge Gateway sont prêtes.

- L'état de l'image est Disponible, Importée ou En échec.

Procédure

1. Connectez-vous à Horizon Universal Console.
2. Accédez à **Ressources > Images** pour afficher une liste d'images.
3. Cliquez sur le lien du nom de l'image à supprimer.
4. Sélectionnez la version à supprimer.
5. Cliquez sur **Supprimer**.
6. Dans **Supprimer la version de l'image**, cliquez sur **Supprimer** pour démarrer le processus de suppression.

   Cette action supprimera la version de l'image de tous les sites associés. S'il s'agit de la seule version de cette image, l'image parente associée sera également supprimée.

Cloner une image

Lorsque des modifications importantes sont apportées à l'image parente, clonez une version de l'image pour créer une image à partir d'une version de l'image publiée existante.

Avant d'effectuer l'une des étapes suivantes, vérifiez également les informations clés dans Déploiements de Microsoft Azure et IMS.

Avec ces étapes, créez une version de l'image avec une version incrémentée à partir de versions majeures ou mineures disponibles ou partiellement disponibles.

Conditions préalables

- L'image est importée et publiée.
- L'image sélectionnée est disponible ou partiellement disponible.
- Au moins un réseau virtuel et un sous-réseau de locataire (poste de travail) sont sélectionnés pour le fournisseur.

Procédure

1. Sur la page **Accueil** d'Horizon Universal Console, cliquez sur **Images**.
2. Sur la page **Images**, cliquez sur un lien d'image pour copier la version de l'image.
3. Sélectionnez une image et cliquez sur **Copier > Copier en tant qu'image**.
4. Dans la section **Informations générales**, ajoutez le **Nom de l'image**, puis cliquez sur **Suivant**.
5. Dans **Réseau**, sélectionnez le réseau à utiliser pour la nouvelle VM de l'image copiée, puis cliquez sur **Enregistrer**.

Cloner une version de l'image

Le clonage d'une version de l'image dans Horizon Cloud Service - next-gen crée une version incrémentée de l'image que vous pouvez ensuite publier comme version standard. Lorsque vous

avez publié ces images clonées sur vos cibles choisies, vous pouvez utiliser ces clones publiés pour créer des groupes de pools.

Avant d'effectuer l'une des étapes suivantes, vérifiez également les informations clés dans Déploiements de Microsoft Azure et IMS.

Conditions préalables

- L'image est importée et publiée.
- La version sélectionnée est disponible ou partiellement disponible.
- Au moins un réseau virtuel et un sous-réseau de locataire (poste de travail) sont sélectionnés pour le fournisseur.

Procédure

1. Sur la page **Accueil** d'Horizon Universal Console, cliquez sur **Images**.
2. Sur la page **Images**, cliquez sur un lien d'image pour répertorier les versions de l'image.
3. Sélectionnez une image et cliquez sur **Publiée > Copier en tant que version de l'image**.
4. Dans la section **Informations générales**, sélectionnez l'une des options suivantes et cliquez sur **Suivant**.
   - Sélectionnez **Majeure** pour mettre à niveau l'image, par exemple, pour un autre logiciel. Cela augmente la majeure partie du numéro de version.
   - Sélectionnez **Mineure** pour mettre à niveau l'image de manière incrémentielle, par exemple pour les mises à niveau de correctifs ou de logiciels existants. Cela incrémente la partie mineure du numéro de la version.

     Vous pouvez disposer de quatre-vingt-dix-neuf (99) versions au maximum d'une image de mise à niveau majeure ou mineure. Vous pouvez créer 99 versions majeures au total. 99 versions mineures au total peuvent être créées avec n'importe quelle version majeure.
5. Dans le panneau **Réseau**, sélectionnez le réseau à utiliser pour la nouvelle VM de la version de l'image copiée, puis cliquez sur **Enregistrer**.

Modifier une version de l'image

Vous pouvez modifier les marqueurs d'une version de l'image dont l'état est Partiellement disponible ou Disponible.

Conditions préalables

- L'image est importée et publiée.
- L'état de la version sélectionnée est Partiellement disponible ou Disponible.

Procédure

1. Connectez-vous à Horizon Universal Console.

2 Sur la page d'accueil, cliquez sur **Images** dans la vignette **Images**.

3 Sur la page **Images**, cliquez sur le lien d'une image à l'état **Disponible** pour répertorier les versions de l'image.

4 Sur la page des versions de l'image, sélectionnez une version de l'image, puis cliquez sur **Modifier**.

5 Sur la page Modifier la version, ajoutez ou modifiez **Description** et ajoutez ou supprimez des **Marqueurs** existants, ou ajoutez de nouveaux **Marqueurs**.

   Si vous ajoutez des marqueurs existants d'une version à la version modifiée actuelle, tous les pools associés au marqueur sont mis à jour vers la version actuelle. Vous ne pouvez pas supprimer les Marqueurs associés aux Pools. Si un marqueur associé à un agent de version antérieure est sélectionné, un message d'avertissement s'affiche. Il est recommandé de sélectionner un marqueur avec la dernière version de l'agent.

6 Cliquez sur **Enregistrer**.

Publication d'une image

Après avoir ajouté une image et vérifié ses détails, vous pouvez la publier à partir d'Horizon Cloud Service - next-gen.

Avant d'effectuer l'une des étapes suivantes, vérifiez également les informations clés dans Déploiements de Microsoft Azure et IMS.

Conditions préalables

Vérifiez que les tâches suivantes sont terminées avant de poursuivre :

- L'enregistrement de domaine est terminé.
- Microsoft Entra ID est connecté à VMware Cloud.
- Le site a été créé.
- Unified Access Gateway et la passerelle Edge sont prêts.
- Les informations sur l'image sont vérifiées et l'état de l'image est Non publiée.
- `softwareupdate.vmware.com` peut être résolu et accessible depuis les sous-réseaux de gestion et de locataire (poste de travail) à l'aide du port `443` sur le protocole TCP pour télécharger les logiciels liés à l'agent utilisés dans les opérations de création d'images système. Il doit être accessible directement ou via un proxy Edge (si celui-ci est défini). Le proxy proprement dit doit être accessible à la VM d'image dans les sous-réseaux de locataire (poste de travail). Le service d'image utilise le proxy configuré au niveau du dispositif Edge. Pour plus d'informations, reportez-vous à la section Conditions requises pour les ports et les protocoles pour votre déploiement d'Horizon Cloud dans Microsoft Azure.
- Si ce modèle de VM de type GPU est sélectionné, vérifiez que les pilotes de GPU NVIDIA sont installés sur la VM. Pour plus d'informations, reportez-vous à la section Installer les pilotes GPU NVIDIA sur les VM série N exécutant Windows.

- Au moins un réseau virtuel et un sous-réseau de locataire (poste de travail) sont sélectionnés pour le fournisseur.
- Le cas échéant, installez manuellement Horizon Agent dans l'image.

  Horizon Cloud Service - next-gen installe automatiquement Horizon Agent pendant le workflow de publication. Toutefois, si l'installation de l'agent avant le workflow de publication est nécessaire pour votre cas d'utilisation spécifique, reportez-vous à l'article 91998 de la base de connaissances. Si vous installez manuellement Horizon Agent, lorsque vous effectuez la procédure suivante, désélectionnez la bascule **Installer Horizon Agent**.
- Assurez-vous que Microsoft Azure Custom Script Extensions (CSE), Azure RunCommand et Sysprep ne sont pas bloqués ou interrompus par des stratégies, des pare-feu ou des solutions externes sur la VM d'image dans Microsoft Azure. Pendant le processus de publication des images Azure, Azure Custom Script Extension et Azure RunCommand sont utilisés et l'image est généralisée à l'aide de Sysprep avant la capture dans Azure Compute Gallery.

  Si vous configurez un proxy dans la VM d'image, l'URL `https://softwareupdate.vmware.com/` doit être sur liste autorisée afin que l'URL soit contournée par le proxy.

  Horizon Cloud Service - next-gen nécessite que CSE installe Horizon Agent. Par conséquent, si vous utilisez la stratégie Azure pour limiter l'installation d'extensions sur une VM d'image, qui est une VM utilisée pour la préparation d'image, procédez de l'une des manières suivantes lors de la phase de stratégie d'attribution de la configuration afin d'éviter l'échec du processus de publication.

  - Assurez-vous que les stratégies de sécurité Microsoft Azure associées aux extensions de script personnalisé autorisent l'exécution et l'exécution des extensions de script personnalisé sur la machine virtuelle d'image.

    Note Lorsque vous attribuez une stratégie, vous pouvez sélectionner des exclusions qui sont des ressources à exclure de l'attribution de stratégie. Si vous utilisez cette méthode, sélectionnez les ressources liées à l'image à exclure de la stratégie.
  - Autorisez l'exécution d'une extension de script personnalisé nommée **`vmw-hcs-image-CustomScriptExtension`**. Pendant le processus de publication, Horizon Cloud Service - next-gen utilise le nom **`vmw-hcs-image-CustomScriptExtension`** pour l'extension de script personnalisé attaché à la VM d'image.

Procédure

1. Sur la page **Accueil** d'Horizon Universal Console, cliquez sur la vignette **Images** pour accéder à la page **Images**. Cliquez sur une image qui est dans l'état **Prêt à publier**.
2. Sur la page de détails de l'image, sélectionnez la **Version** de l'image, puis cliquez sur le menu déroulant **Non publiée > Publier**.

3 Dans la section **Destination**, sélectionnez le **Dispositif Horizon Edge source** dans lequel la version de l'image a été importée, est présélectionnée et ne peut pas être désélectionnée.

Note L'image sera toujours publiée sur le dispositif Horizon Edge source.

Pour publier l'**image** sur d'autre dispositifs Dispositifs Horizon Edge, cochez les cases dans le tableau. Cliquez sur **Suivant**.

4 Dans la section **Propriétés**, vous pouvez faire glisser l'option pour sélectionner **Désactiver les mises à jour Windows automatiques**.

Cela désactive les fonctionnalités de poste de travail physique pour améliorer les performances et l'utilisation de la capacité des VM, et permet d'éviter les problèmes Sysprep de Microsoft Windows.

5 Vous pouvez faire glisser la bascule pour **supprimer des applications du Windows Store**, également appelées modules AppX, et désactiver les mises à jour automatiques et les téléchargements d'applications et du Windows Store. Cela améliore les performances et permet d'éviter les problèmes Sysprep de Microsoft Windows.

Les applications Windows Store suivantes sont conservées et ne seront pas supprimées lors du processus de publication :

```
Microsoft.DesktopAppInstaller
Microsoft.Messaging
Microsoft.MSPaint
Microsoft.Windows.Photos
Microsoft.MicrosoftStickyNotes
Microsoft.WindowsCalculator
Microsoft.WindowsCommunicationsApps
Microsoft.WindowsSoundRecorder
Microsoft.WindowsStore
Microsoft.WindowsNotepad
Microsoft.ScreenSketch
Microsoft.Xbox.TCUI
Microsoft.XboxApp
Microsoft.XboxGameCallableUI
Microsoft.XboxGameOverlay
Microsoft.XboxGamingOverlay
Microsoft.XboxIdentityProvider
Microsoft.XboxSpeechToTextOverlay
MSTeams
Windows.CBSPreview
windows.immersivecontrolpanel
Windows.PrintDialog
```

6 Vous pouvez faire glisser la bascule vers l'option **Activer la récupération de l'erreur de publication** pour créer une VM de sauvegarde pour la récupération de l'image si une erreur irrécupérable se produit pendant le processus de publication. Cliquez sur **Suivant**.

7 Si vos agents préférés sont déjà installés sur l'image, désélectionnez l'option **Installer Horizon Agent**.

Important L'option **Installer Horizon Agent** est activée par défaut, car les agents ne sont généralement pas déjà installés sur une image et l'opération de publication installe les agents. Cependant, si vos agents préférés sont déjà installés sur l'image, veillez à désactiver cette bascule. Lorsque cette bascule est activée et que vous cliquez sur **Publier**, le système exécute le processus d'installation de l'agent sur l'image dans le cadre de la publication de l'image. Lorsque des agents sont déjà installés sur l'image et que vous avez activé cette bascule, puis que vous cliquez sur **Publier**, des conflits d'opérations peuvent se produire, car le système exécute le processus d'installation de l'agent sur une image sur laquelle les agents sont déjà installés.

8 Effectuez des sélections pour **Fonctionnalités d'Horizon Agent** et cliquez sur **Suivant**.

9 Dans la section **Opérations de l'image publiée**, vous pouvez faire glisser la bascule vers **Analyser les applications distantes**, applicable uniquement aux images multisession (Azure Virtual Desktop ou RDSH). En outre, vous pouvez faire glisser la bascule vers **Valider l'image publiée**, afin de valider l'image publiée pour vérifier qu'aucune erreur ne se produit lorsque l'image est utilisée pour provisionner les pools, lorsqu'un pool généré par le système est utilisé pour valider l'image.

Si vous faites glisser la bascule vers l'option **Valider l'image publiée**, la durée du processus de publication risque d'augmenter.

10 Si vous activez l'option **Analyser les applications distantes** ou l'option **Valider l'image publiée**, sélectionnez un **Réseau virtuel** de destination qui sera associé au pool généré par le système créé à partir de l'image. Sélectionnez le même réseau virtuel de locataire que vous prévoyez d'utiliser pour la création des pools à l'avenir.

11 **Sélectionnez un réseau** pour les opérations de l'image publiée. Cliquez sur **Publier**.

Vérification des détails de l'image avant la publication

Avant de publier des images, vérifiez que les informations de l'image sont exactes.

Conditions préalables

Pour vous assurer que les images sont visibles via différents abonnements, vous devez d'abord configurer le contrôle d'accès basé sur les rôles (RBAC). Pour plus d'informations, reportez-vous à la section Pour utiliser un rôle personnalisé pour l'enregistrement d'applications Horizon Cloud.

Procédure

1 Connectez-vous à Horizon Cloud Service.

2 Accédez à **Ressources > Images** pour afficher une liste d'images.

3 Cliquez sur le lien du nom de l'image pour afficher le tableau **Versions** qui répertorie les versions et l'état de l'image.

4 Vérifiez les détails de l'image.

   a Cliquez sur le lien de la version de l'image à vérifier.

   b Vérifiez les informations des options **Propriétés**, **Copies d'images**, **Pools**, **Pools d'analyses des applications** et **Applications distantes**.

Publication d'une image en échec avec des erreurs irrécupérables

Si une image échoue avec des erreurs irrécupérables, telles que des erreurs de validation de l'image ou Sysprep, vous pouvez la republier depuis le début.

Procédure

1 Se connecter à VMware Horizon® Cloud Service™ - next-gen

2 Sur la page **Accueil** d'Horizon Universal Console, cliquez sur **Images**.

3 Sur la page **Images**, cliquez sur le lien de l'image **En échec** pour accéder à la page des versions de l'image.

4 Sur cette page, sélectionnez l'image et cliquez sur **Erreur > Publier** pour republier l'image depuis le début.

   La publication à partir de zéro n'est possible que lorsque les options **Activer la récupération de l'erreur de publication** et **Valider l'image publiée** sont activées pendant Publication d'une image.

Valider une image publiée

Vous pouvez valider une image publiée pendant votre processus de gestion d'images.

Conditions préalables

- La passerelle Edge Gateway est prête.
- L'image a été publiée.
- Au moins un réseau virtuel et un sous-réseau de locataire (poste de travail) sont sélectionnés pour le fournisseur.

Procédure

1 Sur la page **Accueil** d'Horizon Universal Console, cliquez sur **Images**.

2 Sur la page **Images**, cliquez sur le lien de l'image pour accéder à la page des versions de l'image.

3 Sélectionnez une version de l'image à valider et cliquez sur **Publiée > Valider**.

4 Sélectionnez un réseau à utiliser pour la validation de l'image.

5 Cliquez sur **Enregistrer** pour déclencher la validation.

Échec de la revalidation d'une image lors de la validation

Vous pouvez revalider une image qui a précédemment échoué lors de la validation dans votre processus de gestion d'images.

Conditions préalables

- La passerelle Edge Gateway est prête.
- L'image a été publiée.
- Au moins un réseau virtuel et un sous-réseau de locataire (poste de travail) sont sélectionnés pour le fournisseur.

Procédure

1. Sur la page **Accueil** d'Horizon Universal Console, cliquez sur **Images**.
2. Sur la page **Images**, cliquez sur le lien de l'image **En échec** pour accéder à la page des versions de l'image.
3. Sélectionnez le nom de la version de l'image à valider et cliquez sur **Publiée > Valider**.
4. **Sélectionnez un réseau** à utiliser pour la validation de l'image. Cliquez sur **Enregistrer**.

Republication des versions de l'image

Vous pouvez retenter la publication de version de l'image ayant échoué ou développer les emplacements d'une version de l'image vers des instances de fournisseur supplémentaires.

Utilisez la fonctionnalité **Republier** d'Horizon Cloud Service pour les cas d'utilisation suivants.

- Si une tentative de publication d'une version de l'image échoue.

  Il n'est pas nécessaire de supprimer l'ancienne image et de commencer depuis le début pour republier la version de l'image.

- Si la version de l'image n'était pas incluse dans la publication initiale pour une instance de fournisseur

  Vous pouvez republier une version de l'image pour l'ajouter à une instance de fournisseur.

Avant d'effectuer l'une des étapes suivantes, vérifiez également les informations clés dans Déploiements de Microsoft Azure et IMS.

Republier une version d'image vers des instances de fournisseur supplémentaires

Lorsque vous disposez de plusieurs instances de fournisseur, vous devrez peut-être développer les emplacements d'une version de l'image vers des instances de fournisseur supplémentaires (dispositifs Edge) autres que celles sélectionnées lors d'une phase de publication précédente.

Développez l'emplacement d'une version de l'image sur une nouvelle instance de fournisseur.

Conditions préalables

L'état de la version de l'image doit être Partiellement publiée, En échec ou Disponible.

Procédure

1. Sur la page **Accueil** d'Horizon Universal Console, cliquez sur **Images**.
2. Sur la page **Images**, cliquez sur un lien d'image publiée.
3. Sélectionnez l'image publiée et cliquez sur **Publier**.
4. Sur la page **Republier l'image**, les dispositifs Horizon Edge sur lesquels la publication de la version de l'image a échoué sont sélectionnés automatiquement et ne peuvent pas être désélectionnés. Sélectionnez le dispositif Edge qui n'inclut aucune image, puis cliquez sur **Republier**.

Republier une image ayant échoué

Si une tentative de publication d'une image échoue, vous pouvez utiliser le workflow Republier pour retenter la publication. L'option Republier permet de redéclencher l'opération de publication à partir du point de défaillance.

Conditions préalables

L'état de l'image doit être Partiellement publiée, En échec ou Disponible.

Procédure

1. Sur la page **Accueil** d'Horizon Universal Console, cliquez sur **Images**.
2. Sur la page **Images**, cliquez sur le lien d'image ayant échoué.
3. Sélectionnez l'image ayant échoué et cliquez sur **Publier**.
4. Sur la page **Republier l'image**, les dispositifs Horizon Edge sur lesquels l'image n'a pas pu être publiée sont sélectionnés automatiquement et ne peuvent pas être désélectionnés. Cliquez sur **Republier**.

Analyser des applications dans des postes de travail distants

Vous pouvez analyser des applications pendant votre processus de gestion des images.

Conditions préalables

- La passerelle Edge Gateway est prête.
- L'image a été publiée.
- Au moins un réseau virtuel et un sous-réseau de locataire (poste de travail) sont sélectionnés pour le fournisseur.

Procédure

1. Sur la page **Accueil** d'Horizon Universal Console, cliquez sur **Images**.
2. Sur la page **Images**, cliquez sur le lien de l'image pour accéder à la page des versions de l'image.

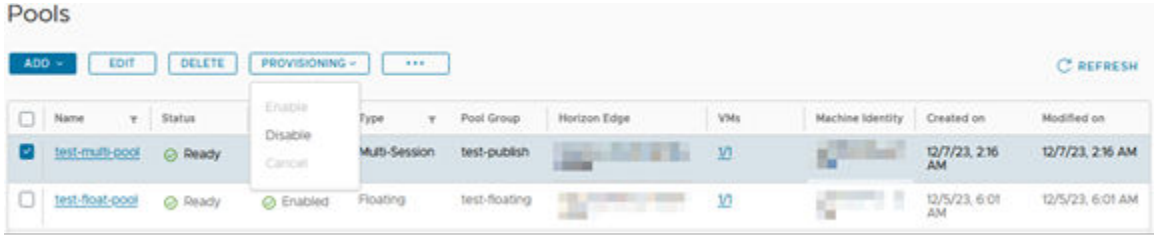
3 Sélectionnez le nom de la version de l'image à analyser, puis cliquez sur le bouton **Publiée > Analyser les applications**

4 Sélectionnez un réseau pour déclencher l'analyse.

5 Pour déclencher l'analyse, cliquez sur **Enregistrer**.

Gestion de provisionnement du pool

Lorsque vous terminez le workflow **Ajouter un pool** pour créer un pool pour un dispositif Microsoft Azure Edge, le système commence à provisionner des VM pour ce pool. Vous pouvez ensuite gérer le provisionnement des VM de ce pool de plusieurs manières dans la console Horizon Universal Console. Par exemple, si vous constatez que vous avez fait une erreur dans la configuration du pool, vous pouvez annuler ce dernier au lieu d'attendre la fin du provisionnement. D'autres options sont également disponibles.



Réessayer le provisionnement du pool

Vous pouvez effectuer cette tâche lorsque, sur la page Pools, un pool affiche l'état Erreur.

Pourquoi effectuer cette tâche ?

Pour permettre à la console Horizon Universal Console de vous aider à résoudre une erreur de provisionnement du pool, afin de pouvoir réessayer de provisionner le pool.

Comment effectuer cette tâche ?

Reportez-vous à la section Réessayer le provisionnement du pool.

Annuler le provisionnement du pool

Pourquoi effectuer cette tâche ?

Pour gagner du temps en arrêtant le processus de provisionnement du pool, qui peut parfois prendre beaucoup de temps. Vous pouvez constater que vous avez fait une erreur dans le mode de provisionnement du pool. Vous pouvez annuler le provisionnement du pool, tenter de résoudre le problème de configuration et reprovisionner le pool.

Comment effectuer cette tâche ?

Sur la page Pools, lorsqu'un pool affiche l'état Extension, sélectionnez **Provisionnement > Annuler**.

Résultat

Le provisionnement des VM s'arrête immédiatement et l'état du pool change, par exemple, sur Partiellement provisionné, Prêt ou Erreur. Les VM qui sont dans un état de provisionnement ou de personnalisation sont supprimées.

Désactiver le provisionnement du pool

Pourquoi effectuer cette tâche ?

Pour empêcher le provisionnement de nouvelles VM sur un pool spécifique. Cette option permet d'empêcher explicitement le provisionnement de VM sur ce pool jusqu'à la réactivation du provisionnement avec l'option **Activer**.

Comment effectuer cette tâche ?

Sur la page Pools, lorsque le provisionnement du pool est répertorié comme **Activé**, sélectionnez **Provisionnement > Désactiver**.

Résultat

Le provisionnement de nouvelles VM s'arrête et l'état du pool change, par exemple sur Partiellement provisionné, Prêt ou Erreur. Lorsque vous appliquez cette option, le traitement des VM qui sont dans un état de provisionnement ou de personnalisation continue.

Activer le provisionnement du pool

Pourquoi effectuer cette tâche ?

Pour permettre l'augmentation ou la réduction d'un pool. Cette option permet d'autoriser explicitement le provisionnement de VM sur un pool pour l'augmenter et le réduire si nécessaire.

Comment effectuer cette tâche ?

Sur la page Pools, lorsque le provisionnement du pool est répertorié comme **Désactivé**, vous pouvez activer le provisionnement du pool pour permettre une augmentation ou une réduction d'un pool. Sélectionnez **Provisionnement > Activer**.

Résultat

Le pool augmente ou se réduit en fonction de la demande.

Créer un pool

Une fois que vous disposez d'au moins une image dans la console Horizon Universal Console, vous pouvez créer un pool basé sur cette image.

Conditions préalables

Avant de créer un pool, le système requiert la configuration des éléments suivants dans votre environnement de nouvelle génération. Assurez-vous que ces éléments sont en place.

- Fournisseur d'identité de l'utilisateur final : vérifiez que vous avez configuré un fournisseur d'identité à utiliser pour l'identité de l'utilisateur final. Pour obtenir le contexte, reportez-vous à la section Gestion des identités et des accès dans un environnement Horizon Cloud Service - next-gen.
  - Si vous utilisez Microsoft Entra ID comme fournisseur d'identité de l'utilisateur final, vérifiez que la configuration de Microsoft Entra ID Connect est terminée.
- Fournisseur d'identité de machine : vérifiez que vous avez mis en place la configuration d'un fournisseur d'identité de machine. Ce fournisseur établit l'identité de machine des machines virtuelles qui fournissent des applications et des postes de travail distants.
  - Lorsque vous utilisez Microsoft Entra ID pour l'identité de l'utilisateur final, vous pouvez également l'utiliser pour l'identité de machine ou utiliser votre domaine Active Directory pour l'identité de machine.

    Note Lors de l'utilisation de Microsoft Entra ID pour l'identité de machine, sachez que lors de la suppression d'une VM ou d'un pool joint à Microsoft Entra ID, le fournisseur spécifié du pool nécessite des autorisations spécifiques pour supprimer l'entrée de périphérique de Microsoft Entra ID lors de la suppression du pool ou de la VM.

    Les autorisations requises sont les suivantes :

    ```
    Scope: Microsoft Graph https://graph.microsoft.com/
    Permission : Device.ReadWrite.All Read and write devices
    Admin Consent Required: Yes
    ```

    Pour utiliser le portail Azure afin d'ajouter les autorisations d'application au principal de service du fournisseur, accédez à **Enregistrements d'applications**, sélectionnez l'enregistrement d'application du principal de service et utilisez l'interface utilisateur **Autorisation d'API** pour ajouter l'autorisation `Device.ReadWrite.All` de l'application **Microsoft Graph**.
  - Si vous prévoyez d'utiliser votre domaine Active Directory pour l'identité de machine, assurez-vous d'avoir configuré le domaine Active Directory. Pour obtenir le contexte, reportez-vous à Configuration de votre domaine Active Directory.

    Note Lorsque vous utilisez Workspace ONE Access pour l'identité de l'utilisateur final, vous devez configurer un domaine Active Directory à utiliser pour l'identité de machine.
- Assurez-vous que le dispositif Horizon Edge est créé et que les déploiements de la passerelle Horizon Edge et d'UAG affichent des états sains (en vert) dans la console Horizon Universal Console sur **Ressources > Capacité > Dispositifs Horizon Edge**.

- Assurez-vous que l'image VDI ou à sessions multiples que vous utiliserez dans ce pool est publiée. Vous pouvez vérifier l'état de l'image dans la console Horizon Universal Console sur **Ressources > Images**.

Procédure

1. Dans la console Horizon Universal Console, accédez à la page **Pools** en cliquant sur **Ressources > Pools**
2. Démarrez l'assistant de création de pool en cliquant sur **Ajouter > Microsoft Azure**.
3. Dans l'assistant **Ajouter un pool**, saisissez un nom unique pour le pool dans le champ **Nom de pool** et, éventuellement, ajoutez une **Description**.
4. Sélectionnez un type de pool.
   - **Session unique dédiée** pour l'expérience de poste de travail VDI persistant dans lequel chaque poste de travail est mappé à un seul utilisateur.
   - **Session unique flottante** pour l'expérience de poste de travail VDI non persistant dans laquelle plusieurs utilisateurs peuvent utiliser le poste de travail à des moments différents et le poste de travail se réinitialise après chaque session d'utilisateur.
   - **Sessions multiples** pour les applications et postes de travail publiés basés sur une session.

   Après avoir sélectionné le type de pool, les sections suivantes de l'assistant affichent automatiquement les sélections appropriées pour le type de pool sélectionné.
5. Dans la section **Postes de travail**, pour la sous-section **Destination**, sélectionnez les valeurs des options **Site**, **Horizon Edge** et **Fournisseur**.
6. Toujours dans la sous-section **Destination**, si vous souhaitez utiliser des zones de disponibilité Azure, activez l'option **Utiliser les zones de disponibilité Azure**.

   Les zones de disponibilité Azure sont une fonctionnalité de haute disponibilité disponible avec Microsoft Azure. Lorsque vous sélectionnez **Utiliser les zones de disponibilité Azure**, les machines virtuelles d'un pool sont réparties sur toutes les zones de disponibilité afin d'éviter les interruptions de service de toutes les machines virtuelles du pool en cas de panne dans une zone de disponibilité Azure donnée.

   Note Pour plus d'informations sur les limitations de la prise en charge de la zone de disponibilité Azure, reportez-vous à la documentation de Microsoft suivante.

7 Dans la sous-section **Image**, sélectionnez une option **Type de génération** et une option **Image** pour ce pool.

Note

- Les images avec les VM Microsoft Azure de génération 1 et 2 sont prises en charge.
- Si vous sélectionnez **V1**, seules les images avec une VM Microsoft Azure de génération 1 et les modèles prenant en charge la génération 1 peuvent être sélectionnés.
- Votre sélection pour le **Type de génération** agit comme un filtre pour déterminer les images répertoriées dans le menu déroulant **Image** et les modèles répertoriés dans le menu déroulant **Modèle**.

8 Sélectionnez le **Marqueur** de l'image sélectionnée.

Vous devez ajouter un ou plusieurs marqueurs pour modifier ultérieurement les pools d'une version de l'image. Ajoutez les marqueurs s'ils n'ont pas été ajoutés précédemment à la version de l'image. Pour plus d'informations, reportez-vous à la section Ajouter une version à une image de la galerie de calcul Microsoft Azure existante.

Note Si un marqueur associé à une version antérieure de l'agent est sélectionné, un message d'avertissement s'affiche. Il est recommandé de sélectionner un marqueur avec la dernière version de l'agent.

9 Faites glisser la bascule en regard de l'option **Disposez-vous d'une licence valide pour ce système d'exploitation Windows ?** afin de confirmer que vous disposez de licences Windows éligibles avec un abonnement Software Assurance ou Windows Server pour appliquer cet avantage Azure Hybrid Benefit, puis cochez la **case**.

10 Dans la sous-section **Détails de la VM**, sélectionnez des valeurs pour les options **Modèle de filtre**, **Modèle**, **Type de disque**, **Taille du disque** et **Chiffrer les disques** de votre pool.

Note Dans le paramètre **Modèle**, reportez-vous à l'article de la base de connaissances Types et tailles de VM Microsoft Azure pour Horizon Cloud Service - next-gen (89090) pour en savoir plus sur la compatibilité des différents types et des différentes tailles de VM Microsoft Azure avec un environnement de nouvelle génération.

- Vous pouvez utiliser les paramètres **Modèle de filtre** pour réduire le nombre d'options de modèles de VM Microsoft Azure répertoriées lorsque vous configurez le paramètre **Modèle**. La liste réduite inclut un sous-ensemble de modèles en fonction de vos besoins spécifiques.

Vous pouvez filtrer la liste de modèles de VM Microsoft Azure par **Balise**, **Série**, **Type de GPU** et **Type de disque**. Cliquez sur **+** pour ajouter d'autres filtres, en affinant potentiellement davantage la liste avec chaque filtre.

Balise	est égal à	■ L'option **Recommandé par VMware** indique les modèles de VM Microsoft Azure qui fonctionnent particulièrement bien pour les pools. ■ L'option **Haute performance** indique les modèles de VM Microsoft Azure qui proposent un support Premium pour les disques.
Série	est égal à	Utilisez le menu déroulant pour afficher la liste des différentes séries de VM Microsoft Azure. Sélectionnez une série qui répond le mieux à vos besoins.
Type de GPU	est égal à	Vous pouvez utiliser le filtre **Type de GPU** pour sélectionner un modèle de VM Microsoft Azure avec GPU activé. ■ **NONE** permet de filtrer les modèles avec GPU activé de la liste. ■ **AMD** n'inclut que les modèles avec GPU AMD activé dans la liste. ■ **NVIDIA** n'inclut que les modèles avec GPU NVIDIA activé dans la liste.
Type de disque	est égal à	Vous pouvez utiliser le filtre **Type de disque** pour sélectionner **Premium**, qui fournit un support Premium pour les disques.

- Sélectionnez un type de **Modèle** de VM Microsoft Azure à utiliser pour le pool ou acceptez la valeur par défaut.

  1 Pour accepter un modèle par défaut, acceptez celui qui est répertorié ou utilisez le menu déroulant pour en sélectionner un autre.

  2 Pour sélectionner un autre modèle, cliquez sur X, puis cliquez sur le menu déroulant et sélectionnez un modèle.

  Si vous n'avez pas utilisé le paramètre **Modèle de filtre**, la liste de modèles est très longue. Si vous avez utilisé le paramètre **Modèle de filtre**, la liste sera probablement plus gérable.

- Vous pouvez sélectionner l'option **Type de disque** en fonction du modèle de VM sélectionné, ainsi que de la région et de l'abonnement Microsoft Azure.
- Vous pouvez passer la valeur **Taille du disque** de 127 à 4 095 Go. La valeur **Taille du disque** par défaut est de 127.
- Si vous souhaitez chiffrer les disques de toutes les VM de ce pool, faites glisser la bascule sur **Chiffrer les disques**.

11 Dans la sous-section **Identité de machine (Domaine)**, sélectionnez un fournisseur **d'identité de machine** à utiliser pour ce pool.

Les choix sont les suivants :

- Domaine Active Directory configuré dans votre environnement de nouvelle génération afin de fournir l'identité de machine. Avec cette sélection, vous pouvez remplacer l'unité d'organisation (UO) `CN=Computers` par une **Unité d'organisation de l'ordinateur** spécifique dans laquelle les machines du pool sont créées dans ce domaine Active Directory. Par défaut, les machines du pool sont créées dans `CN=Computers`.
- Choix d'**Azure Active Directory**. Lorsque vous sélectionnez **Azure Active Directory**, le champ **Unité d'organisation de l'ordinateur** est désactivé, car le système n'utilise pas d'unités d'organisation de l'ordinateur dans ce cas.

  Lorsque vous utilisez **Azure Active Directory** pour l'identité de machine du pool, vous devez configurer RBAC dans **Azure Active Directory** afin que seuls les utilisateurs ou les groupes d'utilisateurs disposant du rôle **Connexion d'administrateur de machine virtuelle** ou **Connexion d'utilisateur de machine virtuelle** puissent se connecter à leurs droits.

  Lorsque vous configurez RBAC au niveau du groupe de ressources, pour faciliter l'identification des groupes de ressources associés aux pools joints à Azure Active Directory, les balises suivantes sont utilisées dans les groupes de ressources des pools :

  - **pool-name** : indique le nom du pool entré lors de la création du pool
  - **Add-joint** : s'il est défini avec **true**, cette valeur indique que les VM du pool sont des machines jointes à Microsoft Entra ID

Note Tous les périphériques Windows 11 et Windows 10 sont pris en charge, sauf les éditions Home de Windows Server 2019 et les machines virtuelles plus récentes s'exécutant dans Azure (le noyau du serveur n'est pas pris en charge).

12 Dans la sous-section **Provisionnement**, configurez les paramètres selon vos besoins.

a Sélectionnez le mode de provisionnement des VM dans la sous-section Provisionner des VM, entre **À la demande** et **Tout à la fois**.

b Entrez le **Nombre maximal de VM** pouvant être provisionnées pour ce pool.

c Si l'option **À la demande** est sélectionnée, sélectionnez le **Nombre minimal de VM de rechange** et le **Nombre maximal de VM de rechange**.

13 Dans la sous-section **Propriétés**, spécifiez les éléments suivants :

- **Préfixe de nom de VM** : saisissez un préfixe à utiliser pour les VM du pool.
- **Réutiliser les noms de VM** : cette option spécifie la réutilisation des noms de VM après la suppression de celles-ci.

- **Nom d'utilisateur de l'administrateur de poste de travail** et **Mot de passe de l'administrateur de poste de travail** : saisissez les informations d'identification pour le compte d'administrateur local utilisé pour accéder au système d'exploitation de l'image et à utiliser lors du processus de conversion de l'image.
- **Utiliser le proxy sortant** : vous pouvez faire glisser cette option pour router les demandes sortantes vers Internet via un serveur proxy.

14 Passez à la section suivante en cliquant sur **Suivant**.

15 Dans la sous-section **Réseaux**, sélectionnez les réseaux virtuels et les sous-réseaux de locataire (poste de travail).

Par défaut, les postes de travail virtuels utilisent des adresses IPv4. Pour que la machine virtuelle utilise des adresses IPv4 et IPv6, activez l'option **Activer la prise en charge de la double pile** et sélectionnez les sous-réseaux configurés comme double pile.

Note Lorsque vous activez l'option double pile, seuls les sous-réseaux configurés comme double pile sont répertoriés.

16 Dans la sous-section **VMware Dynamic Environment Manager**, vous pouvez éventuellement sélectionner une configuration VMware Dynamic Environment Manager pour ce pool.

17 Pour enregistrer le pool récemment créé dans votre environnement, cliquez sur **Enregistrer**.

Après avoir cliqué sur **Enregistrer**, le système offre la possibilité de démarrer le flux pour ajouter ce nouveau pool à un nouveau groupe de pools ou l'ajouter à un groupe de pools existant, ou de reporter cette tâche à plus tard.

- **AJOUTER AU GROUPE DE POOLS** : cliquez sur ce bouton pour démarrer le flux d'ajout du nouveau pool à un groupe de pools existant, avec l'option permettant de créer un groupe de pools auquel ce pool sera ajouté.
- **TERMINER** : cliquez sur ce bouton pour différer la tâche d'ajout du pool à un groupe de pools. Lorsque vous cliquez sur **TERMINER**, le système revient à la page **Pools** avec le pool récemment créé répertorié. Sur la page **Pools**, vous pouvez ajouter un pool à un groupe de pools en sélectionnant le pool et en cliquant sur **... > Ajouter au groupe de pools**.

18 Si vous avez cliqué sur **AJOUTER AU GROUPE DE POOLS** à la fin de l'assistant de création de pools, le système démarre l'assistant d'ajout du pool à un groupe de pools.

Le système démarre automatiquement le flux avec le type de groupe de pools sélectionné en fonction du type de pool que vous ajoutez.

Pour plus d'informations sur le flux **AJOUTER AU GROUPE DE POOLS**, reportez-vous à la section Créer un groupe de pools à session unique ou Créer un groupe de pools à plusieurs sessions.

Vous pouvez également sélectionner un pool et l'ajouter à un pool en cliquant sur **AJOUTER AU GROUPE DE POOLS** si aucun groupe de pools n'est associé à un groupe de pools.

Résultats

Lorsqu'un pool est répertorié sur la page **Pools**, vous pouvez utiliser les éléments de l'interface utilisateur de la page pour effectuer des actions sur le pool, telles que la modification de la définition du pool et la suppression de ce dernier.

Pour un pool auquel aucun groupe de pools n'est associé, vous pouvez l'ajouter à un groupe de pools en sélectionnant le pool et en cliquant sur **... > Ajouter au groupe de pools**.

Étape suivante

- Surveillez le provisionnement du pool et prenez les mesures appropriées. Reportez-vous à la section Gestion de provisionnement du pool
- Créez un groupe de pools. Reportez-vous à la section Créer un groupe de pools.

Créer un groupe de pools

Les groupes de pools permettent d'autoriser l'accès à tout moment des utilisateurs ou des groupes à des postes de travail et à des applications. Vous pouvez créer un pool à une ou à plusieurs sessions.

Créer un groupe de pools à session unique

Les groupes de pools permettent d'autoriser l'accès à tout moment des utilisateurs ou des groupes à des postes de travail et à des applications. À l'aide d'Horizon Cloud Service - next-gen, vous pouvez créer une session unique qui inclut des pools à partir de n'importe quel fournisseur, ainsi que des stratégies.

Procédure

1. Sur la page **Accueil**, cliquez sur la vignette **Groupes de pools** pour accéder à la page **Groupes de pools**.
2. Cliquez sur **Ajouter** pour sélectionner le pool **Ajouter un groupe de pools à session unique**.
3. Sur la page **Ajouter un groupe de pools à session unique**, ajoutez un **Nom** de pool unique.
4. Ajoutez un **Nom complet** et une **Description**.

   Nom complet est le nom à afficher aux utilisateurs finaux sur les instances d'Horizon Client. Il ne peut pas dépasser 64 caractères. S'il reste vide, le nom de groupe de pools sera utilisé par défaut.
5. Choisissez un **Type de groupe de pools** entre **Dédié**, pour l'expérience de poste de travail VDI persistant mappé à un seul utilisateur final, et **Flottant**, pour l'expérience de poste de travail VDI non persistant auquel plusieurs utilisateurs peuvent accéder à différents moments et qui se réinitialise après chaque session.
6. Sélectionnez un pool dans **Pools**, puis cliquez sur **Suivant**.

7 Dans la section **Applications App Volumes**, sélectionnez les applications App Volumes que vous souhaitez rendre disponibles sur des postes de travail flottants. Cliquez sur **Suivant**.

Les applications App Volumes sélectionnées au niveau du groupe de pools sont fournies aux VM flottantes. Cette allocation s'ajoute à l'allocation d'applications App Volumes au niveau du droit (utilisateur/groupe d'utilisateurs).

Note

- Vous pouvez sélectionner les applications App Volumes et les rendre disponibles sur les postes de travail uniquement pour **Postes de travail flottants**. Cette fonctionnalité n'est pas disponible pour **Postes de travail dédiés**.
- Pour fournir une application App Volumes, App Volumes Agent doit être installé sur l'image du pool et le module d'application doit être disponible dans le dispositif Horizon Edge.
- Un module d'application doit être disponible dans une région particulière afin d'être fourni à une VM de la même région.
- Les applications sans modules capturés ne peuvent pas être sélectionnées. La case à cocher est désactivée et ne peut pas être cochée.

8 Dans la section **Détails de l'application**, sélectionnez un module pour chaque application.

9 Si un utilisateur est autorisé à accéder à différents modules de la même application via le groupe de pools et les droits d'utilisateur ou de groupe d'utilisateurs, choisissez entre **Groupe de pools** et **Droit d'utilisateur ou de groupe d'utilisateurs** pour **Priorité de conflit** pour choisir le module à fournir. Cliquez sur **Suivant**.

10 Dans la section **Stratégies** des paramètres de **Client** par défaut, sélectionnez **Protocole par défaut** pour les sessions d'utilisateurs finaux.

Vous pouvez faire glisser la bascule vers l'option **Autoriser les utilisateurs à sélectionner un protocole** lorsqu'ils se connectent à un poste de travail.

11 Sélectionnez **Type de client préféré** pour lancer des droits dans **Horizon Client** ou un **Navigateur**.

12 Pour le groupe de pools **Dédié**, sélectionnez l'option pour **Afficher le nom de la machine attribuée**.

L'option **Afficher le nom de la machine attribuée** affiche le nom d'hôte de la machine attribuée plutôt que le nom complet du groupe de pools lorsque vous vous connectez à Horizon Client.

Si plusieurs machines d'un groupe de pools sont attribuées à un utilisateur, le nom de la machine attribuée s'affiche toujours. Cette fonctionnalité n'est pas disponible pour les groupes de pools **Flottants**.

13 Dans la sous-section **Intermédiation**, sélectionnez **Portée** pour rechercher des postes de travail disponibles sur **N'importe quel site** ou **Limiter à un seul site**.

14 Dans le champ **Affinité de connexion au site**, sélectionnez le site par défaut auquel les utilisateurs finaux se connecteront, depuis **Site le plus proche** et **Site de base**.

Vous pouvez faire glisser la bascule **Restriction du site de base** pour empêcher les utilisateurs finaux ou les groupes d'utilisateurs d'accéder au droit uniquement via le remplacement du site de base du droit ou via le site de base de l'utilisateur si aucun remplacement n'est désigné. Si cette option n'est pas sélectionnée, le site le plus proche sera utilisé.

15 Dans la sous-section **SSO**, vous pouvez faire glisser la bascule pour activer l'authentification SSO du pool.

Vous devez avoir répondu aux conditions préalables à la configuration de l'un des types SSO qu'Horizon Cloud prend en charge sur la passerelle Passerelle Horizon Edge, ainsi que toutes les conditions requises pour ce type SSO. Si les conditions préalables requises par le type SSO configuré ne sont pas remplies, l'utilisateur final sera invité à entrer ses informations d'identification.

16 Pour **Type de groupe de pool Dédié**, dans la section **Gestion de l'alimentation**, spécifiez un seuil pour **VM inutilisées**, qui correspond au nombre minimal de machines virtuelles à maintenir sous tension par rapport au nombre total de machines virtuelles d'un groupe de pools à un moment donné.

Une machine virtuelle inutilisée est une machine virtuelle provisionnée et mise sous tension, mais sans utilisateur connecté. Ce paramètre s'applique à chaque groupe de pools du droit, sauf si une planification de gestion de l'alimentation est spécifiée.

17 Dans le champ **Temps de protection contre la mise hors tension**, ajoutez le nombre de minutes (de 1 à 60) pendant lesquelles une machine virtuelle est protégée après la mise sous tension. Le port par défaut est 30.

18 Pour **Type de groupe de pools Flottant**, dans la section **Gestion de l'alimentation**, choisissez entre **Basé sur l'occupation** et **Non basé sur l'occupation** pour le **Type de gestion de l'alimentation**.

19 Pour **Basé sur l'occupation**, sélectionnez le seuil d'utilisation de la machine virtuelle pour ce droit avec lequel une nouvelle machine virtuelle est respectivement démarrée et purgée dans **Optimisé pour les performances**, **Équilibré** et **Optimisé pour le coût** dans le champ **Mode de gestion de l'alimentation**.

En sélectionnant **Optimisé pour les performances**, une nouvelle machine virtuelle est démarrée plus rapidement, ce qui rend la capacité disponible pour une éventuelle expérience utilisateur améliorée.

En sélectionnant **Optimisé pour le coût**, la machine virtuelle présente un taux d'utilisation plus élevé avant de démarrer une nouvelle machine virtuelle, ce qui peut contribuer à réduire les coûts.

20 Ajoutez **Nombre minimal de VM** pour le pourcentage minimal de machines virtuelles à maintenir sous tension par rapport au nombre total de machines virtuelles dans un groupe de pools à un moment donné.

   Ce paramètre s'applique à chaque groupe de pools du droit, sauf si une planification de gestion de l'alimentation est spécifiée.

21 Dans le champ **Temps de protection contre la mise hors tension**, ajoutez le nombre de minutes (de 1 à 60).

   Une VM est protégée contre la mise hors tension après la mise sous tension en raison d'une erreur de marge. Le port par défaut est 30.

22 Pour **Non basé sur l'occupation**, spécifiez un seuil de **VM inutilisées**, qui correspond au nombre total de machines virtuelles à maintenir sous tension par rapport au nombre total de machines virtuelles dans un groupe de pools à un moment donné.

   Une machine virtuelle inutilisée est une machine virtuelle provisionnée et mise sous tension, mais sans utilisateur connecté. Ce paramètre s'applique à chaque groupe de pools du droit, sauf si une planification de gestion de l'alimentation est spécifiée.

23 Dans le champ **Temps de protection contre la mise hors tension**, ajoutez le nombre de minutes (de 1 à 60).

   Une VM est protégée contre la mise hors tension après la mise sous tension en raison d'une erreur de marge. Le port par défaut est 30.

24 Vous pouvez également ajouter une **Planification de la gestion de l'alimentation** en cliquant sur **Ajouter une planification** et en ajoutant des informations.

25 Dans la section **Traitement du délai d'expiration**, déterminez à quel moment une session déconnectée est fermée dans le champ **Fermer les sessions déconnectées**. Sélectionnez **Jamais**, **Immédiat** ou **Fermeture de session après**.

   La valeur par défaut pour l'option **Fermer les sessions déconnectées** est **Jamais**. Si vous sélectionnez **Fermeture de session après**, spécifiez le délai d'expiration après lequel les sessions déconnectées sont fermées.

   La valeur par défaut de **Fermeture de session après** est de 120 minutes. Pour **Délai d'expiration de session d'application vide**, choisissez entre **Jamais** et **Expiration après**, puis ajoutez un délai en minutes après lequel la session vide expire.

   Choisissez entre **Fermer la session** et **Déconnecter**, car le délai d'expiration se produit pour une session d'application vide. Quand une session déconnectée est fermée, elle est perdue.

   Entrez le nombre maximal de minutes pour la session dans le champ **Durée de vie maximale de session**. La valeur par défaut de **Durée de vie maximale de session** est de 10 080 minutes.

   Dans le champ **Délai d'expiration de session inactive**, entrez la durée pendant laquelle une session utilisateur peut être inactive avant que le système ne force une déconnexion. La valeur par défaut du **Délai d'expiration de session inactive** est de 10 080 minutes.

26 Cliquez sur **Enregistrer**.

27 Cliquez sur **AUTORISER LE GROUPE DE POOLS** pour autoriser l'accès des utilisateurs ou des groupes d'utilisateurs à ce groupe de pools maintenant, ou cliquez sur **TERMINER** pour l'autoriser ultérieurement.

Créer un groupe de pools à plusieurs sessions

Les pools permettent d'autoriser l'accès à tout moment des utilisateurs ou des groupes à des postes de travail et à des applications. Vous pouvez créer un pool à plusieurs sessions qui inclut des pools de n'importe quel fournisseur, ainsi que des stratégies.

Procédure

1 Sur la page **Accueil**, cliquez sur la vignette **Groupes de pools** pour accéder à la page **Groupes de pools**.

2 Cliquez sur **Ajouter** pour sélectionner le groupe de pools à **Plusieurs sessions**.

3 Sur la page **Ajouter un groupe de pools à plusieurs sessions**, ajoutez un **Nom** de groupe de pools unique.

4 Ajoutez un **Nom complet** et une **Description**.

Nom complet est le nom à afficher aux utilisateurs finaux sur les instances d'Horizon Client. Il ne peut pas dépasser 64 caractères. S'il reste vide, le nom de pool sera utilisé par défaut.

5 Sélectionnez un **Type de groupe de pools** dans **Poste de travail publié**, **Application publiée** et **Poste de travail et application publiés**.

6 Dans **Poste de travail publié**, sélectionnez un pool dans **Pools**, puis cliquez sur **Suivant**. Pour **Stratégies**, passez à l'étape 11.

7 Dans la section **Applications manuelles**, cliquez sur **Ajouter** pour créer une application manuelle.

8 Dans la fenêtre modale **Ajouter une application manuelle**, ajoutez un **Nom** pour l'application et, éventuellement, cliquez sur **Parcourir** pour parcourir un fichier **Icône** et ajouter une icône. Ajoutez les champs **Chemin d'accès**, **Version** et **Éditeur** pour l'application. Vous pouvez éventuellement sélectionner un paramètre entre **Tous les pools** et **Personnalisé**, puis ajouter des paramètres d'application et éventuellement **Dossier de démarrage**.

9 Sélectionnez les applications manuelles que vous souhaitez rendre disponibles comme applications publiées dans le groupe de pools. Cliquez sur **Suivant**. Vous pouvez également **modifier** et **supprimer** une application en cliquant sur les trois points en regard de son nom dans la liste.

10 Dans la section **Attributs d'application**, vous pouvez éventuellement spécifier des attributs pour les applications sélectionnées. Par défaut, le mode de sessions multiples est désactivé. Vous pouvez modifier le mode de sessions multiples pour les applications.

11 Dans la section **Stratégies** des paramètres de **Client** par défaut, sélectionnez **Protocole par défaut** pour les sessions d'utilisateurs finaux.

   Vous pouvez faire glisser la bascule vers l'option **Autoriser les utilisateurs à sélectionner un protocole** lorsqu'ils se connectent à un poste de travail.

12 Sélectionnez **Type de client préféré** pour lancer des droits dans **Horizon Client** ou un **Navigateur**.

13 Dans la sous-section **Intermédiation**, sélectionnez **Portée** pour rechercher des postes de travail disponibles sur **N'importe quel site** ou **Limiter à un seul site**.

14 Dans le champ **Affinité de connexion au site**, sélectionnez le site par défaut auquel les utilisateurs finaux se connecteront, depuis **Site le plus proche** et **Site de base**.

   Vous pouvez faire glisser la bascule **Restriction du site de base** pour empêcher les utilisateurs finaux ou les groupes d'utilisateurs d'accéder au droit uniquement via le remplacement du site de base du droit ou via le site de base de l'utilisateur si aucun remplacement n'est désigné. Si cette option n'est pas sélectionnée, le site le plus proche sera utilisé.

15 Dans la sous-section **SSO**, vous pouvez faire glisser la bascule pour activer l'authentification SSO du pool.

   Vous devez avoir répondu aux exigences pour configurer l'un des types SSO qu'Horizon Cloud prend en charge sur la passerelle Horizon Edge, ainsi que toutes les exigences relatives à ce type SSO. Si les conditions préalables requises par le type SSO configuré ne sont pas remplies, l'utilisateur final sera invité à entrer ses informations d'identification.

16 Dans la section **Gestion de l'alimentation**, choisissez entre **Basé sur l'occupation** et **Non basé sur l'occupation** pour **Type de gestion de l'alimentation**. **Basé sur l'occupation** optimise la consommation d'énergie en fonction de la charge d'occupation du pool. **Non basé sur l'occupation** optimise la consommation d'énergie en fonction du nombre de machines virtuelles inutilisées mises sous tension par rapport au nombre total de machines virtuelles provisionnées.

17 Pour **Basé sur l'occupation**, sélectionnez le seuil d'utilisation de la machine virtuelle pour ce droit avec lequel une nouvelle machine virtuelle est respectivement démarrée et purgée dans **Optimisé pour les performances**, **Équilibré** et **Optimisé pour le coût** dans le champ **Mode de gestion de l'alimentation**.

   En sélectionnant **Optimisé pour les performances**, une nouvelle machine virtuelle est démarrée plus rapidement, ce qui rend la capacité disponible pour une éventuelle expérience utilisateur améliorée. En sélectionnant **Optimisé pour le coût**, la machine virtuelle présente un taux d'utilisation plus élevé avant de démarrer une nouvelle machine virtuelle, ce qui peut contribuer à réduire les coûts.

18 Ajoutez **Nombre minimal de VM** pour le pourcentage minimal de machines virtuelles à maintenir sous tension par rapport au nombre total de machines virtuelles dans un groupe de pools à un moment donné.

Ce paramètre s'applique à chaque groupe de pools du droit, sauf si une planification de gestion de l'alimentation est spécifiée.

19 Pour **Temps de protection contre la mise hors tension**, ajoutez le nombre de minutes (de 1 à 60).

Une VM est protégée contre la mise hors tension après la mise sous tension en raison d'une erreur de marge. Le port par défaut est 30.

20 Pour **Non basé sur l'occupation**, spécifiez un seuil de **VM inutilisées**, qui correspond au nombre total de machines virtuelles à maintenir sous tension par rapport au nombre total de machines virtuelles dans un groupe de pools à un moment donné.

Une machine virtuelle inutilisée est une machine virtuelle provisionnée et mise sous tension, mais sans utilisateur connecté. Ce paramètre s'applique à chaque groupe de pools du droit, sauf si une planification de gestion de l'alimentation est spécifiée.

21 Pour **Temps de protection contre la mise hors tension**, ajoutez le nombre de minutes (de 1 à 60).

Une VM est protégée contre la mise hors tension après la mise sous tension en raison d'une erreur de marge. Le port par défaut est 30.

22 Vous pouvez également ajouter une **Planification de la gestion de l'alimentation** en cliquant sur **Ajouter une planification** et en ajoutant des informations.

23 Remplissez la section Équilibrage de charge en fonction des descriptions d'options qui suivent.

Note Les paramètres suivants peuvent vous aider à obtenir un équilibre souhaité de la consommation d'énergie et des performances dans votre environnement.

Option	Description
Durée entre l'allocation de sessions consécutives	Ce paramètre entraîne le déploiement de nouvelles sessions d'utilisateurs afin de limiter le nombre de sessions attribuées à une VM pendant la période configurée. Par exemple, si ce paramètre est de 20 secondes et qu'un utilisateur est attribué à VM1 au cours des 20 dernières secondes, l'utilisateur suivant est attribué à VM2.
Utilisation du CPU	Valeur de seuil de l'utilisation du CPU en pourcentage. Vous pouvez définir une valeur comprise entre 0 et 100. La valeur recommandée est 90, ce qui est également la valeur par défaut.
Utilisation de la mémoire	Valeur de seuil de la mémoire en pourcentage. Vous pouvez définir une valeur comprise entre 0 et 100. La valeur recommandée est 90, ce qui est également la valeur par défaut.
Longueur de la file d'attente du disque	Seuil du nombre moyen de demandes de lecture et d'écriture qui ont été remises en file d'attente pour le disque sélectionné pendant l'intervalle d'échantillonnage. Vous pouvez définir la valeur sur n'importe quel nombre entier positif. Par défaut, ce paramètre n'est pas pris en compte pour l'équilibrage de charge. La valeur par défaut est 0.

Option	Description
Latence de lecture du disque	Seuil de la durée moyenne de lecture des données du disque en millisecondes. Vous pouvez définir la valeur sur n'importe quel nombre entier positif. Par défaut, ce paramètre n'est pas pris en compte pour l'équilibrage de charge. La valeur par défaut est 0.
Latence d'écriture du disque	Seuil de la durée moyenne d'écriture des données sur le disque en millisecondes. Vous pouvez définir la valeur sur n'importe quel nombre entier positif. Par défaut, ce paramètre n'est pas pris en compte pour l'équilibrage de charge. La valeur par défaut est 0.
Indice de charge de l'hôte	Valeur de seuil globale à laquelle une VM est considérée comme étant complète et ne reçoit aucune nouvelle session. Vous pouvez entrer une valeur comprise entre 0 et 100 secondes. La valeur par défaut est de 90. La valeur est calculée en comparant l'utilisation du CPU, de la mémoire et du disque avec les valeurs de seuil correspondantes. La ressource dont l'utilisation est la plus élevée par rapport à son seuil bénéficie de la meilleure pondération.

24 **Activez la maintenance progressive** dans la section **Maintenance progressive** pour assurer l'actualisation automatisée des VM à plusieurs sessions afin de maintenir la disponibilité. Cela permet d'effacer les ressources mises en cache ou les fuites de mémoire, évitant ainsi les problèmes liés aux sessions des utilisateurs finaux.

25 Pour **Type de maintenance**, sélectionnez **Planifiée** ou **Session**.

La maintenance progressive déclenche une actualisation de machine virtuelle. Avec l'option Planifiée, l'actualisation est déclenchée tous les jours ou toutes les semaines en fonction des paramètres entrés. Avec l'option Session, l'actualisation est déclenchée une fois que les sessions auxquelles vous pouvez participer sont ouvertes. Dans les deux cas, l'actualisation ne se produit pas tant que l'utilisateur final n'est pas déconnecté.

26 Sélectionnez **Quotidienne** ou **Hebdomadaire** comme **Récurrence** dans la liste déroulante pour définir la fréquence à laquelle planifier l'actualisation de la machine virtuelle.

27 Sélectionnez le **Fuseau horaire** approprié pour le paramètre d'heure planifiée.

28 Ajoutez l'**Heure planifiée** de la journée à laquelle vous souhaitez planifier l'actualisation des machines virtuelles.

29 Ajoutez un nombre à **VM mises au repos simultanément par pool** pour définir le nombre de machines virtuelles pouvant être arrêtées simultanément pour maintenance.

Lors de ce processus, les machines virtuelles assurent le service, mais ne sont pas utilisées pour de nouvelles sessions.

30 Sélectionnez **Redémarrer** ou **Recréer** comme **Action de VM** pour les machines virtuelles nécessitant une maintenance.

Si vous sélectionnez **Redémarrer**, les machines virtuelles affectées sont redémarrées. Si vous sélectionnez **Recréer**, les machines virtuelles affectées sont supprimées, puis reprovisionnées à l'aide de la dernière image.

31 Dans la section **Traitement du délai d'expiration**, déterminez à quel moment une session déconnectée est fermée dans le champ **Fermer les sessions déconnectées**. Sélectionnez **Jamais**, **Immédiat** ou **Fermeture de session après**. La valeur par défaut pour l'option **Fermer les sessions déconnectées** est **Jamais**. Si vous sélectionnez **Fermeture de session après**, spécifiez le délai d'expiration après lequel les sessions déconnectées sont fermées. La valeur par défaut de **Fermeture de session après** est de 120 minutes. Quand une session déconnectée est fermée, elle est perdue. Entrez le nombre maximal de minutes pour la session dans le champ **Durée de vie maximale de session**. La valeur par défaut de **Durée de vie maximale de session** est de 10 080 minutes. Dans **Délai d'expiration de session inactive**, entrez la durée pendant laquelle une session utilisateur peut être inactive avant que le système ne force une déconnexion. La valeur par défaut du **Délai d'expiration de session inactive** est de 10 080 minutes.

    Faites votre choix entre **Jamais** et **Expiration après** pour **Délai d'expiration de session d'application vide**. La valeur par défaut pour **Délai d'expiration de session d'application vide** est **Jamais**. Si un utilisateur exécute une session d'application et qu'aucune application ne s'exécute dans cette session, celle-ci est considérée comme vide. Si vous sélectionnez **Expiration après**, ajoutez un délai en minutes après lequel la session vide expire. La valeur par défaut pour **Expiration après** est de 1 minute. Dans le champ **À l'expiration du délai**, choisissez entre **Fermer la session** et **Déconnecter**. La valeur par défaut pour **À l'expiration du délai** est **Fermer la session** où la session se fermera sans déconnexion. Le paramètre **Délai d'expiration de session d'application** s'applique si vous sélectionnez **Application publiée** ou **Poste de travail et application publiés**, et pas pour **Postes de travail publiés**.

32 Cliquez sur **Enregistrer**.

33 Cliquez sur **AUTORISER LE GROUPE DE POOLS** pour autoriser l'accès des utilisateurs ou des groupes d'utilisateurs à ce groupe de pools maintenant, ou cliquez sur **TERMINER** pour l'autoriser ultérieurement.

Configurer un client de groupe de pools comme Direct Connect uniquement

Dans Horizon Cloud Service - next-gen, vous pouvez configurer un client de groupe de pools en connexion directe afin que vos utilisateurs Horizon Client internes puissent se connecter directement à des ressources internes telles que des postes de travail et des agents sans avoir besoin d'utiliser le nom de domaine complet externe d'Unified Access Gateway.

Vous pouvez autoriser un client d'un groupe de pools à se connecter directement à des ressources internes, telles que des postes de travail et des agents, et à contourner Unified Access Gateway. Vous pouvez spécifier l'option Direct Connect lors de la création ou de la modification d'un groupe de pools. L'option Direct Connect est disponible pour n'importe quel type de groupe de pools : dédié, flottant ou multisession.

Pour configurer cette option, vous devez d'abord respecter les conditions préalables suivantes :

- En tant qu'administrateur, spécifiez l'option Direct Connect pour le groupe de pools.

À partir de la console Horizon Universal Console, cliquez sur **Ressources > Groupes de pools** et activez l'option **Direct Connect uniquement** dans la section Client de la page de l'indicateur d'étape **Stratégies**.

- En tant qu'administrateur, spécifiez les plages réseau internes à rendre disponibles pour Direct Connect.

  À partir de la console Horizon Universal Console, cliquez sur **Paramètres > Paramètres du client > Plages réseau** et spécifiez les plages réseau internes à rendre disponibles pour Direct Connect.

Un exemple de modification d'un groupe de pools existant pour autoriser Direct Connect s'affiche ci-dessous.

1. Ouvrez la console Horizon Universal Console.
2. Cliquez sur **Ressources > Groupes de pools**.
3. Sélectionnez un groupe de pools existant, puis cliquez sur **Modifier**.
4. Sur la page **2. Stratégies**, activez le bouton bascule **Direct Connect uniquement** dans la section Client de la page.

   Lorsque vous activez le bouton **Direct Connect uniquement**, le bouton **Accès interne uniquement** est automatiquement activé. Ce paramètre est actuellement inaccessible indépendamment de l'option **Direct Connect uniquement**. Pour plus d'informations, reportez-vous au texte d'aide explicatif pour les deux boutons.
5. Cliquez sur **Enregistrer**.

Pour confirmation, vous pouvez vérifier la page de résumé Stratégies du groupe de pools pour afficher l'état de l'option **Direct Connect uniquement** dans la section Intermédiation de la page.

Cette option se traduit de la manière suivante pour les utilisateurs finaux :

- S'il ne s'agit pas d'un utilisateur interne et qu'il se connecte en dehors de la plage d'adresses IP configurée, les droits pour le groupe de pools qui sont configurés comme **Direct Connect uniquement** ne s'affichent pas.
- S'il s'agit d'un utilisateur interne, les droits du groupe de pools qui sont configurés comme **Direct Connect uniquement** sont lancés sans l'intervention d'Unified Access Gateway. D'autres droits sont lancés à l'aide d'Unified Access Gateway.

Pour obtenir des informations complémentaires sur la création de groupes de pools, reportez-vous aux sections Créer un groupe de pools à session unique et Créer un groupe de pools à plusieurs sessions.

Réessayer le provisionnement du pool

Si un provisionnement du pool à une ou plusieurs sessions échoue, il a pu rencontrer une ou plusieurs erreurs pendant le processus de provisionnement. Vous pouvez résoudre les erreurs et réessayer le provisionnement du pool.

Pour obtenir un exemple spécifique d'erreur de provisionnement du pool, reportez-vous à la section Détails du pool dans Horizon Cloud Service - next-gen.

Procédure

1 Connectez-vous à Horizon Universal Console.

2 Cliquez sur **Pools** sur la vignette **Pools**.

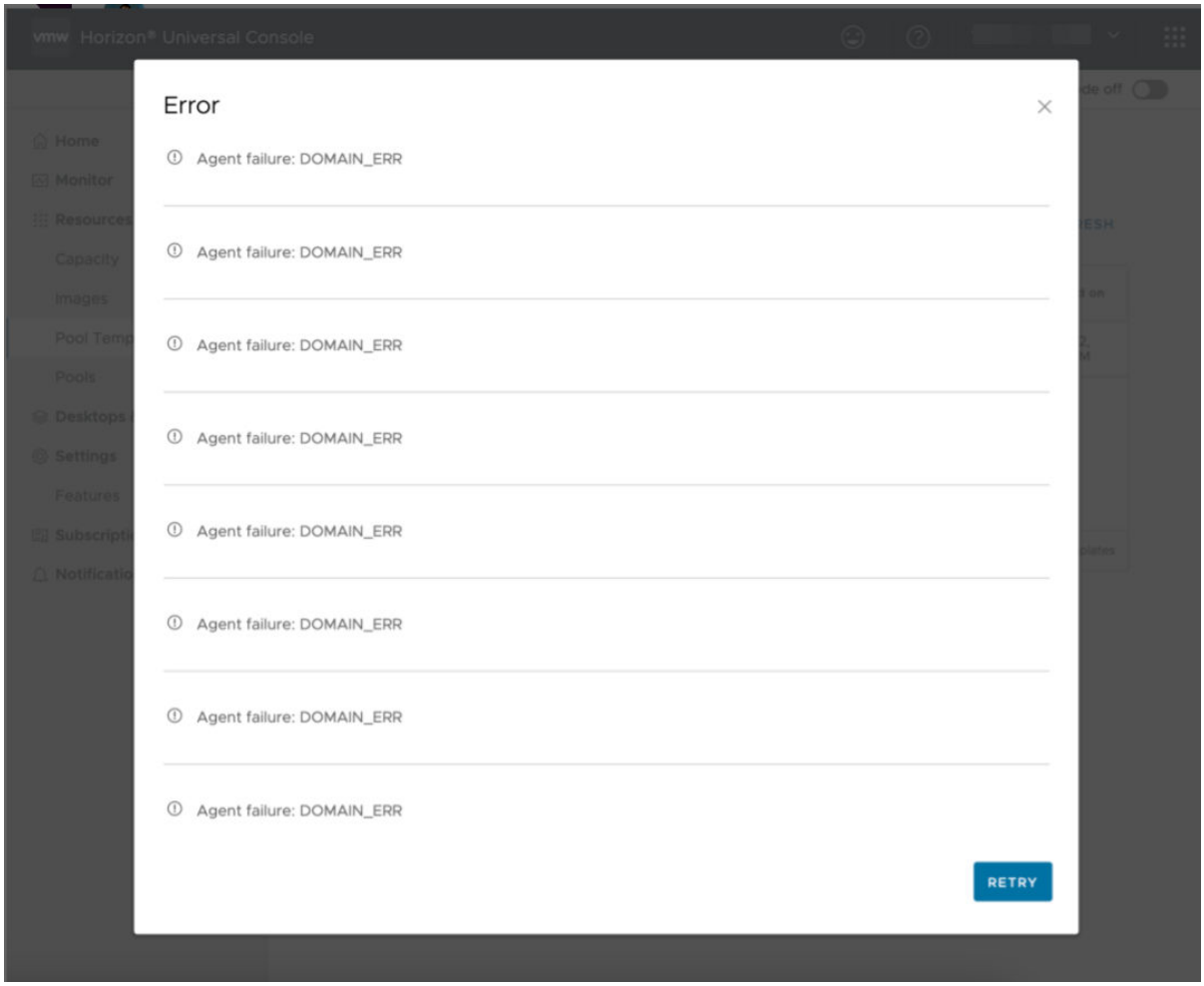
3 Cliquez sur l'info-bulle de l'état **Erreur** du pool ayant échoué sur la page **Pools**.

4 Cliquez sur **Afficher tout** pour afficher la liste complète des erreurs.

Le bouton **Afficher tout** s'affiche s'il y a plus de deux erreurs.

5 Corrigez les erreurs, puis cliquez sur **Réessayer**.

6 Cliquez sur **Afficher les journaux** pour accéder à la page **Journal d'activité**.



Modifier un pool

Modifiez les pools de votre environnement à l'aide de la console Horizon Universal Console.

Note Le système permet de modifier des propriétés spécifiques dans la configuration du pool. Les propriétés que vous pouvez mettre à jour sont décrites dans les étapes ci-dessous. Vous ne pouvez pas changer certaines valeurs configurées lors de la modification du pool après sa création, telles que le nom et le type du pool. Pour obtenir une description des éléments qui peuvent être spécifiés lors de la création du pool, reportez-vous à la section Créer un pool.

Procédure

1 Dans la console Horizon Universal Console, accédez à la page **Pools** en cliquant sur **Ressources > Pools**

2 Dans l'onglet **Pools**, sélectionnez le pool à modifier, puis cliquez sur **Modifier**.

3 Dans la section **Modifier le pool**, vous pouvez mettre à jour la description.

Cette section indique également le type de pool, l'un des types suivants :

- **Session unique dédiée** pour l'expérience de poste de travail VDI persistant dans lequel chaque poste de travail est mappé à un seul utilisateur.
- **Session unique flottante** pour l'expérience de poste de travail VDI non persistant dans laquelle plusieurs utilisateurs peuvent utiliser le poste de travail à des moments différents et le poste de travail se réinitialise après chaque session d'utilisateur.
- **Sessions multiples** pour les applications et postes de travail publiés basés sur une session.

4 Dans la section **Postes de travail**, la sous-section **Destination** affiche les champs **Site**, **Horizon Edge** et **Fournisseur** configurés. Ces valeurs ne sont pas modifiables pour un pool existant.

5 Toujours dans la sous-section **Destination**, si vous souhaitez utiliser des zones de disponibilité Azure, activez l'option **Utiliser les zones de disponibilité Azure**.

Les zones de disponibilité Azure sont une fonctionnalité de haute disponibilité disponible avec Microsoft Azure. Lorsque vous sélectionnez **Utiliser les zones de disponibilité Azure**, les machines virtuelles d'un pool sont réparties sur toutes les zones de disponibilité afin d'éviter les interruptions de service de toutes les machines virtuelles du pool en cas de panne dans une zone de disponibilité Azure donnée.

Note

- Pour plus d'informations sur les limitations de la prise en charge de la zone de disponibilité Azure, reportez-vous à la documentation de Microsoft suivante.
- Sachez que, lorsque vous activez des zones de disponibilité Azure lors de la modification d'un pool, seules les machines virtuelles créées après l'activation sont réparties dans les zones de disponibilité Azure. Les machines virtuelles existantes ne sont pas déplacées.

6 Dans la sous-section **Image**, vous pouvez remplacer l'image du pool par une image différente en sélectionnant les options **Type de génération** et **Image** pour ce pool.

Note

- Les images avec les VM Microsoft Azure de génération 1 et 2 sont prises en charge.
- Si vous sélectionnez **V1**, seules les images avec une VM Microsoft Azure de génération 1 et les modèles prenant en charge la génération 1 peuvent être sélectionnés.
- Votre sélection pour le **Type de génération** agit comme un filtre pour déterminer les images répertoriées dans le menu déroulant **Image** et les modèles répertoriés dans le menu déroulant **Modèle**.

7 Sélectionnez le **Marqueur** de l'image sélectionnée.

Vous devez ajouter un ou plusieurs marqueurs pour modifier ultérieurement les pools d'une version de l'image. Ajoutez les marqueurs s'ils n'ont pas été ajoutés précédemment à la version de l'image. Pour plus d'informations, reportez-vous à la section Ajouter une version à une image de la galerie de calcul Microsoft Azure existante.

Note Si un marqueur associé à une version antérieure de l'agent est sélectionné, un message d'avertissement s'affiche. Il est recommandé de sélectionner un marqueur avec la dernière version de l'agent.

8 Vérifiez que l'option en regard de **Disposez-vous d'une licence valide pour ce système d'exploitation Windows ?** est activée afin de confirmer que vous disposez de licences Windows éligibles avec un abonnement Software Assurance ou Windows Server pour appliquer cet avantage Azure Hybrid Benefit, puis cochez la case de confirmation.

9 Dans la sous-section **Détails de la VM**, sélectionnez des valeurs pour les options **Modèle de filtre**, **Modèle**, **Type de disque**, **Taille du disque** et **Chiffrer les disques** de votre pool.

Note Dans le paramètre **Modèle**, reportez-vous à la section Types et tailles de VM Microsoft Azure pour Horizon Cloud Service - next-gen (89090) pour en savoir plus sur la compatibilité des différents types et des différentes tailles de VM Microsoft Azure avec VMware Horizon Cloud Service - next-gen.

- Vous pouvez utiliser les paramètres **Modèle de filtre** pour réduire le nombre d'options de modèles de VM Microsoft Azure répertoriées lorsque vous configurez le paramètre **Modèle**. La liste réduite inclut un sous-ensemble de modèles en fonction de vos besoins spécifiques.

Vous pouvez filtrer la liste de modèles de VM Microsoft Azure par **Balise**, **Série**, **Type de GPU** et **Type de disque**. Cliquez sur **+** pour ajouter d'autres filtres, en affinant potentiellement davantage la liste avec chaque filtre.

Balise	est égal à	■ L'option **Recommandé par VMware** indique les modèles de VM Microsoft Azure qui fonctionnent particulièrement bien pour les pools. ■ L'option **Haute performance** indique les modèles de VM Microsoft Azure qui proposent un support Premium pour les disques.
Série	est égal à	Utilisez le menu déroulant pour afficher la liste des différentes séries de VM Microsoft Azure. Sélectionnez une série qui répond le mieux à vos besoins.
Type de GPU	est égal à	Vous pouvez utiliser le filtre **Type de GPU** pour sélectionner un modèle de VM Microsoft Azure avec GPU activé. ■ **NONE** permet de filtrer les modèles avec GPU activé de la liste. ■ **AMD** n'inclut que les modèles avec GPU AMD activé dans la liste. ■ **NVIDIA** n'inclut que les modèles avec GPU NVIDIA activé dans la liste.
Type de disque	est égal à	Vous pouvez utiliser le filtre **Type de disque** pour sélectionner **Premium**, qui fournit un support Premium pour les disques.

- Sélectionnez un type de **Modèle** de VM Microsoft Azure à utiliser pour le pool ou acceptez la valeur par défaut.

  1 Pour accepter un modèle par défaut, acceptez celui qui est répertorié ou utilisez le menu déroulant pour en sélectionner un autre.

  2 Pour sélectionner un autre modèle, cliquez sur X, puis cliquez sur le menu déroulant et sélectionnez un modèle.

  Si vous n'avez pas utilisé le paramètre **Modèle de filtre**, la liste de modèles est très longue. Si vous avez utilisé le paramètre **Modèle de filtre**, la liste sera probablement plus gérable.

- Vous pouvez sélectionner l'option **Type de disque** en fonction du modèle de VM sélectionné, ainsi que de la région et de l'abonnement Microsoft Azure.
- Vous pouvez passer la valeur **Taille du disque** de 127 à 4 095 Go. La valeur **Taille du disque** par défaut est de 127.
- Si vous souhaitez chiffrer les disques de toutes les VM de ce pool, faites glisser la bascule sur **Chiffrer les disques**.

10 Dans la sous-section **Identité de machine (Domaine)**, l'identité de la machine configurée du pool s'affiche.

Si ce pool existant est configuré pour utiliser votre domaine Active Directory local, vous pouvez éventuellement modifier l'unité d'organisation que le pool utilise pour les identités de la machine.

Note Pour éviter les conflits de noms, lorsque le pool réutilise des noms de VM, vous ne pouvez pas modifier la valeur du champ **Unité d'organisation de l'ordinateur**. L'état affiché de l'option **Réutiliser les noms de VM** dans la sous-section Propriétés indique si le pool réutilise ou non des noms de VM.

11 Dans la sous-section **Provisionnement**, mettez à jour les paramètres si nécessaire et comme vous le souhaitez.

a Si le provisionnement du pool est désactivé, vous pouvez cliquer sur **Activer** pour le réactiver.

Cette option n'est disponible que lorsque le provisionnement du pool a été précédemment désactivé pour ce pool, ce qui peut être effectué avec les sélections **Provisionnement > Désactiver** ou **Provisionnement > Annuler**.

b Vous pouvez modifier votre sélection du mode de provisionnement des VM dans la sous-section Provisionner des VM, entre **À la demande** et **Tout à la fois**.

c Vous pouvez modifier le **Nombre maximal de VM** pouvant être provisionnées pour ce pool.

d Si l'option **À la demande** est sélectionnée, vous pouvez modifier le **Nombre minimal de VM de rechange** et le **Nombre maximal de VM de rechange**.

12 Dans la sous-section **Propriétés**, vous pouvez mettre à jour les éléments suivants lors de la modification d'un pool existant :

- **Utiliser le proxy sortant** : pour acheminer les demandes sortantes vers Internet via un serveur proxy, activez cette option et spécifiez les valeurs de l'hôte proxy, du port du proxy et éventuellement des adresses IP de contournement du proxy (pour les adresses IP pour lesquelles le proxy sortant ne sera pas appliqué).

13 Passez à la section suivante en cliquant sur **Suivant**.

14 Dans la sous-section **Réseaux**, sélectionnez les réseaux virtuels et les sous-réseaux de locataire (poste de travail).

Note L'option de double pile n'est pas modifiable lorsque vous modifiez un pool.

15 Dans la sous-section **VMware Dynamic Environment Manager**, vous pouvez éventuellement sélectionner une configuration VMware Dynamic Environment Manager pour ce pool.

Redimensionner les postes de travail virtuels

Vous pouvez redimensionner des postes de travail virtuels individuels en modifiant le type et la taille de VM Azure sur les postes de travail déjà créés et déployés qui se trouvent dans une attribution de poste de travail dédié.

Procédure

1. Connectez-vous à VMware Horizon® Cloud Service™ - next-gen.
2. Sur la page **Accueil**, cliquez sur **Pools**.
3. Sur la page **Pools**, cliquez sur **VM** d'un **Pool** dans un **Pool dédié**.
4. Sélectionnez une ou plusieurs **VM** dans un **État Hors tension** et provisionné. Cliquez sur **Modifier**.
5. Sélectionnez un **Modèle** de VM dans le menu déroulant.
6. Dans l'écran **Modifier les VM**, sélectionnez un **Type de disque** dans le menu déroulant.

   Les options de **Type de disque** sont basées sur le modèle de VM sélectionné, votre abonnement Microsoft Azure et votre région.
7. Modifiez la **Taille du disque**. Les tailles de disque comprises entre 127 et 4 095 Go sont autorisées. La taille du disque par défaut est de 127. Cliquez sur **Enregistrer**.

Gestion de l'alimentation et équilibrage de charge de VM à sessions multiples dans un pool

Horizon Cloud Service - next-gen utilise un indice de charge de l'agent, basé sur vos paramètres d'équilibrage de charge, pour la gestion de l'alimentation et l'équilibrage de charge des VM à sessions multiples dans un pool.

Les agents Horizon Cloud Service - next-gen utilisent les paramètres de seuil suivants pour calculer l'indice de charge de l'agent. La valeur de l'indice est comprise entre 0 et 100, et est utilisée pour mesurer la charge sur chaque VM. Configurez ces paramètres à l'aide de stratégies de groupes de pools.

- **Seuil d'utilisation du CPU**
- **Seuil d'utilisation de la mémoire**
- **Seuil de longueur de file d'attente de disque**
- **Seuil de latence de lecture du disque**
- **Seuil de latence d'écriture du disque**

En raison du rôle essentiel que joue l'indice de charge de l'agent dans la gestion de l'alimentation et l'équilibrage de charge, sélectionnez les valeurs appropriées pour atteindre l'équilibre souhaité entre la consommation d'énergie et les performances.

Détermination par le système de l'utilisation de VM dans un pool

Le système détermine l'utilisation de VM dans un pool spécifique en sélectionnant la plus élevée des deux valeurs de pourcentage suivantes :

- Occupation de session

  Nombre de sessions actives dans un pool divisé par le nombre total de sessions possibles sur les VM sous tension dans le pool. Le nombre de sessions possibles est calculé en multipliant le nombre de VM sous tension dans le pool par la valeur Sessions par VM que vous avez spécifiée pour le pool.

- Indice de charge moyen

  Indice de charge moyen de l'agent, comme décrit ci-dessus, des VM sous tension dans le pool.

Pour l'extension du pool, le système compare ensuite la valeur d'indice de charge moyenne sélectionnée au seuil élevé spécifié pour le paramètre de gestion de l'alimentation.

Pour que l'extension se produise, le paramètre Nombre maximal de VM doit être supérieur à 1.

Dans les deux exemples suivants, le paramètre Gestion de l'alimentation est Performances optimisées. Le seuil élevé du paramètre Performances optimisées est de 50 %, ce qui signifie que lorsque l'utilisation atteint 50 %, le système met l'une des machines virtuelles inutilisées sous tension.

Exemple : extension du pool en raison d'une occupation de session supérieure au seuil élevé

Dans cet exemple, les paramètres suivants sont utilisés :

- Sessions par VM = 20
- Seuil élevé de gestion de l'alimentation = 50 %

Avant l'extension	Après l'extension
VM sous tension VM 1 ■ Sessions en cours d'exécution = 10 ■ Indice de charge de l'agent = 25 % **Valeurs d'utilisation** ■ Occupation de session = 10 sessions en cours d'exécution /(20 sessions par machine virtuelle x 1 VM) = 50 % ■ Indice de charge moyen = indice de charge de l'agent 25 % /1 VM = 25 % La plus grande des deux valeurs est de 50 %, ce qui correspond au seuil élevé pour le paramètre Performances optimisées pour la gestion de l'alimentation. Par conséquent, le système met sous tension une deuxième machine virtuelle.	**VM sous tension** VM 1 ■ Sessions en cours d'exécution = 10 ■ Indice de charge de l'agent = 25 % VM 2 ■ Sessions en cours d'exécution = 0 ■ Indice de charge de l'agent = 0 % **Valeurs d'utilisation** ■ Occupation de session = (sessions en cours d'exécution 10 + 0) /(20 sessions par VM x 2 VM) = 25 % ■ Indice de charge moyen = (indice de charge de l'agent 25 % + 0 %) /2 VM = 12,5 % La plus grande des deux valeurs est de 25 %, ce qui est inférieur au seuil élevé pour le paramètre Performances optimisées pour la gestion de l'alimentation. Par conséquent, le système n'effectue aucune action.

Exemple : extension du pool en raison d'un indice de charge moyen dépassant le seuil élevé

Dans cet exemple, les paramètres suivants sont utilisés :

- Sessions par VM = 20
- Seuil élevé de gestion de l'alimentation = 50 %

Avant l'extension	Après l'extension
VM sous tension VM 1 ■ Sessions en cours d'exécution = 5 ■ Indice de charge de l'agent = 50 % **Valeurs d'utilisation** ■ Occupation de session = 5 sessions en cours d'exécution /(20 sessions par VM x 1 VM) = 25 % ■ Indice de charge moyen = indice de charge de l'agent 50 % /1 VM = 50 % La plus grande des deux valeurs est de 50 %, ce qui correspond au seuil élevé pour le paramètre Performances optimisées pour la gestion de l'alimentation. Par conséquent, le système met sous tension une deuxième machine virtuelle.	**VM sous tension** VM 1 ■ Sessions en cours d'exécution = 5 ■ Indice de charge de l'agent = 50 % VM 2 ■ Sessions en cours d'exécution = 0 ■ Indice de charge de l'agent = 0 % **Valeurs d'utilisation** ■ Occupation de session = (sessions en cours d'exécution 5 + 0) /(20 sessions par VM x 2 VM) = 12,5 % ■ Indice de charge moyen = (indice de charge de l'agent 50 % + 0 %) /2 VM = 25 % La plus grande des deux valeurs est de 25 %, ce qui est inférieur au seuil élevé pour le paramètre Performances optimisées pour la gestion de l'alimentation. Par conséquent, le système n'effectue aucune action.

Détails du pool dans Horizon Cloud Service - next-gen

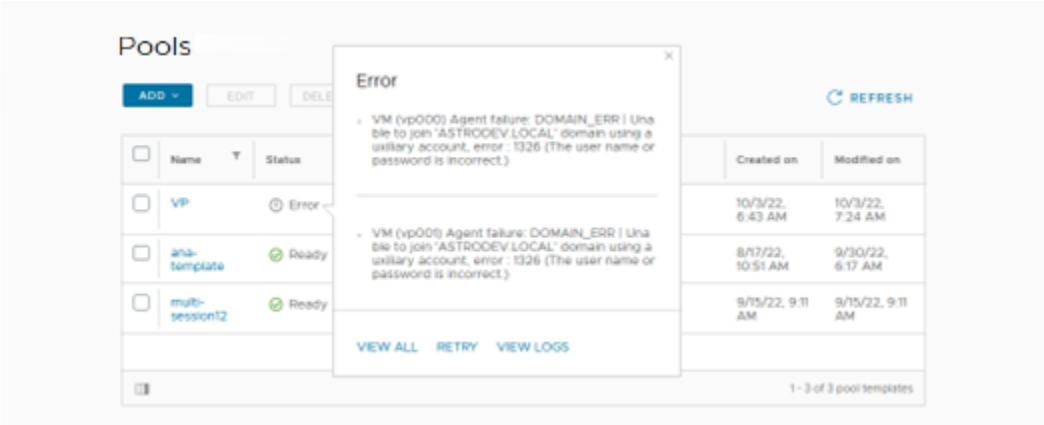
Vous pouvez afficher et vérifier les détails d'un ou de plusieurs pools sur la page Résumé du pool dans Horizon Cloud Service - next-gen.

Procédure

1 Connectez-vous à Horizon Universal Console.

2 Sur la page Accueil, cliquez sur **Pools** sur la vignette **Pools**.

a Si des pools affichent une erreur, cliquez sur **Erreur** pour afficher l'erreur et la résoudre.



b Si vous constatez une erreur commençant par `Anomaly detected for template`, supprimez les ressources indésirables, consultez l'article 90261 de la base de connaissances, puis cliquez sur **Réessayer**.

Lorsqu'une nouvelle tentative réussit, la VM passe à un état **Extension**, **Réduction** ou **Prêt**.

Pour plus d'informations sur le provisionnement du pool, reportez-vous à la section Réessayer le provisionnement du pool.

3 Cliquez sur un lien **Pools Nom** pour accéder à la page de détails des **Pools**.

4 Cliquez sur **Présentation** pour afficher les options **Capacité**, **Sessions**, **Paramètres généraux** et **Provisionnement**. Sur la page **Présentation**, vous pouvez afficher **Capacité de session**, c'est-à-dire **Maximum**, **Provisionné** et **En cours d'utilisation**. Vous pouvez également afficher les **Sessions en cours d'utilisation Connectées** et **Déconnectées**.

Vous pouvez également cliquer sur **Modifier** ou sur **Supprimer** les **Pools** sur la page de détails des **Pools**.

5 Dans les onglets **VM**, **Sessions** et **Activité de l'administrateur**, cliquez sur **Gérer les colonnes** pour sélectionner les colonnes qui ne s'affichent pas dans le tableau par défaut, telles que la colonne **ID de zone de disponibilité** et la colonne **Adresse IPv6**.

   Par exemple, dans l'onglet **VM**, utilisez l'option **Gérer les colonnes** et sélectionnez **ID de zone de disponibilité** pour ajouter cette colonne à la liste des machines virtuelles. La colonne **ID de zone de disponibilité** répertorie la zone de disponibilité Azure pour chaque machine virtuelle de la liste. Vous pouvez ensuite voir comment les machines virtuelles d'un pool sont réparties dans les zones de disponibilité Azure.

   Pour plus d'informations sur les limitations de la prise en charge de la zone de disponibilité Azure, reportez-vous à la documentation de Microsoft suivante.

6 Cliquez sur **VM** pour afficher la liste des **VM**.

   Ne **mettez pas hors tension** ni ne **mettez sous tension** une VM en dehors de la console Horizon Universal Console via le portail Microsoft Azure ou via l'arrêt du SE invité. Si vous le faites, l'état interne est mis à jour pour refléter le dernier état de la VM, tel qu'il s'affiche sur le portail Microsoft Azure. Cette mise à jour peut prendre entre 10 et 15 minutes. En outre, si une VM est arrêtée en externe, mais pas désallouée, le système la désalloue pour réduire les coûts. Les actions de synchronisation s'affichent dans **Journaux d'activité** comme **Activité système**.

7 Cliquez sur le **menu déroulant** pour sélectionner un pool. Le menu déroulant répertorie le pool principal et tous les pools d'extension du pool principal.

8 Cliquez sur **Sessions** pour afficher la liste des **Sessions**.

9 Dans l'onglet **Sessions**, cliquez sur les trois points d'une ligne pour **fermer** une session.

10 Cliquez sur **Activité de l'administrateur** pour afficher des détails sur les activités initiées par les administrateurs sur le pool sélectionné.

11 Dans l'onglet **Activité de l'administrateur**, cliquez sur **Exporter** pour exporter un journal de l'activité initiée par les administrateurs sur le pool sélectionné.

   Le journal inclut l'activité de l'administrateur pendant une période que vous spécifiez, comprise entre 1 et 90 jours. Le journal fournit des détails sur chaque événement admin-activity, par exemple l'initiateur et la date de l'événement.

Détails du groupe de pools dans Horizon Cloud Service - next-gen

Vous pouvez afficher et vérifier les détails d'un ou de plusieurs pools sur la page Résumé des pools.

Procédure

1 Connectez-vous à Horizon Universal Console.

2 Cliquez sur la vignette **Groupes de pools** de la page **Accueil**.

3 Cliquez sur un lien **Groupe de pools Nom** sur la page **Groupe de pools**, pour accéder à la page Détails du pool.

4 Cliquez sur **Présentation** pour afficher **Capacité de session**, **Sessions en cours d'utilisation**, **Stratégies**, **Gestion de l'alimentation** et **Traitement du délai d'expiration**.

5 Cliquez sur **Pools** pour afficher la liste des **Pools**.

6 Cliquez sur **Applications** pour afficher la liste des **Applications**.

   Pour les groupes de pools flottants, cliquez sur **Applications App Volumes** pour afficher la liste des applications App Volumes ajoutées au groupe de pools flottants. Vous pouvez **ajouter** des applications App Volumes au groupe de pools flottants existant et les **supprimer** de ce dernier. L'onglet **Applications** s'applique uniquement aux types d'applications publiées et de groupes de pools d'applications et de postes de travail publiés.

7 Cliquez sur **Droits** pour afficher la liste des **Droits**.

8 Cliquez sur **Sessions** pour afficher la liste des **Sessions**.

   Horizon Cloud Service - next-gen prend en charge la distribution d'applications Windows 10 multisession uniques pour chaque session d'utilisateur.

9 Cliquez sur les trois points consécutifs pour **fermer** une session.

Gestion des utilisateurs Admin et des licences pour votre environnement Horizon Cloud Service - next-gen

Cette page de documentation fournit des liens vers les pages pratiques sur l'ajout d'utilisateurs Admin, leur attribution de rôles et la gestion de vos licences.

Attribution de rôles administratifs aux utilisateurs Horizon Universal Console

Vous pouvez créer des utilisateurs administratifs Horizon Cloud et leur attribuer des rôles. Les rôles fournissent aux utilisateurs administratifs des autorisations d'accès spécifiées à Horizon Universal Console, telles que l'affichage d'informations spécifiques ou la prise de mesures spécifiques.

Rôles d'administration pour Horizon Universal Console

Chaque rôle accorde des autorisations de création, de lecture, de mise à jour et de suppression pour la zone spécifiée et des autorisations de lecture uniquement pour les éléments restants.

Rôles	Zone d'autorisations
Administrateur	Accès à l'ensemble de l'interface utilisateur et de l'API.
Administrateur en lecture seule	Accès en lecture seule à l'interface utilisateur et à l'API
Administrateur de pools	pools et VM
Administrateur de déploiements	Dispositifs Dispositifs Horizon Edge, instances d'Unified Access Gateway et fournisseurs
Administrateur du groupe de pools	Groupes de pools

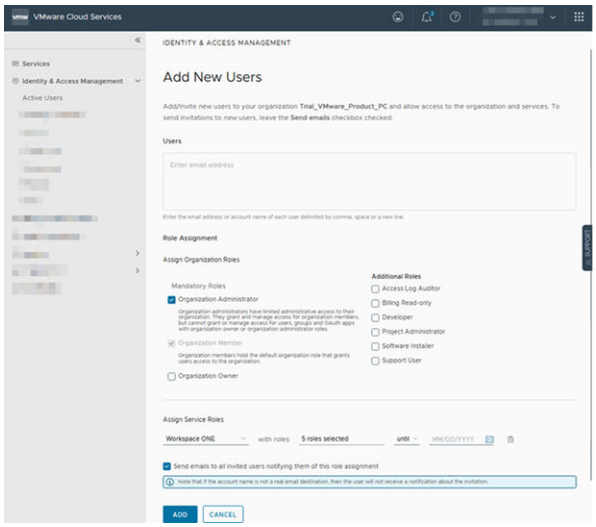
Rôles	Zone d'autorisations
Administrateur de droits	Droits
Administrateur d'images	Images

Ajouter des utilisateurs Horizon Universal Console et attribuer des rôles

Pour fournir aux utilisateurs administratifs des droits d'accès à Horizon Universal Console, utilisez la console VMware Console Cloud Services pour leur attribuer d'abord un rôle d'organisation. Vous pouvez ensuite attribuer des rôles d'Horizon Cloud Services à ces utilisateurs.

Cette tâche nécessite l'accès à Console Cloud Services. Pour ajouter de nouveaux utilisateurs, vous devez être propriétaire ou administrateur de l'organisation.

Note Pour plus d'informations sur les VMware Cloud™ Services, reportez-vous à la documentation du produit VMware Cloud Services. D'autres noms de VMware Cloud services s'affichent dans la documentation et les produits VMware, par exemple « Plate-forme VMware Cloud Services » (CSP) et « Plate-forme d'engagement de VMware Cloud Services ».



Procédure

1 Connectez-vous à Console Cloud Services.

2 Dans le menu de gauche, sélectionnez **Gestion des identités et des accès > Utilisateurs actifs**.

Note Le nœud **Gestion des identités et des accès** n'est disponible que pour les propriétaires et administrateurs d'organisations.

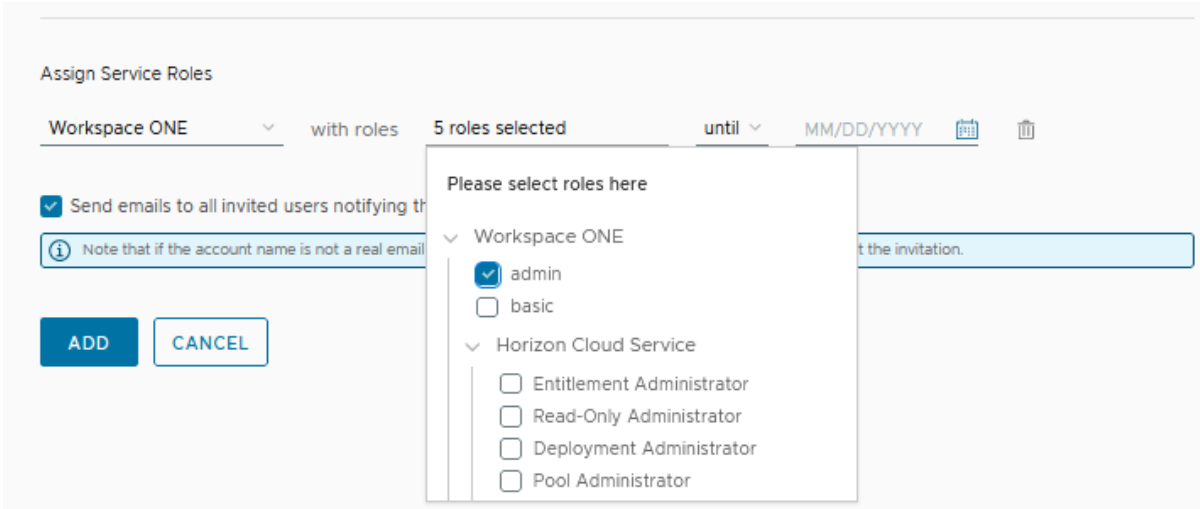
3 Sélectionnez **Utilisateurs actifs > Ajouter des utilisateurs**.

4 Dans la zone de texte **Utilisateurs**, ajoutez les adresses e-mail des personnes auxquelles vous souhaitez attribuer des rôles administratifs.

5 Sélectionnez un rôle d'organisation pour les utilisateurs que vous avez ajoutés.

Les propriétaires et administrateurs d'organisations peuvent utiliser la Console Cloud Services pour ajouter et modifier des utilisateurs.

6 Cliquez sur **Ajouter un service** et, si nécessaire, sélectionnez Workspace ONE.



7 Cliquez sur la zone de texte **avec des rôles** pour afficher la liste des rôles disponibles. Si vous le souhaitez, sélectionnez des rôles supplémentaires.

8 Dans le menu déroulant suivant, sélectionnez **avec** ou **jusqu'à**, selon que vous souhaitez définir les autorisations pour qu'elles expirent à un moment donné.

9 Dans le champ suivant, le cas échéant, indiquez une date d'expiration.

10 Cliquez sur **Ajouter**.

Résultats

Les utilisateurs que vous avez ajoutés ont désormais accès à Horizon Universal Console avec les autorisations que vous leur avez accordées.

Autres actions que vous pouvez effectuer sur la page Utilisateurs actifs

Après avoir utilisé la Console Cloud Services pour ajouter des utilisateurs, vous pouvez effectuer plusieurs autres actions sur la page Utilisateurs actifs.

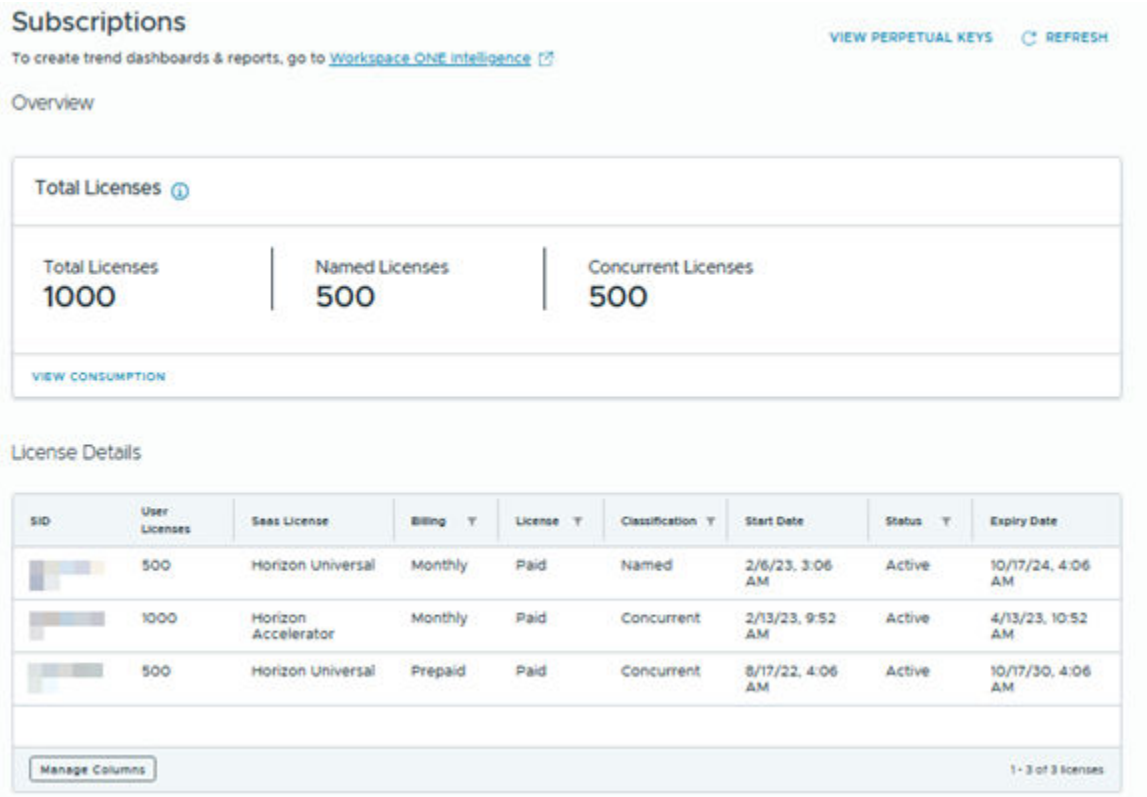
Vous pouvez effectuer les actions suivantes dont la plupart sont identiques ou semblables aux étapes de configuration du test initial d'Horizon Availability Monitoring.

Action	Description
Recherchez la liste des utilisateurs actifs.	Entrez une chaîne de texte dans la zone de texte **Rechercher** pour rechercher la liste des utilisateurs actifs.
Affichez les informations liées au rôle d'un utilisateur actif sélectionné.	Cliquez sur la flèche à deux pointes en regard du nom d'un utilisateur actif pour afficher les informations suivantes. ■ Rôle d'organisation de cet utilisateur, tel qu'Administrateur de l'organisation, Propriétaire de l'organisation et Membre de l'organisation. ■ Les services de cet utilisateur, tels que Horizon Cloud Service, et les rôles attribués à l'utilisateur pour ce service, tels qu'Administrateur d'images et Administrateur d'inventaires.
Modifiez le rôle d'un utilisateur.	Sélectionnez un utilisateur et cliquez sur **Modifier les rôles**. La modification des rôles est très semblable à la procédure d'ajout de rôles décrite précédemment.
Supprimez les utilisateurs.	Sélectionnez un ou plusieurs utilisateurs et cliquez sur **Supprimer les utilisateurs**.

Utiliser Horizon Universal Console pour suivre vos licences Horizon

L'objectif de la page Abonnements est d'aider les administrateurs à déterminer rapidement l'état de leurs licences d'abonnement Horizon.

Pour afficher vos licences d'abonnement Horizon, cliquez sur **Abonnements** dans le menu de gauche.



Les détails suivants s'appliquent à la page Abonnements.

- Vous pouvez consulter le nombre de licences dont dispose votre déploiement dans la section Nombre total de licences. La section répertorie le nombre total de licences et le nombre de licences par classification. Reportez-vous aux informations suivantes concernant les classifications des licences.
- Vous pouvez modifier la manière dont la page présente les détails de la licence en utilisant les flèches de tri ou les filtres disponibles sur la page. Par exemple, dans l'en-tête du tableau, vous pouvez utiliser des filtres pour les colonnes **Classification** (**Simultané** ou **Nommé**) et **État**, entre autres. Vous pouvez également utiliser des flèches de tri pour les colonnes **Date de début** et **Date d'expiration**, entre autres.
- SID

  ID de l'instance de service

  Identifiant unique généré pour chaque abonnement
- Facturation : les types de facturation de licence sont les suivants.

  Payée

  Une facture a été payée au début de la licence.

  Mensuelle

  Une facture est émise chaque mois de la licence.

  Essai

  Aucune facture, car il s'agit d'une licence d'essai
- Classification : les classifications du modèle d'utilisation de licence sont les suivantes.

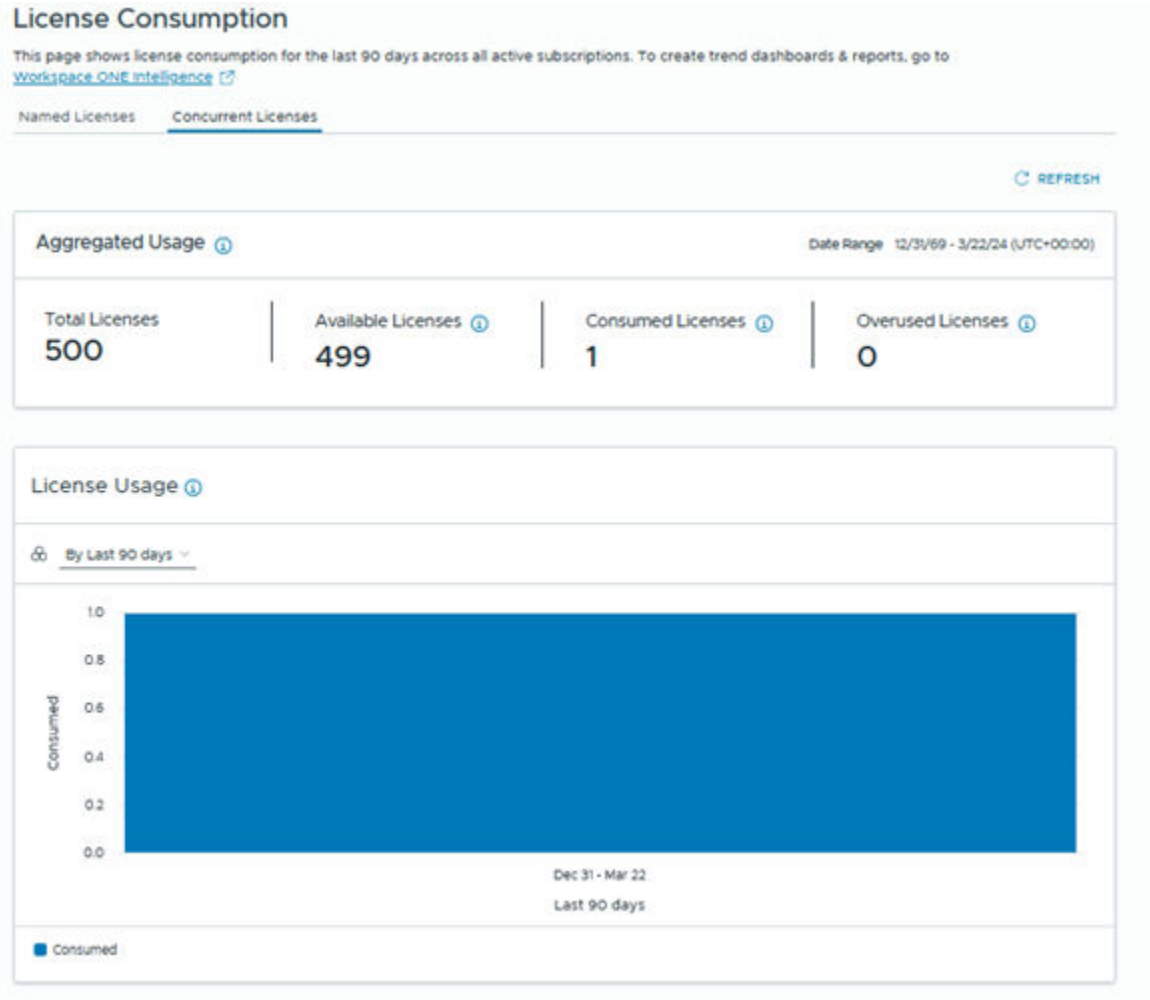
  Important Actuellement, les mesures de consommation des licences sont disponibles uniquement pour les déploiements de Microsoft Azure en mode natif. Les mesures de consommation ne sont actuellement pas disponibles pour les déploiements d'Horizon 8.

  Pour afficher les détails de consommation des licences, cliquez sur **Afficher la consommation**. Sur la page Consommation des licences, des onglets sont disponibles pour les types de licences auxquels vous êtes abonné. Par conséquent, vous pouvez afficher l'onglet **Licences simultanées**, l'onglet **Licences nommées** ou les deux.

  Licences simultanées

Correspond à une licence qui suit le nombre total d'utilisateurs finaux qui accèdent au logiciel ou l'utilisent à un moment donné pour maintenir une connexion active ou inactive à leurs postes de travail ou à leurs applications à partir d'un périphérique de point de terminaison. Reportez-vous aux exemples suivants.

- Un utilisateur simultané exécutant simultanément trois postes de travail via trois périphériques de point de terminaison différents est compté trois fois, une fois pour chacune des sessions des trois postes de travail connectés simultanément.
- Un utilisateur simultané exécutant simultanément trois postes de travail via le même périphérique de point de terminaison et le même client n'est compté qu'une seule fois.



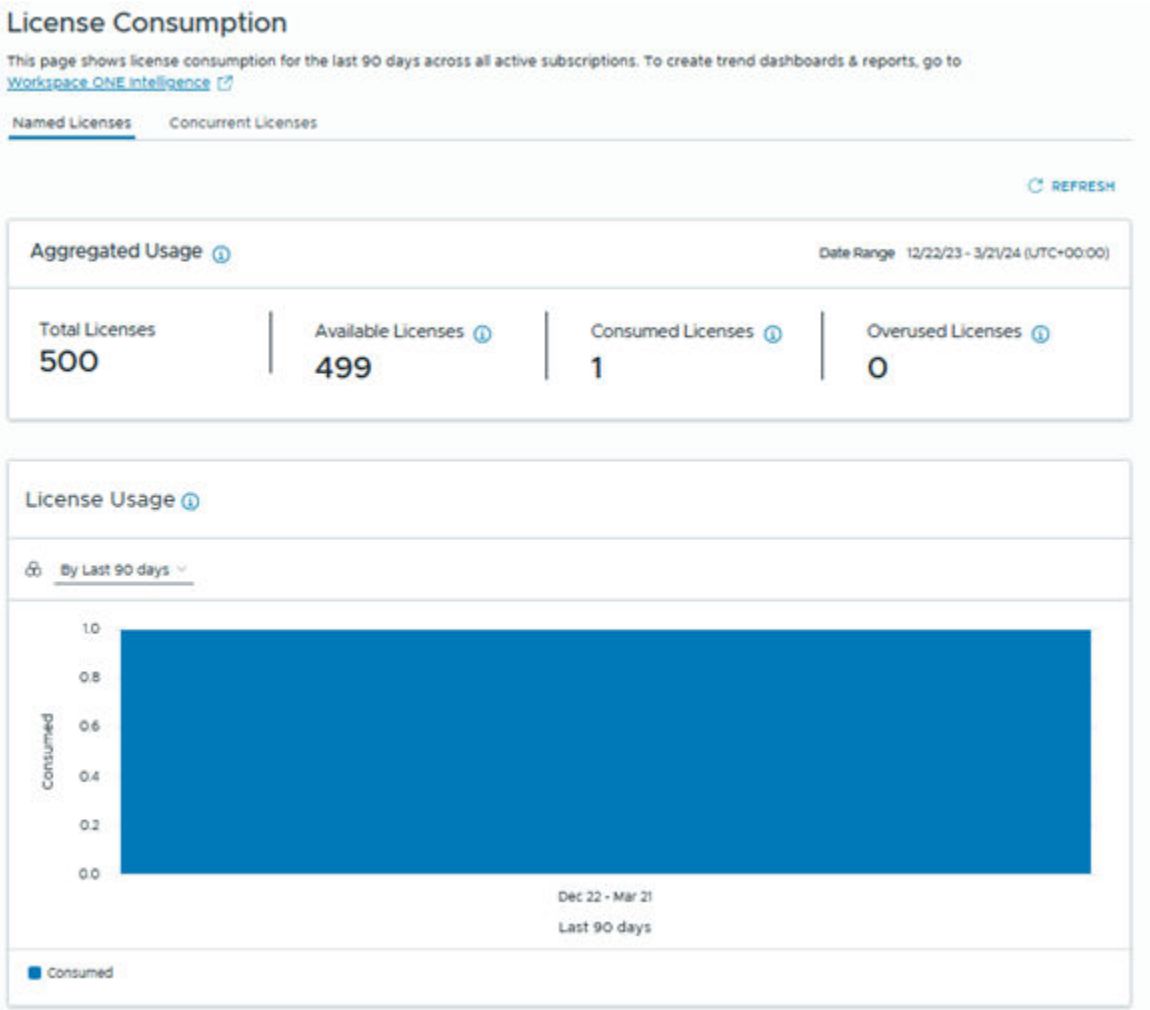
Note Cliquez sur **Actualiser** pour mettre à jour les statistiques d'utilisation maximale.

La page Licences simultanées affiche des informations sur vos licences simultanées, telles que le nombre total de licences simultanées disponibles et les statistiques d'utilisation maximale. Ces dernières indiquent le nombre le plus élevé de licences simultanées en cours d'utilisation pendant des périodes spécifiques.

Par défaut, le système affiche les détails de l'utilisation des licences **Par les 90 derniers jours** avec l'option permettant d'afficher les détails d'utilisation **Par mois** ou **Par les 7 derniers jours**.

Licences nommées

Il s'agit d'une licence qui suit les utilisateurs finaux uniques qui ont accédé au logiciel ou qui l'ont utilisé pour se connecter à leurs postes de travail ou applications. VMware Horizon Cloud Service - next-gen compte le nombre d'utilisateurs finaux uniques qui ont lancé une session au cours des 90 derniers jours depuis hier. Un utilisateur unique accédant à plusieurs postes de travail et applications est compté une seule fois.



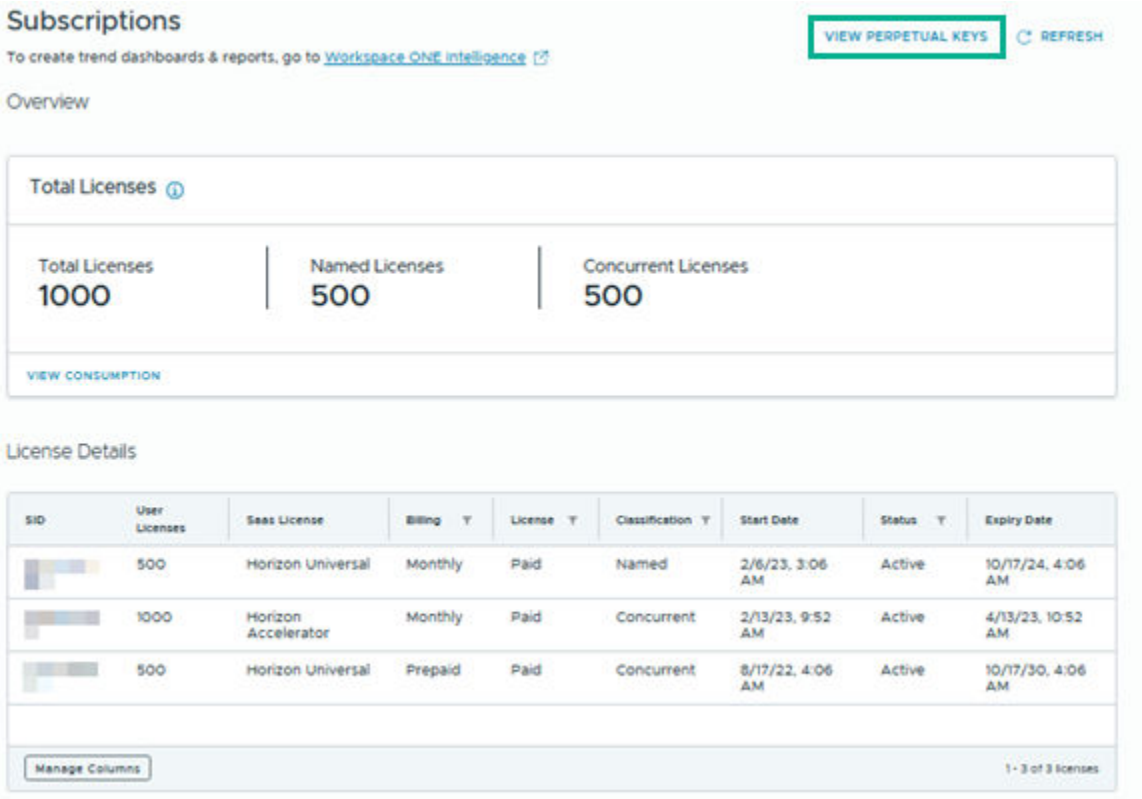
Par défaut, le système affiche les détails de l'utilisation des licences **Par les 90 derniers jours** avec l'option permettant d'afficher les détails d'utilisation **Par mois** ou **Par les 7 derniers jours**.

Utiliser Horizon Universal Console pour obtenir des clés d'infrastructure d'entreprise

Cette page de documentation décrit comment Horizon Universal Console vous permet d'obtenir des clés de licence pour les produits d'infrastructure d'entreprise VMware.

Si votre abonnement Horizon Cloud inclut des produits VMware de base tels que vSphere, vSAN, vCenter, ThinApp Client, ThinApp Virtual Packager, App Volumes Enterprise et Workstation, et que vous vous connectez à Horizon Universal Console avec le rôle Administrateur, la console fournit un lien pour afficher les clés de licence de l'infrastructure d'entreprise sur la page Abonnement de la console.

Si vous ne respectez pas les exigences précédentes, la console n'affiche pas le lien **Afficher les clés perpétuelles**.



Génération d'une clé

En cliquant sur **Afficher les clés perpétuelles**, l'écran Clés de licence de l'infrastructure d'entreprise s'affiche, ce qui vous permet de générer et d'afficher les clés de licence de l'infrastructure d'entreprise. Pour générer les clés de licence, vous devez répondre aux exigences suivantes.

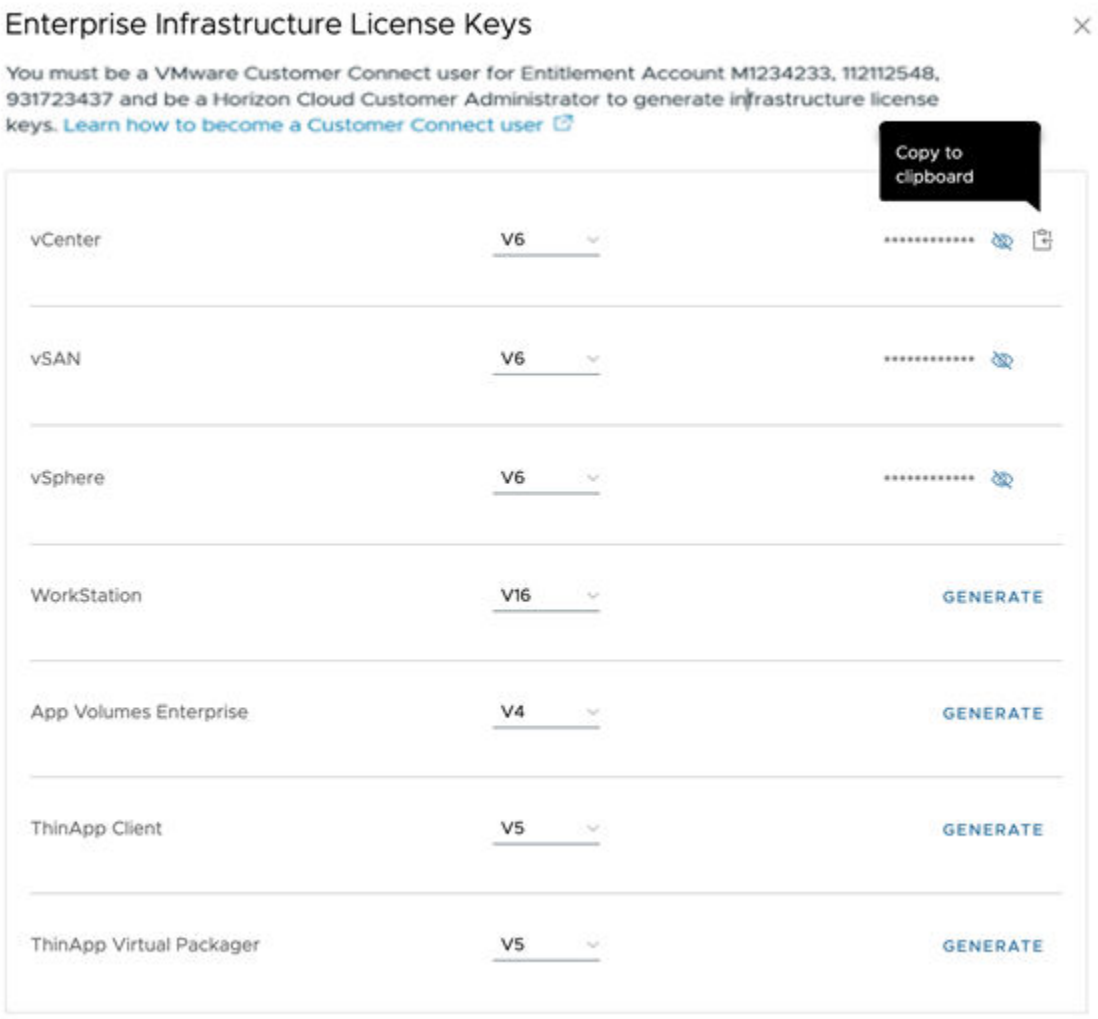
- Disposer du rôle d'administrateur
- Être un utilisateur VMware Customer Connect

Pour générer une clé de licence pour un produit spécifique, dans l'écran Clés de licence de l'infrastructure d'entreprise, sélectionnez une version dans le menu déroulant de ce produit, puis cliquez sur **Générer**. La clé de ce produit s'affiche.

Affichage ou copie d'une clé

Lorsque vous cliquez sur **Afficher les clés perpétuelles**, l'écran Clés de licence de l'infrastructure d'entreprise s'affiche, ce qui vous permet d'afficher les clés de licence de l'infrastructure d'entreprise générées précédemment. Pour afficher les clés de licence, vous devez disposer du rôle Administrateur ou Administrateur en lecture seule.

Pour afficher une clé générée, cliquez sur l'icône en forme d'œil en regard de la clé de licence. Pour copier une clé générée, cliquez sur l'icône **Copier** en regard de la clé de licence.



Mettre à niveau votre passerelle Horizon 8 Edge vers une nouvelle version à l'aide d'Horizon Cloud Service - next-gen Universal Console

Si une version plus récente est disponible pour votre passerelle Horizon 8 Edge déployée, vous pouvez effectuer une mise à niveau manuelle vers la nouvelle version en suivant une séquence d'étapes indiquées dans Horizon Cloud Service - next-gen Universal Console.

Vous pouvez déterminer si une nouvelle version est disponible pour une passerelle Horizon 8 Edge déployée et utiliser une séquence d'étapes décrites dans la section **Capacité** d'Horizon Universal Console pour effectuer une mise à niveau vers cette nouvelle version.

Ce workflow est disponible pour les dispositifs Edge Horizon View non fédérés.

Note Si le dispositif Edge à mettre à niveau est connecté, désactivez l'ancienne VM sur laquelle le dispositif Edge est déployé, puis procédez à la mise à niveau comme décrit ci-dessous. Si la mise à niveau réussit, vous pouvez ignorer la VM de version antérieure. Si la mise à niveau échoue, recommencez la mise à niveau lorsque vous y êtes invité. Si vous ne souhaitez pas réessayer, remettez la VM sous tension pour que le dispositif Edge soit à nouveau actif et qu'aucune donnée ne soit perdue.

Procédure

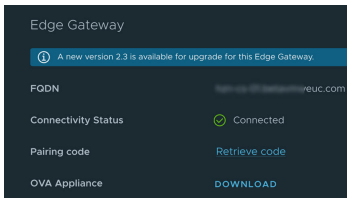
Effectuez une mise à niveau vers une nouvelle version de la passerelle Horizon 8 Edge à l'aide de cette procédure.

1 Connectez-vous à Horizon Cloud Service - next-gen et, sur la page Horizon Universal Console, cliquez sur **Capacité** dans le volet de navigation de gauche.

2 Sur la page **Capacité** résultante, cliquez sur l'onglet **Résumé** et vérifiez les informations du dispositif Edge sélectionné, en particulier les informations de la zone **Passerelle Edge** de la page.

Tous les dispositifs Edge disponibles pour la mise à niveau sont répertoriés dans l'onglet **Maintenance** de la section **Mises à niveau disponibles**. Les informations de mise à niveau sont également disponibles sur la page de détails de chaque dispositif Edge individuel.

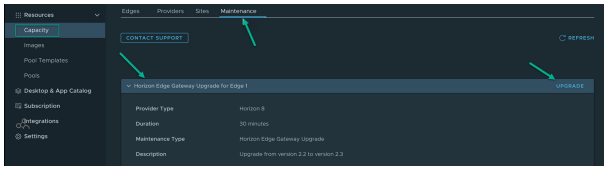
Si une nouvelle version de la passerelle Edge est disponible, un message indiquant `A new version n.n is available for upgrade for this Edge Gateway.` s'affiche dans la zone Passerelle Edge de la page.



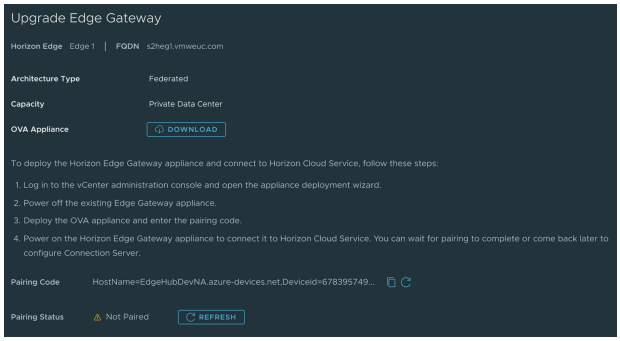
3 Pour l'option **Code de couplage**, cliquez sur **Récupérer le code**. Copiez et collez pour enregistrer le code récupéré à un endroit sûr en vue d'une récupération ultérieure. Vous aurez besoin de ce code de couplage à l'étape suivante.

4 Pour l'option **Dispositif OVA**, cliquez sur **Télécharger**. Notez le nom et l'emplacement du téléchargement du fichier OVA pour les récupérer ultérieurement. Vous aurez besoin de ce dispositif OVA à une étape ultérieure.

5 Pour procéder à la mise à niveau de la passerelle Edge spécifiée, cliquez sur l'onglet **Maintenance** de la page **Capacité**, puis cliquez sur **Mettre à niveau** pour la passerelle Edge spécifiée.



6 Suivez les instructions à l'écran pour accéder au dispositif OVA, déployer le dispositif de passerelle Edge et vous connecter à Horizon Cloud Service - next-gen, comme indiqué dans l'exemple d'écran suivant.



7 Une fois la mise à niveau terminée, le dispositif Edge n'est plus affiché comme disponible pour la mise à niveau dans l'onglet Maintenance et le message de bannière de mise à niveau ne s'affiche plus.

Comme indiqué précédemment, vous pouvez ignorer la VM de version antérieure si la mise à niveau réussit. Si la mise à niveau échoue, recommencez la mise à niveau lorsque vous y êtes invité. Si vous ne souhaitez pas réessayer après l'échec de la mise à niveau, remettez la VM sous tension pour que le dispositif Edge soit à nouveau actif et qu'aucune donnée ne soit perdue.

Surveillance de votre environnement Horizon Cloud Service - next-gen

Vous pouvez utiliser la console Horizon Universal Console dans Horizon Cloud Service - next-gen pour rechercher des utilisateurs, afficher leurs données de poste de travail et d'application, télécharger des journaux de VM et vérifier les informations d'événement collectées, telles que les notifications, les événements d'audit et les activités système et utilisateur.

Fonctionnalité de support technique dans votre environnement Horizon Cloud Service - next-gen

Horizon Universal Console permet de surveiller l'utilisation par un utilisateur final des applications et des postes de travail virtuels, et de résoudre les problèmes. En tant qu'administrateur d'Horizon Universal Console, vous pouvez utiliser la fonctionnalité de recherche de la console pour rechercher des utilisateurs. Vous pouvez rechercher des sessions pour des utilisateurs particuliers afin de résoudre des problèmes et d'effectuer des opérations de maintenance sur des postes de travail spécifiques.

Objectif de la fonctionnalité de support technique

Dans votre organisation, des administrateurs ayant accès à Horizon Universal Console peuvent aider les utilisateurs finaux dans diverses activités, telles que l'utilisation de postes de travail virtuels et d'applications distantes fournis par votre environnement. Ces administrateurs peuvent également surveiller les sessions des utilisateurs finaux ou les instances de postes de travail pour identifier les problèmes susceptibles d'avoir une incidence sur les sessions.

Dans Horizon Universal Console, les éléments suivants prennent en charge la réalisation des tâches liées au support technique :

- Fonctionnalité de recherche d'Horizon Universal Console. Les employés du support technique peuvent utiliser cette fonctionnalité pour rechercher un utilisateur final spécifique.
- Fonctionnalité fiche utilisateur. À l'aide d'une fiche d'utilisateur spécifique, les employés du support technique peuvent examiner les sessions de cet utilisateur pour résoudre les problèmes et exécuter des opérations de maintenance sur des postes de travail spécifiques.

Préparation de votre environnement pour la fonctionnalité de support technique en fonction du type de fournisseur

La fonctionnalité de support technique sur Horizon Universal Console prend en charge les déploiements de Microsoft Azure et d'Horizon 8.

Note Vous pouvez afficher les informations du support technique pour les environnements Microsoft Azure et Horizon 8 côte à côte lorsque vous disposez d'un environnement hybride.

Horizon Cloud Service - next-gen on Microsoft Azure

Les conditions préalables sont des étapes obligatoires que vous effectuez pendant le processus d'intégration. Après l'intégration, la fonctionnalité de support technique fonctionne alors par défaut.

Horizon Cloud Service - next-gen on Horizon 8

Assurez-vous que les conditions préalables sont remplies pour que la fonctionnalité de support technique soit compatible avec votre environnement. Reportez-vous à la section Effectuer les conditions préalables pour la fonctionnalité de support technique pour un environnement Horizon 8.

Effectuer les conditions préalables pour la fonctionnalité de support technique pour un environnement Horizon 8

Remplissez les conditions requises suivantes pour vous assurer que la fonctionnalité de support technique est compatible avec un environnement Horizon 8.

Procédure

- Assurez-vous que vous disposez d'une licence universelle Horizon pour votre déploiement.
- Intégrez Horizon 8 Edge à Horizon Cloud Service - next-gen.

- Assurez-vous que votre fournisseur d'identité est synchronisé avec le plan de contrôle Horizon Cloud Service - next-gen.

  La synchronisation SID est requise.
- Activez la surveillance de l'agent.
- Assurez-vous que des informations d'identification secondaires ont été ajoutées pour le compte utilisé pour le couplage d'Horizon Connection Server dans Horizon Connection Server.

  L'ajout des informations d'identification secondaires permet de rechercher des utilisateurs ou des groupes à partir de domaines approuvés unidirectionnels.
- Assurez-vous que le compte utilisé pour se connecter à Horizon Connection Server dispose des privilèges Gérer l'opération de redémarrage (`MACHINE_REBOOT`) et Gérer les sessions (`MANAGE_VDI_SESSION`).

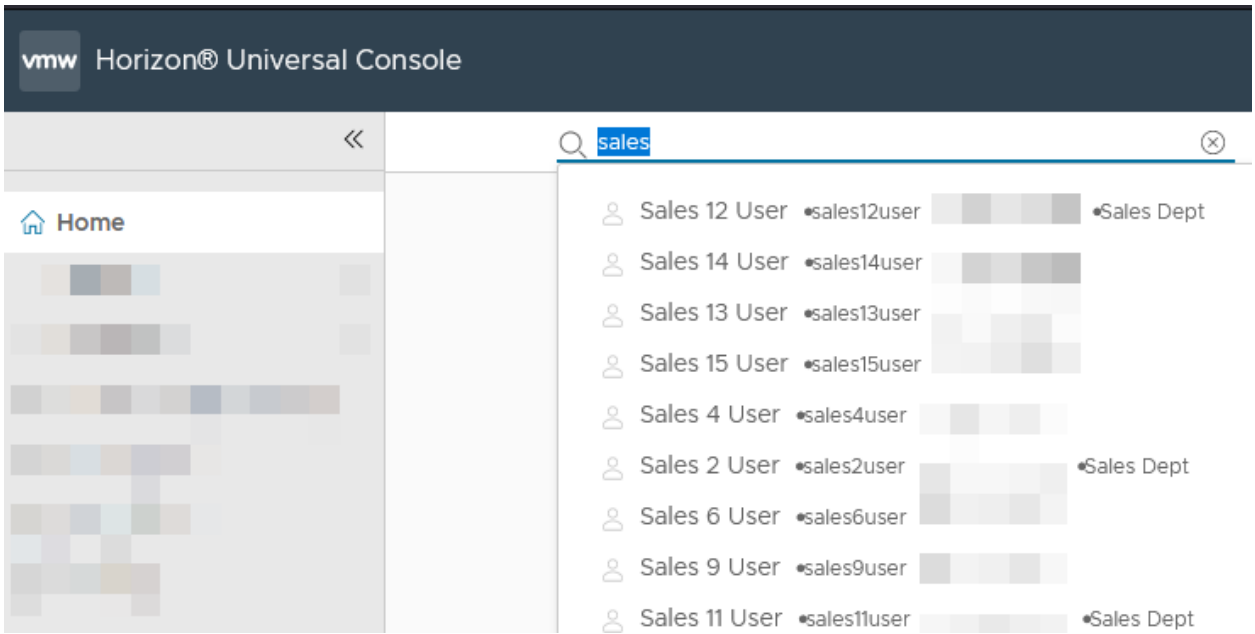
Étape suivante

Utilisez les fonctionnalités de recherche et de support technique d'Horizon Universal Console, comme décrit dans les sections suivantes.

Utilisation de la fonctionnalité de recherche de la console

Utilisez la fonctionnalité de recherche d'Horizon Universal Console pour localiser un utilisateur final spécifique dans votre environnement selon le nom. Vous pouvez rechercher des utilisateurs par prénom, nom de famille ou nom complet.

Sur n'importe quelle page d'Horizon Universal Console, entrez votre terme de recherche dans la zone de texte de recherche. Lorsque vous avez entré au moins trois (3) caractères dans la zone de texte de recherche, les noms qui commencent par ces caractères s'affichent. Pour affiner les résultats, vous pouvez continuer à entrer d'autres caractères.



Lorsque le nom de l'utilisateur que vous recherchez s'affiche, cliquez dessus pour obtenir plus d'informations sur cet utilisateur. Pour plus d'informations, reportez-vous à la section Utilisation de la fonctionnalité de fiche utilisateur et de support technique d'Horizon Cloud.

Utilisation de la fonctionnalité de fiche utilisateur et de support technique d'Horizon Cloud

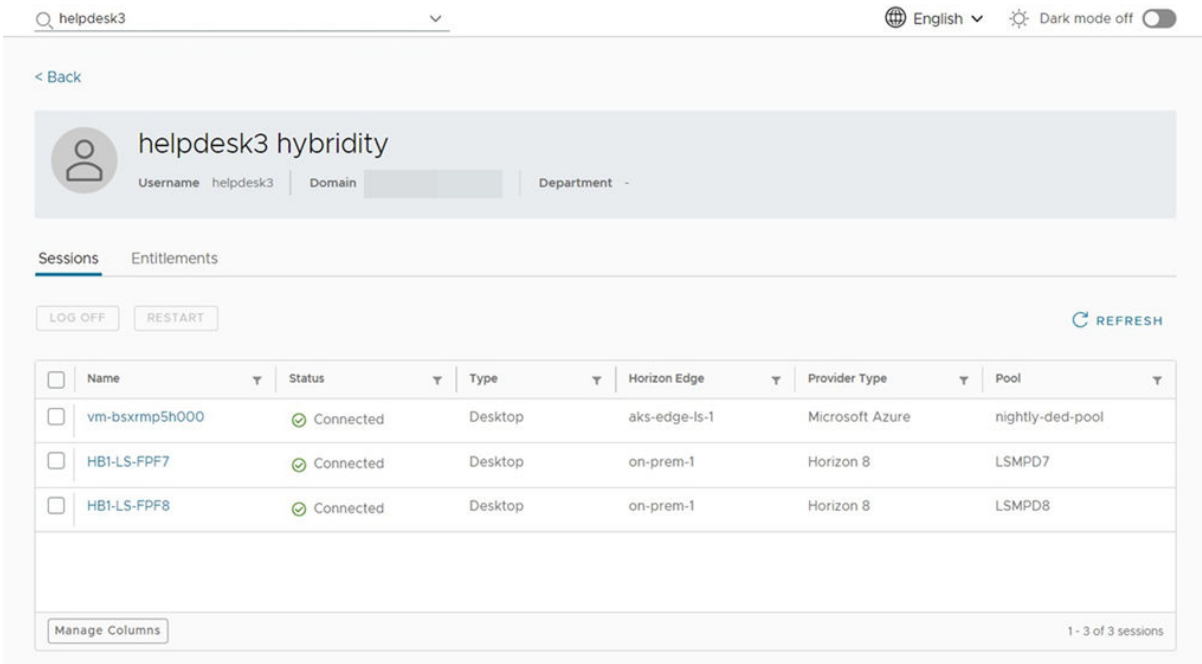
Utilisez la fonctionnalité de fiche utilisateur accessible avec Horizon Universal Console comme tableau de bord pour utiliser des ressources attribuées d'un utilisateur final spécifique, telles que les postes de travail et les applications de ce dernier. Initiez l'accès à la fonctionnalité de support technique en recherchant un utilisateur.

Utilisez la fonctionnalité de recherche d'Horizon Universal Console pour afficher la fiche d'un utilisateur spécifique. Pour savoir comment rechercher un utilisateur final, reportez-vous à la section Utilisation de la fonctionnalité de recherche de la console. Lorsque vous cliquez sur le nom d'un utilisateur final dans les résultats de la recherche, le système affiche la fiche de cet utilisateur final.

Vous pouvez afficher des données informatives dans le contexte de l'utilisateur final spécifique et sur les sessions actives et les droits de cet utilisateur final.

Sessions

Pour obtenir des informations sur les sessions actives de l'utilisateur, accédez à la fiche utilisateur.



Dans l'onglet **Sessions**, vous pouvez effectuer les actions suivantes.

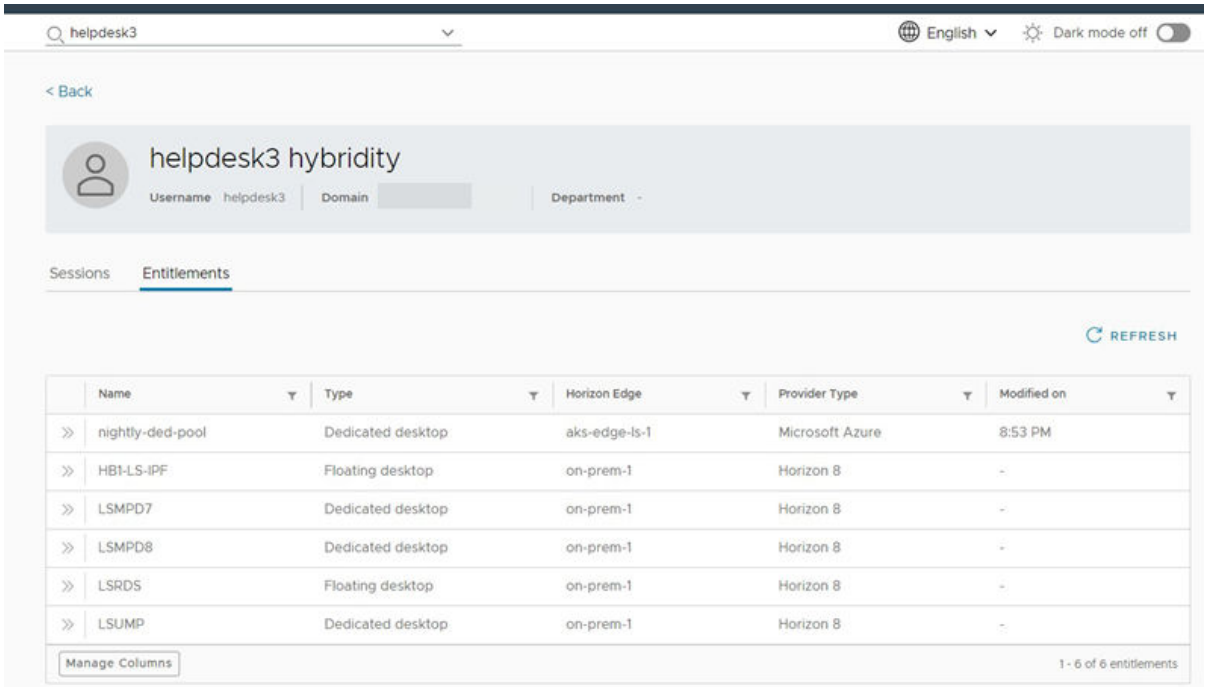
- Afficher la liste des sessions, qui inclut les applications et les sessions.
- Cocher la case d'une session spécifique pour activer les actions suivantes.
  - **Fermer la session** pour fermer la session.

- **Redémarrer** pour redémarrer la session.

- Afficher les détails d'une session spécifique en cliquant sur le **Nom** de la session.
  - Les détails disponibles peuvent varier selon le type de fournisseur.
  - Les détails de la session incluent des détails sur la machine cliente et des détails supplémentaires, tels que la VM, la session, l'utilisation du CPU, l'utilisation de la mémoire et les statistiques d'intermédiation de segments d'ouverture de session pour la dernière session active.

Droits

Pour obtenir des informations sur les droits des utilisateurs, accédez à la fiche utilisateur et sélectionnez l'onglet **Droits**.



Dans l'onglet **Droits**, vous pouvez effectuer les actions suivantes.

- Afficher les applications ou les postes de travail virtuels attribués à cet utilisateur final spécifique.
- Développer un droit pour afficher les détails de la VM ou de l'application.
- Vous pouvez effectuer des opérations sur les postes de travail.
  - Mettre sous tension
  - Mettre hors tension
  - Arrêter
  - Redémarrer

Note Pour les VM Horizon 8, vous pouvez effectuer l'opération **Redémarrer** uniquement.

- Vous pouvez obtenir des informations sur les postes de travail dédiés attribués à l'utilisateur final, même lorsque celui-ci ne dispose pas de session active sur ce poste de travail.

Note Pour les déploiements d'Horizon 8, la fonctionnalité de support technique présente les limitations suivantes.

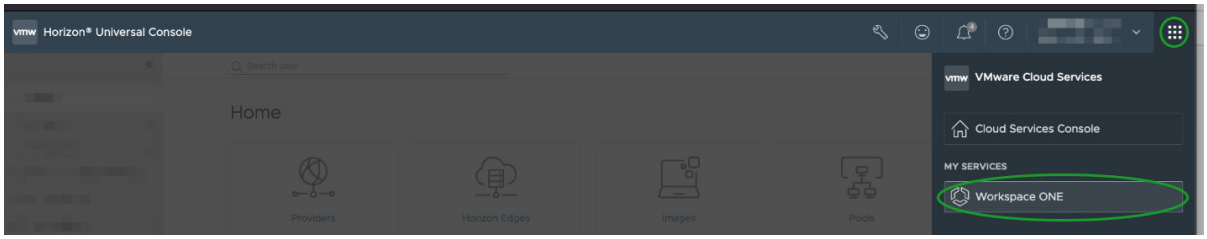
- Actuellement, seules les sessions de poste de travail et les droits locaux à Horizon Connection Server sont pris en charge.
- Les sessions et les droits d'application ne s'affichent pas.
- Les sessions globales réparties par l'instance de Horizon Connection Server couplée, mais hébergées sur un dispositif Horizon Edge distant ne s'affichent pas.
- Les opérations suivantes sur les VM Horizon 8 ne sont pas prises en charge :
  - Mettre hors tension
  - Arrêter
  - Mettre sous tension

Pour refuser l'analyse et les guides de Pendo

Vous pouvez refuser l'analyse et les guides de Pendo à l'aide de Workspace ONE, comme décrit dans les instructions qui suivent.

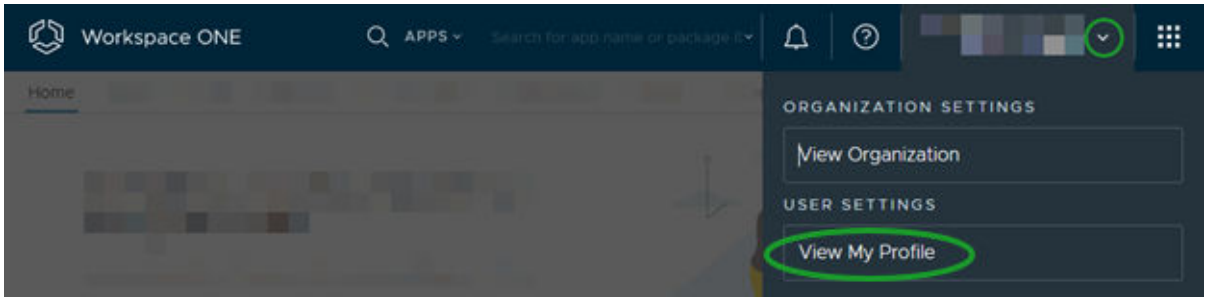
Procédure

1 Dans Horizon Universal Console, cliquez sur le menu Applications VMware Cloud Services ( ) et sélectionnez Workspace ONE.



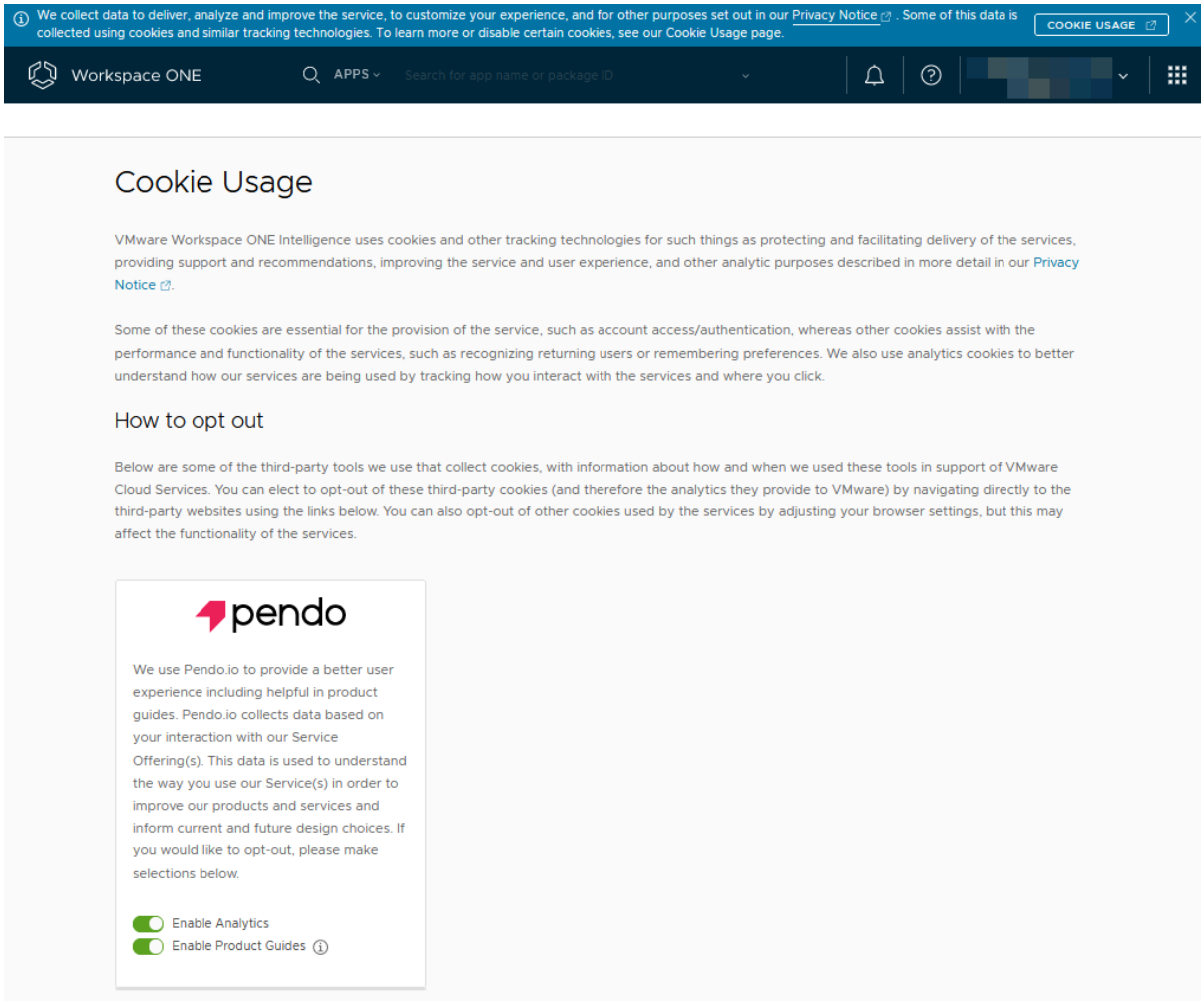
La console Workspace ONE Cloud Admin Hub s'ouvre.

2 Dans la console Workspace ONE Cloud Admin Hub, cliquez sur la flèche vers le bas, qui est le menu déroulant **Paramètres de l'utilisateur/l'organisation** et sélectionnez **Afficher mon profil**.



3 Faites défiler la liste jusqu'à la section Cookies et cliquez sur **Utilisation des cookies**.

La page Utilisation des cookies s'affiche, comme illustré par la capture d'écran suivante.



4 Effectuez la procédure appropriée si vous souhaitez refuser **Activer l'analyse** et **Activer les guides des produits** ou si vous souhaitez refuser uniquement **Activer les guides de produits**.

- Pour refuser les deux options, cliquez sur le bouton bascule **Activer l'analyse**.

- Pour refuser **Activer les guides de produits**, cliquez sur le bouton bascule **Activer les guides de produits**.

Surveillance de l'état des ressources Horizon Cloud à partir de la page d'accueil

Lorsque votre déploiement d'Horizon Cloud est intégré à Workspace ONE Intelligence, vous pouvez utiliser la page d'accueil d'Horizon Universal Console pour surveiller les ressources.

Note Gardez à l'esprit que certaines données et informations affichées peuvent être retardées et ne pas refléter la situation en temps réel. Les données de surveillance proviennent d'Horizon Agent et sont envoyées au lac de données cloud Workspace ONE. Horizon Universal Console interroge le lac de données pour remplir les tableaux de bord. Dans le pire des cas, ce traitement de bout en bout peut entraîner des retards allant jusqu'à 30 minutes.

En termes de surveillance, l'objectif de la page d'accueil est de se concentrer sur les informations qui aident les administrateurs à déterminer rapidement les éléments suivants.

- Santé globale de leur déploiement d'Horizon Cloud.

  Par exemple, en fournissant les informations suivantes.

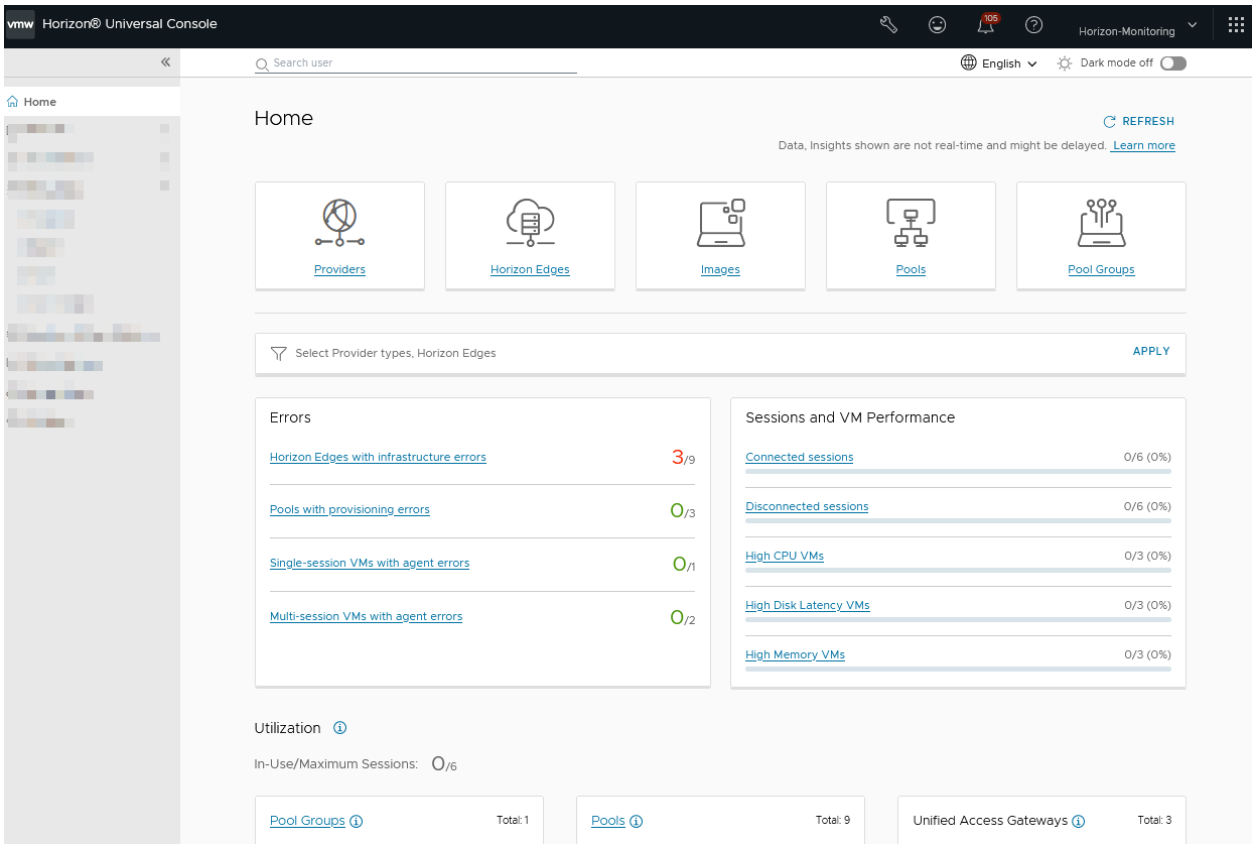
  - Erreurs d'infrastructure Horizon Edge
  - Erreurs de provisionnement de pool
  - Erreurs d'Horizon Agent, pour les agents s'exécutant dans des VM à une ou plusieurs sessions

  En termes de surveillance de la santé globale de leur déploiement d'Horizon Cloud, la page d'accueil aide les administrateurs à déterminer les types de problèmes existants, le cas échéant. Par exemple, les types de problèmes suivants :

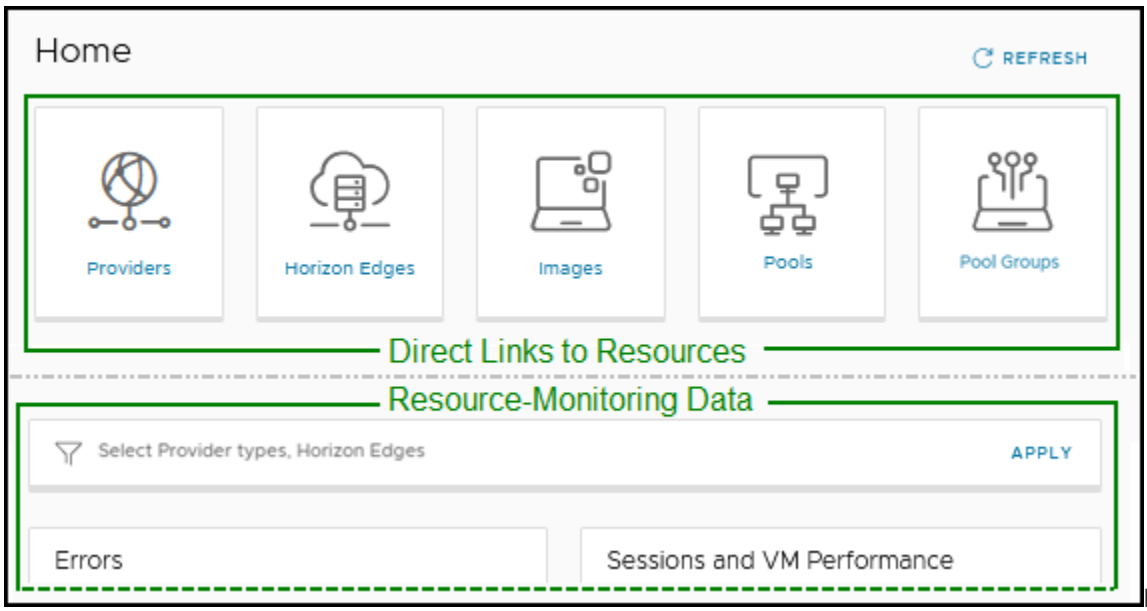
  - Problèmes clairement identifiables
  - Problèmes nécessitant un examen plus approfondi
  - Problèmes indiquant que les administrateurs peuvent adopter une approche de surveillance à court terme
  - Problèmes nécessitant une action corrective immédiate
- Nombre réel de sessions connectées et déconnectées.
- Nombre réel de VM rencontrant des problèmes de performances, tels que des problèmes de CPU, de mémoire et de disque élevés.
- Données d'utilisation de la capacité, notamment l'utilisation des 3 principaux groupes de pools, pools et instances d'Unified Access Gateway.

Sur la page d'accueil, vous pouvez afficher les données ou accéder facilement à celles qui indiquent que les utilisateurs finaux rencontrent actuellement des problèmes d'accès aux postes de travail ou aux applications, ou que les utilisateurs finaux peuvent rencontrer rapidement des problèmes, sauf si vous prenez des mesures.

Vous pouvez commencer à afficher les données de surveillance des ressources et à interagir avec celles-ci sur la page d'accueil après le déploiement d'Horizon Edge et après l'intégration d'Horizon Cloud à Workspace ONE Intelligence. Davantage de données de surveillance des ressources deviennent disponibles lorsque vous continuez à déployer Horizon Cloud.



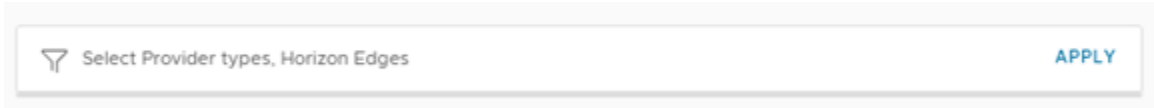
La page d'accueil se compose de deux sections. Le haut de la page d'accueil se compose de boutons de ressources. Ceux-ci sont des liens directs vers vos ressources d'Horizon Cloud. Au-dessous des boutons de ressources, se trouvent des données sur vos ressources, que vous pouvez afficher et avec lesquelles vous pouvez interagir.



Les informations qui suivent expliquent comment interagir avec les données de surveillance des ressources disponibles sur la page d'accueil.

Sélectionner les dispositifs Dispositifs Horizon Edge à surveiller

La page d'accueil affiche la surveillance des ressources lorsque vous utilisez le filtre **Sélectionner les types de fournisseurs, les dispositifs Horizon Edge**. Vous pouvez filtrer par types de fournisseurs et par dispositifs Dispositifs Horizon Edge qui appartiennent aux types de fournisseurs sélectionnés et cliquer sur **Appliquer** pour afficher les données relatives aux **Erreurs** et les informations en direct sur **Sessions et performances de VM** de l'utilisateur final pour les différents types de fournisseurs, tels que Microsoft Azure et Horizon 8.



Par défaut, la page d'accueil affiche les données de surveillance des ressources, à l'exception des données de pools, pour tous vos dispositifs Dispositifs Horizon Edge.

Note La zone Pools de la section Utilisation s'applique à tous les pools de l'ensemble de vos dispositifs Dispositifs Horizon Edge, quels que soient les dispositifs Dispositifs Horizon Edge que vous sélectionnez avec le filtre **Sélectionner les dispositifs Horizon Edge**.

Les données de surveillance d'Horizon Agent sont transmises à Workspace ONE Intelligence et sont intégrées à VMware Horizon® Cloud Service™ - next-gen ou à Splunk en fonction de la gestion des licences. L'activation de l'intégration des données de Workspace ONE Intelligence à VMware Horizon® Cloud Service™ - next-gen a lieu après celle de la surveillance d'Horizon Agent. Pour plus d'informations, reportez-vous à la section Configuration de la surveillance

des données d'Horizon Edge Agent pour Horizon Edge avec Workspace ONEL'intégration des données de VMware Horizon® Cloud Service™ - next-gen à Splunk doit être configurée. Pour plus d'informations, reportez-vous à la section Configuration de la surveillance d'Horizon 8 Edge avec Splunk Enterprise.

Données de surveillance des ressources : erreurs

La section Erreurs de la page d'accueil répertorie les erreurs d'Horizon Edge, les erreurs de provisionnement de pool, les erreurs de VM à session unique et les erreurs de VM à plusieurs sessions.

Pour chaque type d'erreur de ressource, la section Erreurs affiche une fraction, par exemple 2/10, qui indique que deux instances de cette ressource, sur les dix disponibles, rencontrent des erreurs. L'exemple générique suivant fournit plus de détails.

Exemple de type d'erreur de ressource générique

Par exemple, si la section Erreurs répertorie un type d'erreur de ressource suivi de la fraction 2/10, celle-ci indique que pour les dispositifs Dispositifs Horizon Edge sélectionnés avec le filtre **Sélectionner les dispositifs Horizon Edge**, dix instances du type de ressource correspondant sont disponibles et deux d'entre elles rencontrent des erreurs.

Note La fraction, telle que 2/10, n'indique pas le nombre d'erreurs.

Pour obtenir plus de détails, tels que les deux ressources (dans cet exemple) qui rencontrent précisément des erreurs, le nombre total d'erreurs et la nature précise des erreurs, cliquez sur le lien du type d'erreur de ressource et parcourez les objets à la page suivante pour en savoir plus sur les différentes options à votre disposition pour ce type d'erreur de ressource spécifique.

Le cas échéant, la page suivante inclut des liens vers d'autres pages d'Horizon Universal Console ou de la console VMware Cloud Services qui peuvent vous être utiles.

Le tableau suivant répertorie les types d'erreurs de ressources, tels qu'ils apparaissent dans la section Erreurs de la page d'accueil. Le tableau fournit des exemples spécifiques de chaque type d'erreur de ressource. L'exemple de colonne inclut un exemple de fraction et fournit des détails pour cet exemple.

Tableau 6-1. Exemples de type d'erreur de ressource spécifiques

Type d'erreur de ressource	Description	Exemple
Dispositifs Edge Horizon présentant des erreurs d'infrastructure	Dispositifs Horizon Edge rencontrant des erreurs d'infrastructure. Ces erreurs n'incluent pas les erreurs de déploiement d'Horizon Edge. La page Dispositifs Horizon Edge présentant des erreurs d'infrastructure inclut les erreurs envoyées à partir des composants suivants. ■ Passerelle Horizon Edge dans un environnement Microsoft Azure ■ Ces messages d'erreur impliquent une passerelle Horizon Edge dans un environnement Microsoft Azure et incluent des erreurs concernant le déploiement de services dans la passerelle Horizon Edge et la connectivité des services de la passerelle Horizon Edge au plan de contrôle Horizon Cloud Services. Les messages d'erreur suivants servent d'exemple. ■ `Failed to pull module image` ■ `Module is terminating multiple times` ■ `EdgeDevice is disconnected from IoTHub` ■ Unified Access Gateway dans un environnement Microsoft Azure ■ Ces messages d'erreur impliquent une instance d'Unified Access Gateway et incluent des erreurs concernant UAG et les technologies associées, telles que le service Edge, le broker d'authentification, le serveur UT, le service Blast, le protocole PCOIP et le RDP de tunnel. Les messages d'erreur suivants servent d'exemple. ■ `Tunnel Rdp is down` ■ `Failed to fetch UAG certificate` ■ Active Directory ■ Ces messages d'erreur impliquent des erreurs de connexion liées à Active Directory et incluent des erreurs de serveur Active Directory, de compte de liaison et de compte de jonction. Le message d'erreur suivant sert d'exemple. `Failed to connect to AD Server {domainName}`	Type d'erreur de ressource **Dispositifs Edge Horizon présentant des erreurs d'infrastructure** suivi de la fraction 2/2. Dans cet exemple de fraction 2/2, deux dispositifs Dispositifs Horizon Edge sont disponibles et les deux rencontrent des erreurs. Pour obtenir plus d'informations, par exemple le nombre total d'erreurs et la nature précise des erreurs, cliquez sur **Dispositifs Edge Horizon présentant des erreurs d'infrastructure** et accédez aux objets sur la page.
Pools présentant des erreurs de provisionnement	Pools présentant des erreurs de provisionnement.	Type d'erreur de ressource **Pools présentant des erreurs de provisionnement**, suivi de la fraction 3/16.

Tableau 6-1. Exemples de type d'erreur de ressource spécifiques (suite)

Type d'erreur de ressource	Description	Exemple
		Dans cet exemple de fraction 3/16, 16 pools sont disponibles et trois de ces pools rencontrent des erreurs. Pour obtenir plus d'informations, par exemple sur les pools présentant des erreurs, le nombre total d'erreurs, la nature précise des erreurs et le moment où elles se sont produites, cliquez sur **Pools présentant des erreurs de provisionnement**. Vous pouvez ensuite parcourir les objets de la page, ce qui inclut le filtrage des pools affichés sur la page.

Tableau 6-1. Exemples de type d'erreur de ressource spécifiques (suite)

Type d'erreur de ressource	Description	Exemple
VM à session unique présentant des erreurs d'agent	VM à session unique qui rencontrent des erreurs d'agent. En termes de VM présentant des erreurs d'agent, les niveaux de gravité d'erreur suivants s'appliquent. **Critique** Nécessite une attention immédiate. Un service de l'agent s'est potentiellement arrêté et les utilisateurs finaux risquent de ne pas pouvoir se connecter à leurs postes de travail. **Avertissement** Indique un problème de connexion potentiel.	Type d'erreur de ressource **VM à session unique présentant des erreurs d'agent**, suivi de la fraction 4/34. Dans cet exemple de fraction 4/34, 34 VM à session unique sont disponibles et quatre de ces VM rencontrent des erreurs. Pour obtenir plus d'informations, par exemple sur les VM qui rencontrent des erreurs, le nombre total d'erreurs, la gravité de chaque erreur, la version de l'agent associée à chaque erreur, la nature précise des erreurs et le moment où elles se sont produites, cliquez sur **VM à session unique présentant des erreurs d'agent** et accédez aux objets sur la page. En outre, la page propose une méthode pratique de collecte de journal de l'agent par erreur, avec l'option **Générer un journal** visible lorsque vous cliquez sur les trois points verticaux. Pour plus d'informations sur le journal de l'agent associé, reportez-vous à la section Collecter les journaux d'Horizon Agent à l'aide d'Horizon Universal Console.
VM à plusieurs sessions présentant des erreurs d'agent	VM à plusieurs sessions qui rencontrent des erreurs d'agent. En termes de VM présentant des erreurs d'agent, les niveaux de gravité d'erreur suivants s'appliquent. **Critique** Nécessite une attention immédiate. Un service de l'agent s'est potentiellement arrêté et les utilisateurs	Type d'erreur de ressource **VM à plusieurs sessions présentant des erreurs d'agent**, suivi de la fraction 5/52.

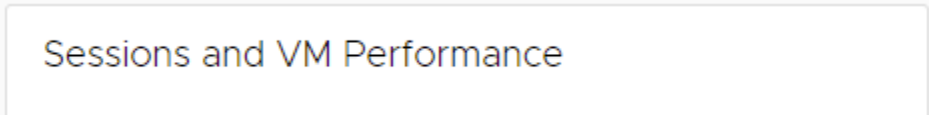
Tableau 6-1. Exemples de type d'erreur de ressource spécifiques (suite)

Type d'erreur de ressource	Description	Exemple
	finaux risquent de ne pas pouvoir se connecter à leurs postes de travail. **Avertissement** Indique un problème de connexion potentiel.	Dans cet exemple de fraction 5/52, 52 VM à plusieurs sessions sont disponibles et cinq de ces VM rencontrent des erreurs. Pour obtenir plus de détails, par exemple sur les VM qui rencontrent des erreurs, le nombre total d'erreurs, la gravité de chaque erreur, la version de l'agent associée à chaque erreur, la nature précise des erreurs et le moment où elles se sont produites, cliquez sur **VM à plusieurs sessions présentant des erreurs d'agent** et accédez aux objets sur la page. En outre, la page propose une méthode pratique de collecte de journal de l'agent par erreur, avec l'option **Générer un journal** visible lorsque vous cliquez sur les trois points verticaux. Pour plus d'informations sur le journal de l'agent associé, reportez-vous à la section Collecter les journaux d'Horizon Agent à l'aide d'Horizon Universal Console.

Données de surveillance des ressources : sessions et performances de VM

La section Sessions et performances de VM de la page d'accueil affiche les données de session et les données de performances de VM. La section sépare les données de session par type de session, comme celles qui sont connectées et celles qui sont déconnectées, et sépare les données de VM par catégories de performances, telles qu'un CPU élevé, une latence de disque élevée et une mémoire élevée. Pour obtenir plus d'informations sur le type de session ou de données de performances de VM répertoriées, cliquez sur le lien vers le type de session spécifique ou le type de données de performances de VM à surveiller et parcourez les objets à la page suivante pour en savoir plus sur les différentes options à votre disposition.

Le cas échéant, la page suivante inclut des liens vers d'autres pages d'Horizon Universal Console ou de la console VMware Cloud Services qui peuvent vous être utiles.



Sessions

Les informations suivantes s'appliquent aux données de session disponibles dans la section Sessions et performances.

- Types de sessions :
  - **Sessions connectées**

    Indique qu'une session de poste de travail ou d'application de l'utilisateur final est connectée. Les sessions connectées incluent les sessions actives et inactives.
  - **Sessions déconnectées**

    Indique qu'une session de poste de travail ou d'application de l'utilisateur final est déconnectée. Une session déconnectée diffère d'une session fermée dans le sens où une session déconnectée continue à consommer de la capacité, contrairement à une session fermée.
- Exemple de fraction de session, 5/37 (13 %) :

  L'exemple de fraction 5/37 (13 %) peut s'appliquer à la fois aux sessions connectées et aux sessions déconnectées. Pour rendre l'exemple plus spécifique, supposez que la session est connectée. Par conséquent, sur la capacité totale de 37 sessions, cinq sont connectées (inclut les états de session actif et inactif), ce qui représente 13 % de la capacité totale.
- Sessions par type de pool :

  Cliquez sur un type de session pour accéder à la page de sessions de ce type de session. Un graphique qui affiche les sessions par type de pool se trouve en haut de la page de sessions.

  Suite à l'exemple précédent, où les **Sessions connectées** sont répertoriées comme fraction 5/37, lorsque vous cliquez sur **Sessions connectées**, la page de sessions connectées affiche un graphique illustrant comment les cinq sessions connectées sont fractionnées entre les types de pools. La répartition peut être semblable à ce qui suit :
  - Postes de travail RDSH = 2 sessions
  - Postes de travail VDI = 1 session
  - Applications RDSH = 2 sessions
- Données de session :

La page de sessions présente également différentes données liées à la session, telles que le type de pool, l'état de la session, le nom d'utilisateur et l'heure de connexion, entre autres.

Info-bulle Vous pouvez modifier la façon dont la page présente les données de session à l'aide de l'un des nombreux filtres disponibles sur la page, tels que les filtres **Type de pool**, **État de la session**, **Nom d'utilisateur** et **Horizon Edge**, entre autres.

Les filtres commencent à filtrer votre entrée une fois que vous avez entré un minimum de deux caractères.

- Fermer les sessions déconnectées :

  Vous pouvez fermer les sessions déconnectées directement sur la page de sessions.

Performances de VM

Les informations suivantes s'appliquent aux données de performances disponibles dans la section Sessions et performances.

- Types de performances de VM :

  Info-bulle Pour les types de performances de VM suivants, vous pouvez modifier la façon dont chaque page présente les données de performances en utilisant l'un des filtres disponibles sur la page, tels que les filtres **Poste de travail**, **Pool** et **Horizon Edge**.

  Les filtres commencent à filtrer votre entrée une fois que vous avez entré un minimum de deux caractères.

  - **VM à CPU élevé**

    Affiche les VM dont l'utilisation du CPU est supérieure ou égale à 80 %.

  - **VM à latence de disque élevée**

    Affiche les VM dont la latence de disque est supérieure ou égale à 20 ms.

  - **VM à mémoire élevée**

    Affiche les VM dont l'utilisation de la mémoire est supérieure ou égale à 80 %.

- Exemple de fraction de performances de VM, 3/42 (7 %) :

L'exemple de fraction 3/42 (7 %) s'applique à tous les types de performances de VM. Sur les 42 VM, trois d'entre elles (ou 7 %) déclenchent l'indicateur pour leur type de performances correspondant.

Note Pour chaque type de performances de VM, si l'une des VM déclenche l'indicateur, une barre codée par couleur accompagne l'étiquette qui correspond à la valeur de pourcentage correspondante, comme suit.

- La plage de 0 à 60 % est en vert, ce qui peut indiquer une sécurité relative concernant ce type de performance. Vous devez déterminer si le pourcentage est problématique, en fonction des spécificités de votre déploiement. Pour rendre l'exemple plus spécifique, supposez que le type de performance de la VM est VM à CPU élevé. Par conséquent, 60 % de VM au maximum rencontrent une utilisation du CPU supérieure à 80 %.
- La plage de 61 à 80 % est en jaune, ce qui indique un problème potentiel concernant ce type de performance.
- La plage de 81 à 100 % est en rouge, ce qui indique qu'une attention immédiate est requise.

Données de surveillance des ressources : utilisation

La section Utilisation de la page d'accueil affiche les trois instances principales ou les plus utilisées de la ressource correspondante.

Les détails suivants s'appliquent à la section Utilisation.

- Exemple de fraction En cours d'utilisation/Nombre maximal de sessions, 4/42 :

  L'exemple de fraction 4/42 indique que pour les types de ressources répertoriés dans la section Utilisation, quatre sessions sont actives, inactives ou déconnectées, tandis que 38 d'entre elles sont disponibles, mais inutilisées.

- Types et totaux de ressources :

  L'étiquette, Total, qui accompagne chaque ressource indique le nombre d'instances de ce type de ressource qui sont disponibles. Par exemple, « **Total de 4 groupes de pools** » indique que 4 groupes pools sont disponibles.

  Note La zone Groupes de pools s'applique toujours à tous les groupes de pools de l'ensemble de vos dispositifs Dispositifs Horizon Edge. Toutefois, la zone Pools et la zone Instances d'Unified Access Gateway s'appliquent uniquement aux groupes de pools et aux instances d'Unified Access Gateway associées aux dispositifs Dispositifs Horizon Edge sélectionnés à l'aide du filtre **Sélectionner les dispositifs Horizon Edge** sur la page d'accueil.

- Instances de ressource
  - Chaque zone de ressource nomme les trois instances les plus utilisées du type de ressource donné. La zone inclut un graphique à barres qui présente le nombre de sessions pour chaque instance de ressource.

    Les mesures de session pour les instances d'Unified Access Gateway diffèrent des mesures de session pour les groupes de pools et les pools, comme suit.

    Groupes de pools

    Le nombre de sessions est la somme des sessions actives, inactives et déconnectées.

    Pools

    Le nombre de sessions est la somme des sessions actives, inactives et déconnectées.

    Instances d'Unified Access Gateway

    Le nombre de sessions est la somme des sessions actives et inactives.

    Info-bulle Passez le pointeur sur une barre d'instance pour afficher les détails de la session sur cette instance de ressource.

Surveillance de votre réseau en fonction des données d'Horizon Agent

Les problèmes réseau de poste de travail de l'utilisateur final sont détectés par l'infrastructure d'Horizon Cloud en fonction de la communication à partir d'instances d'Horizon Agent installées. Horizon Cloud utilise des notifications pour vous communiquer ces problèmes réseau.

Horizon Agent communique des données de trafic réseau, telles que la perte de paquets réseau, la latence réseau, etc., à Horizon Cloud. Horizon Cloud analyse les données et envoie une notification directement à Horizon Universal Console. Pour obtenir des informations générales sur les notifications, reportez-vous à la section Notifications dans Horizon Cloud Service - next-gen.

Lorsqu'une notification liée au réseau, telle que « Dégradation du réseau détectée », s'affiche dans Horizon Universal Console, vous pouvez cliquer sur la notification pour en savoir plus sur le nombre de postes de travail affectés. Vous pouvez afficher les postes de travail affectés sur le rapport de Workspace ONE Intelligence. Vous pouvez accéder à Workspace ONE Intelligence depuis la page d'accueil d'Horizon Universal Console. Pour résoudre les problèmes réseau, vous pouvez examiner l'infrastructure réseau de poste de travail de l'utilisateur final et appliquer des correctifs.

Collecte des journaux de l'agent

L'objectif de la collecte des journaux de diagnostic d'Horizon Agent est généralement de permettre au support VMware d'analyser les problèmes que rencontrent les administrateurs. Le processus implique la collecte, sur des machines virtuelles spécifiques, de bundles de journaux de diagnostic grâce auxquels le support VMware peut diagnostiquer les problèmes. Le terme bundle

DCT (bundle Data Collection Tool) est souvent utilisé par le support VMware en référence à ce type de bundle de journaux.

La collecte des journaux de diagnostic d'Horizon Agent peut se produire de l'une des manières suivantes.

En tant qu'administrateur de client, vous collectez les journaux de l'agent à l'aide d'Horizon Universal Console.

Les administrateurs ont tendance à collecter les journaux de l'agent à l'aide d'Horizon Universal Console après l'envoi d'une demande de support technique. Lors de la formulation d'une réponse à cette demande, l'équipe du support affectée détermine que des bundles de journaux de diagnostic de VM spécifiques sont requis pour diagnostiquer le problème.

Pour plus d'informations sur la collecte des journaux de l'agent, reportez-vous à la section Collecter les journaux d'Horizon Agent à l'aide d'Horizon Universal Console

Pour les clients qui ont choisi d'autoriser l'équipe responsable des opérations de VMware à accéder aux journaux de diagnostic de l'agent, l'équipe génère directement ces journaux afin de déboguer les problèmes des utilisateurs finaux liés aux VM.

Pour résoudre les problèmes plus rapidement, l'équipe responsable des opérations de VMware utilise les journaux de diagnostic d'Horizon Agent pour déboguer les problèmes des utilisateurs finaux liés aux VM.

- En tant qu'administrateur de client, vous disposez d'un contrôle total sur l'affichage et la suppression des journaux générés dans Horizon Universal Console.
- Les journaux d'Horizon Agent sont automatiquement supprimés après 15 jours.
- L'URL de téléchargement des journaux de l'agent est active pendant une durée limitée qui est spécifiée par la date d'expiration des journaux.
- L'équipe responsable des opérations de VMware ne peut ni générer, ni afficher, ni supprimer les journaux de l'agent si vous avez désactivé cette fonctionnalité. Cependant, pour faciliter la maintenance, laissez-la activée.

Pour plus d'informations sur l'autorisation de collecte des journaux de l'agent accordée à l'équipe responsable des opérations de VMware, reportez-vous à la section Autoriser ou empêcher l'équipe responsable des opérations de VMware de collecter les journaux d'Horizon Agent.

Important

- Lorsqu'un journal d'agent est généré, il est répertorié sur la page Journaux de l'agent à laquelle vous pouvez accéder en sélectionnant **Surveiller > Journaux de l'agent**. La colonne « Lancé par » sur la page Journaux de l'agent indique clairement l'utilisateur qui a généré le journal de l'agent : soit un administrateur au sein de votre organisation, soit l'équipe responsable des opérations de VMware.
- Lorsque des journaux de l'agent sont générés ou supprimés, l'activité est enregistrée et disponible sur la page Journaux d'activité. Reportez-vous à la section Surveillance de l'activité de l'administrateur et de l'utilisateur final sur la page Journal d'activité.
- Les journaux de diagnostic peuvent contenir des données générées par des composants tiers, tels que le système d'exploitation Microsoft Windows (notamment des journaux d'événements Windows), et par des composants logiciels VMware, lesquels sont nécessaires pour le débogage.

  Les journaux de diagnostic peuvent contenir des informations d'identification personnelle comme le nom d'utilisateur, l'adresse e-mail, etc. VMware ne peut pas obfusquer ces données sans perdre le contexte des diagnostics. VMware utilise ces données uniquement à des fins de diagnostic et à aucune autre fin.

Collecter les journaux d'Horizon Agent à l'aide d'Horizon Universal Console

Vous pouvez utiliser Horizon Universal Console pour générer, télécharger et supprimer des journaux pour des VM spécifiques.

Avant de continuer, vérifiez les informations d'arrière-plan sur les journaux de l'agent. Reportez-vous à la section Collecte des journaux de l'agent.

Les administrateurs utilisent généralement cette fonctionnalité après avoir soumis une demande de support technique (SR) et, lors de la réponse à cette SR, l'équipe de support affectée détermine que des bundles de journaux de diagnostics de VM spécifiques sont requis pour diagnostiquer le problème. Les entrées de journaux existantes sont remplacées par des journaux récemment générés. Vous pouvez télécharger les journaux existants s'ils peuvent être nécessaires pour référence ultérieure ou supprimer les journaux qui ne sont plus nécessaires. Le terme bundle DCT (bundle Data Collection Tool) est souvent utilisé par l'équipe du support VMware en référence à ce type de bundle de journaux.

Les caractéristiques de sécurité suivantes s'appliquent aux journaux de l'agent que vous collectez.

- Vous disposez d'un contrôle total sur l'affichage et la suppression des journaux générés dans Horizon Universal Console.

- Les journaux d'Horizon Agent sont automatiquement supprimés au bout de 15 jours.
- L'URL de téléchargement des journaux de l'agent est active pendant une durée limitée qui est spécifiée par la date d'expiration des journaux.
- L'équipe responsable des opérations de VMware ne peut ni générer, ni afficher, ni supprimer les journaux de l'agent si vous avez désactivé cette fonctionnalité. Cependant, pour faciliter la maintenance, laissez-la activée.

Conditions préalables

- Vérifiez que l'état de l'instance de la passerelle Passerelle Horizon Edge, de l'instance d'Unified Access Gateway et des pools est Prêt.
- Vérifiez que les agents sur les VM sont disponibles.
- Cet article s'applique uniquement aux dispositifs Microsoft Azure Edge.

Procédure

1. Sélectionnez **Surveiller > Journaux de l'agent**.
2. Cliquez sur **Ajouter**.
3. Sélectionnez un pool pour lequel générer un journal et cliquez sur **Suivant**. Vous pouvez choisir parmi des pools à une ou plusieurs sessions. Seules les VM à l'état Prêt sont disponibles.
4. Sélectionnez toutes les VM pour lesquelles vous souhaitez créer des journaux et cliquez sur **Générer**.

   Vous pouvez choisir entre une et toutes les VM répertoriées qui affichent une coche verte dans la colonne **État des tâches**. L'état des tâches s'exécute au cours du processus de création de journaux. Le processus peut prendre plusieurs minutes.
5. Cliquez sur **Télécharger le journal** pour chaque journal à télécharger.

   Les journaux sont téléchargés à l'aide de votre navigateur.

Étape suivante

Si vous souhaitez supprimer des entrées de journal à tout moment, sélectionnez une entrée de journal à supprimer, cliquez sur **Supprimer**, puis cliquez à nouveau sur **Supprimer**.

Note Vous pouvez sélectionner plusieurs journaux à supprimer s'ils utilisent le même pool.

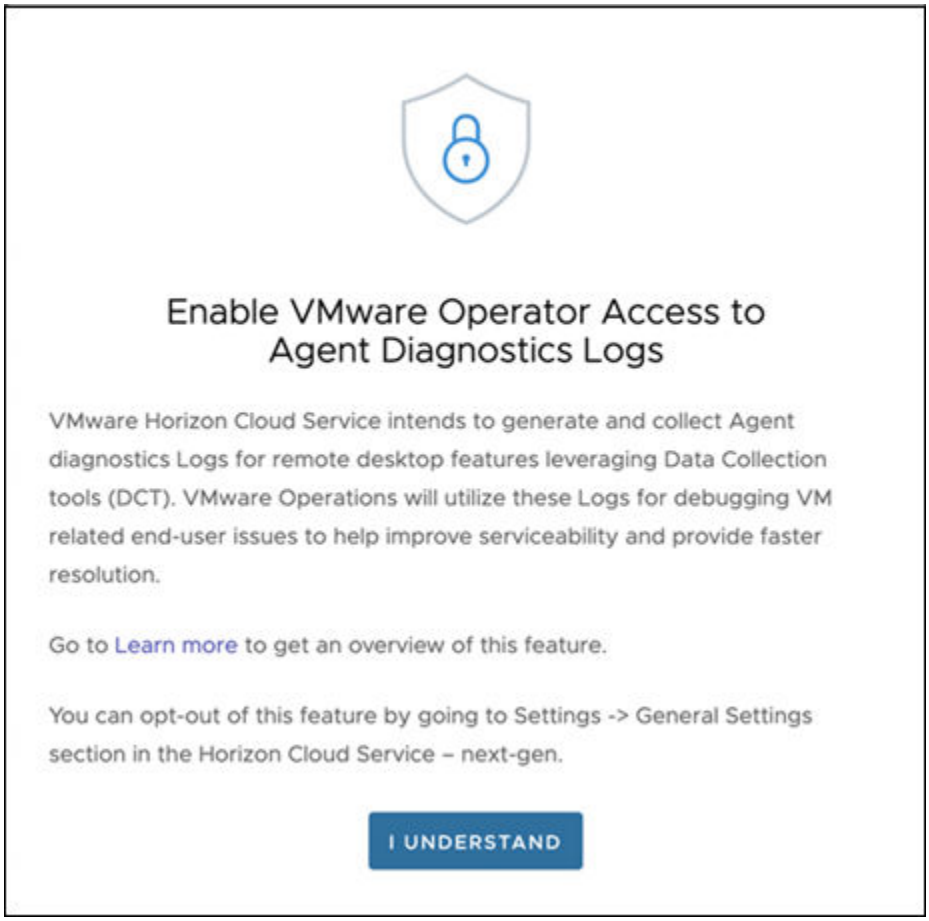
Autoriser ou empêcher l'équipe responsable des opérations de VMware de collecter les journaux d'Horizon Agent

À la suite de la publication de cette fonctionnalité, lorsque vous vous connectez à Horizon Universal Console ou que vous effectuez l'intégration initiale au système Horizon Cloud Service - next-gen, une boîte de dialogue vous explique l'objectif de cette fonctionnalité. Si vous acceptez la fonctionnalité, vous autorisez l'équipe responsable des opérations de VMware à collecter les

journaux de diagnostic de l'agent à partir de vos VM. Vous pouvez désactiver cette fonctionnalité à tout moment.

Avant de continuer, vérifiez les informations d'arrière-plan sur les journaux de l'agent. Reportez-vous à la section Collecte des journaux de l'agent.

La capture d'écran suivante représente la boîte de dialogue qui vous est présentée pour autoriser l'équipe responsable des opérations de VMware à accéder aux journaux de diagnostic de l'agent.



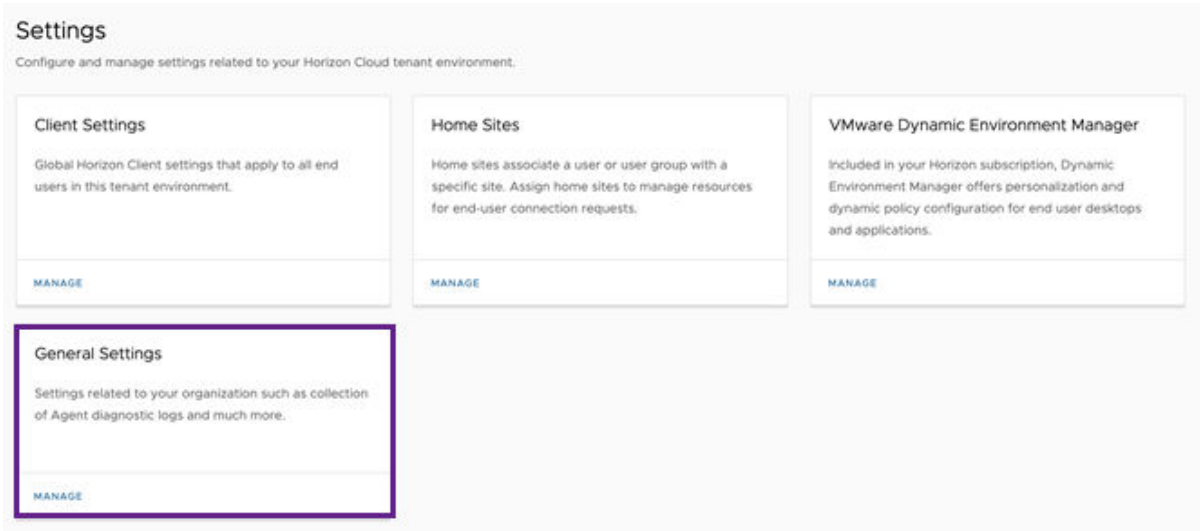
Si vous cliquez sur **Je comprends**, l'équipe responsable des opérations de VMware est autorisée, au besoin, à générer les journaux de diagnostic de l'agent sur des VM pour résoudre un problème spécifique.

Si, après avoir cliqué sur **Je comprends**, vous décidez d'empêcher l'équipe responsable des opérations de VMware de générer et de collecter les journaux de diagnostic d'Horizon Agent, vous pouvez effectuer les étapes suivantes. Inversement, après avoir choisi d'interdire l'accès, vous pouvez effectuer ces mêmes étapes pour autoriser à nouveau l'accès.

Note Par défaut, la création d'un pool autorise l'équipe responsable des opérations de VMware à accéder aux journaux de diagnostic de l'agent sur des VM, sauf si vous désactivez cette fonctionnalité. Vous êtes averti par e-mail et par notification, disponible via l'icône en forme de cloche ( ) située dans le coin supérieur droit de chaque page.

Procédure

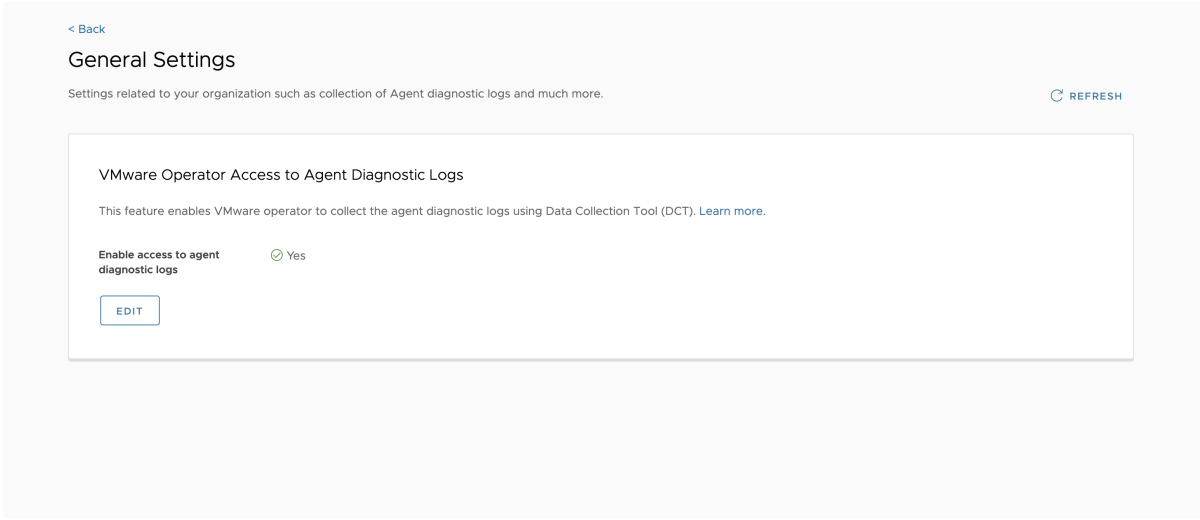
1 Dans Horizon Universal Console, sélectionnez **Paramètres**, puis, dans la vignette Paramètres généraux, cliquez sur **Gérer**.



2 Sur la page Paramètres généraux, cliquez sur **Modifier**.

3 Cliquez sur le bouton bascule **Activer l'accès aux journaux de diagnostic de l'agent** pour inverser le paramètre actuel.

4 Cliquez sur **Enregistrer** pour enregistrer le paramètre.



Surveillance de l'activité de l'administrateur et de l'utilisateur final sur la page Journal d'activité

La page Activité affiche des données sur les événements actuels et passés dans le système.

Pour accéder à la page Journal d'activité, sélectionnez **Surveiller > Journal d'activité**. La page contient l'onglet **Admin** pour les journaux d'audit et les activités système, ainsi que l'onglet **Utilisateur final** pour les événements utilisateur. Vous pouvez effectuer les tâches suivantes :

- Filtrez les événements affichés à l'aide des outils de filtre disponibles dans chaque onglet.
- Actualisez la liste.
- Exportez le journal des événements dans un fichier CSV que vous pouvez télécharger.

Événements administrateur

L'onglet **Admin** affiche un tableau d'informations sur les événements initiés par l'administrateur et le système. Développez un événement pour afficher des détails, tels que des informations sur les événements associés, l'historique des événements de ressources et les sous-tâches.

Le tableau des événements se compose de plusieurs colonnes, notamment celles comportant des titres comme **Événement**, **Statut** et **Type**. La colonne **Type** répertorie deux types d'événements administrateur, comme suit.

Système

Indique les activités du système.

Audit

Indique les journaux d'audit. Différentes opérations initiées par les administrateurs et les opérateurs VMware génèrent les journaux d'audit. Certains journaux d'audit peuvent nécessiter des mesures de votre part, mais bon nombre d'entre eux sont utilisés à titre

informatif uniquement. Par exemple, les audits liés aux mises à jour de la Passerelle Horizon Edge sont informatifs uniquement.

Les options de filtrage suivantes sont disponibles dans l'onglet **Administrateurs** :

- Affichez les événements pendant une période donnée uniquement ou un nom d'opération donné, à l'aide des filtres en haut de l'onglet.
- Filtrez les événements affichés dans le tableau à l'aide de l'outil de filtre dans chaque colonne.

Événements utilisateur

L'onglet **Utilisateur final** affiche le nom d'utilisateur, l'action, l'état et l'heure de journalisation des événements de l'utilisateur final.

Ces options de filtrage sont disponibles dans l'onglet **Utilisateur final** :

- Affichez les événements pendant une période donnée uniquement à l'aide des filtres en haut de l'onglet.
- Filtrez les événements affichés dans le tableau à l'aide de l'outil de filtre dans chaque colonne.

Exportation des journaux d'activité

Les administrateurs peuvent exporter des journaux d'activité pour les administrateurs pendant les 90 derniers jours au maximum. Les journaux sont enregistrés au format CSV. Le nom de fichier inclut un horodatage par défaut, mais vous pouvez personnaliser le nom du fichier si nécessaire.

1. Sur la page d'accueil d'Horizon Universal Console, cliquez sur **Journal d'activité** dans le menu de gauche.
2. Au-dessus du tableau Événements, indiquez si vous voulez afficher tous les événements ou un sous-ensemble d'événements.
3. Sélectionnez les filtres de colonne du tableau et la période d'affichage, des 24 dernières heures aux 90 derniers jours.
4. Cliquez sur **EXPORTER**.
5. Dans la boîte de dialogue Exporter les événements, entrez un nom pour le fichier CSV exporté et cliquez sur **EXPORTER**. Vous êtes redirigé vers la page Journal d'activité sur laquelle un message d'état s'affiche en haut de la page.
6. Pour télécharger le fichier, cliquez sur **Téléchargements** dans le menu de gauche.
7. Dans la colonne Action du fichier exporté, cliquez sur le lien **Télécharger**.
8. Pour afficher le contenu du fichier, double-cliquez sur le fichier dans la liste Téléchargements. Les champs Nom de l'événement, Description, Type, Initié par, État, Nom du site, Nom du dispositif Edge, Heure, Nom de la ressource, ID et Gravité sont inclus dans le fichier.

Détails sur les données d'Horizon Universal Console en temps réel

Notez que les données et les informations affichées sur des écrans spécifiques dans Horizon Universal Console peuvent être retardées et ne pas refléter la situation en temps réel. Les données de surveillance proviennent d'Horizon Agent et sont envoyées au lac de données Workspace ONE Intelligence. Horizon Universal Console interroge le lac de données pour remplir les tableaux de bord.

Le traitement de bout en bout des données de surveillance signalées par l'agent prend du temps et peut entraîner un retard dans l'affichage dans Horizon Universal Console. Le délai est d'environ cinq minutes en moyenne. Dans le pire des cas, ce traitement de bout en bout peut entraîner un retard de 30 minutes au maximum.

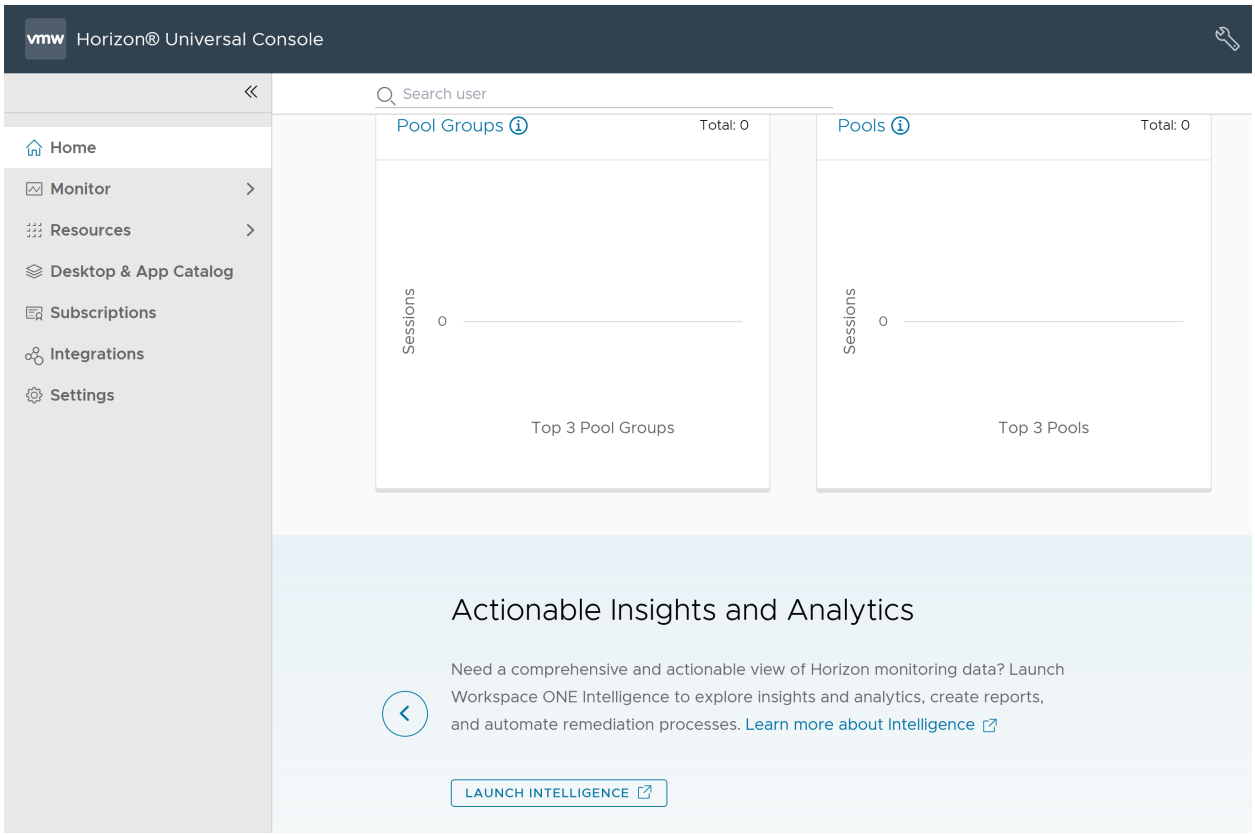
Les écrans d'Horizon Universal Console suivants peuvent subir des retards lors de l'extraction des données du lac de données Workspace ONE Intelligence.

- Page d'accueil d'Horizon Universal Console.
  - Erreurs
  - Sessions et performances de VM
  - Données d'utilisation affichées pour les groupes de pools, les pools et les instances d'Unified Access Gateway
- Informations de session Horizon affichées sur les pages suivantes.
  - **Ressources > Pools**, cliquez sur le Nom d'un pool spécifique pour afficher les détails des sessions lancées sur ce pool spécifique.
    - Page Présentation
    - Page Sessions
  - **Ressources > Groupes de pools**, cliquez sur le nom d'un groupe de pools spécifique pour afficher les détails des sessions lancées sur ce groupe de pools spécifique.
    - Page Présentation
    - Page Sessions
  - Lors de l'utilisation de la fonctionnalité Support technique/Fiche utilisateur, un administrateur tente d'accéder aux détails d'une VM ou d'une session spécifique sur la page Détails de la VM.

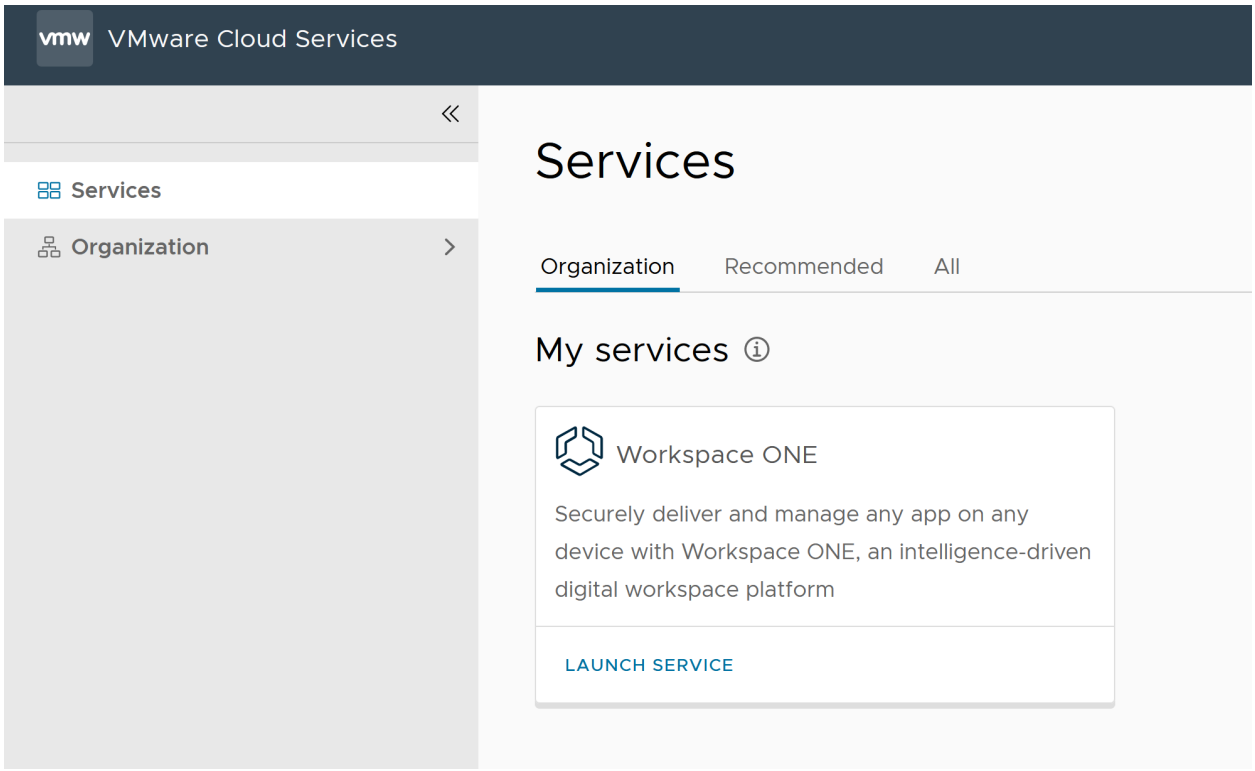
Surveillance d'Horizon Cloud dans Workspace ONE Intelligence

Une fois votre déploiement d'Horizon Cloud intégré à Workspace ONE Intelligence, vous pouvez utiliser Workspace ONE Intelligence pour afficher les tableaux de bord Horizon Cloud et créer des rapports.

Vous trouverez Workspace ONE Intelligence dans la section **Informations et analyse exploitables** de la page d'accueil d'Horizon Universal Console.



Lorsque vous lancez le service Workspace ONE, vous pouvez consulter tous les services que vous êtes autorisé à afficher avec votre licence.



Pour plus d'informations sur l'exploration et l'affichage des tableaux de bord Horizon Cloud et la création de rapports, reportez-vous à la rubrique « Intégration de VMware Horizon » dans le document *Produits VMware Workspace ONE Intelligence*.

Configuration de la surveillance des données d'Horizon Edge Agent pour Horizon Edge avec Workspace ONE

Pour Horizon Agent version 2212, vous pouvez activer la surveillance d'Horizon Agent pour le dispositif Horizon Edge (Horizon 8 et Microsoft Azure) afin de collecter des mesures à partir des VM qui s'affichent sur Workspace ONE et Horizon Universal Console.

Procédure

1. Connectez-vous à votre console vCenter.
2. Téléchargez et installez Horizon Agent.
   - Pour Horizon Agent version 2212, téléchargez Horizon Agent et effectuez une installation silencieuse qui inclut la transmission du paramètre `HORIZON_MONITOR_ENABLED=1`, par exemple, `horizon.exe /s /v "/qn HORIZON_MONITOR_ENABLED=1"`. Pour plus d'informations, reportez-vous à la section Propriétés de l'installation silencieuse d'Horizon Agent.

- Pour Horizon Agent version 2303 ou ultérieure, téléchargez et installez Horizon Agent. Pour la version 2303, la surveillance de la version d'Horizon Agent est activée par défaut et vos données sont envoyées au cloud Workspace ONE.

  Note Si vous ne souhaitez pas que l'agent collecte des mesures et désactive la surveillance, contactez le support client.

3. Redémarrez la machine virtuelle.
4. Pour Horizon Agent version 2212 uniquement, accédez au registre et vérifiez si l'indicateur, `HKLM\Software\VMware, Inc.\VMware HzMon\enabled=1`, est activé.
5. Confirmez que les données de session et d'utilisation de la VM s'affichent sur le tableau de bord Workspace ONE et Horizon Universal Console.

Surveillance des données d'infrastructure d'Passerelle Horizon Edge et d'Unified Access Gateway dans un environnement Horizon 8

Lorsque vous disposez d'une licence Horizon Universal et que vous déployez un dispositif Horizon Edge dans un environnement Horizon 8, vous avez accès à l'onglet **Surveillance de l'infrastructure**, qui vous permet de surveiller les composants d'infrastructure de cette instance d'Horizon Edge. Les données d'infrastructure se composent actuellement d'informations sur les instances d'Unified Access Gateway et d'Horizon Connection Server pour ce dispositif Horizon Edge.

Pour accéder à l'onglet **Surveillance de l'infrastructure**, sélectionnez **Ressources > Capacité**, puis, sur la page Dispositifs Horizon Edge, cliquez sur le nom d'un dispositif Horizon Edge dont la valeur est « Centre de données privé » dans la colonne source. Sur la page de détails d'Horizon Edge, cliquez sur l'onglet **Surveillance de l'infrastructure**. Pour apporter des modifications à ce dispositif Horizon Edge, reportez-vous à la section Afficher les détails et effectuer des actions sur un dispositif Horizon Edge spécifique.

Serveur de connexion

La section Serveur de connexion répertorie toutes les instances d'Horizon Connection Server déployées pour ce dispositif Horizon Edge spécifique. Pour afficher les données d'infrastructure sur une instance d'Horizon Connection Server spécifique, cliquez sur **Afficher** pour cette dernière. Une page s'ouvre et fournit des détails sur cette instance d'Horizon Connection Server.

Les informations suivantes sont disponibles pour cette instance d'Horizon Connection Server spécifique :

- Pendant une période spécifiée, jusqu'à 24 heures, le pourcentage de CPU disponible utilisé
- Pendant une période spécifiée, jusqu'à 24 heures, le pourcentage de mémoire disponible utilisé
- Nombre actuel de sessions utilisées
- Nombre actuel d'utilisateurs

- Dans la section **Services**, la santé de composants Horizon Connection Server dépendants
- Dans la section **Certificate**, la validité du certificat Horizon Connection Server

Les données peuvent vous aider à déterminer la santé et l'utilisation des instances d'Horizon Connection Server et des services associés. En outre, les données peuvent aider à déterminer le dimensionnement requis des instances d'Horizon Connection Server individuelles et du cluster pour ce dispositif Horizon Edge.

Unified Access Gateway

Vous pouvez afficher les dispositifs UAG et leur état global. Pour surveiller un serveur UAG spécifique, cliquez sur **Afficher** pour cette instance d'UAG. Une page s'ouvre avec les informations suivantes :

- Pendant une période spécifiée, jusqu'à 24 heures, le pourcentage de CPU disponible utilisé
- Pendant une période spécifiée, jusqu'à 24 heures, le pourcentage de mémoire disponible utilisé
- Nombre actuel de sessions utilisées
- Dans la section **Services**, la santé d'un module UAG
- Dans la section **Configuration**, détails de la configuration du serveur UAG

Surveillance d'Passerelle Horizon Edge à l'aide de SNMP

Cet article décrit comment activer et configurer les paramètres SNMP (Simple Network Management Protocol) pour la Passerelle Horizon Edge. Cette configuration vous permet de surveiller les événements clés Passerelle Horizon Edge au moyen d'un système de gestion de réseau.

Fonctionnement de la surveillance SNMP avec la Passerelle Horizon Edge

Passerelle Horizon Edge prend en charge la surveillance au moyen d'interruptions SNMP provenant du dispositif Passerelle Horizon Edge lorsque certains événements se produisent. Ces interruptions informent le système de gestion du réseau de l'événement déclencheur ou de la condition.

Note La Passerelle Horizon Edge fonctionne uniquement en tant qu'émetteur d'interruptions et ne prend pas en charge d'autres opérations SNMP, telles que la réception d'une opération `GET`, `GETBULK` ou `GETNEXT`.

Pour activer la surveillance SNMP pour la Passerelle Horizon Edge, vous devez configurer la surveillance SNMP, comme décrit dans cet article.

Les fichiers MIB (Management Information Base) contiennent les définitions des interruptions qui peuvent être fournies par les périphériques gérés. Les fichiers MIB définissent les objets gérés, décrits par les identificateurs d'objets (OID) et les variables disposés dans une hiérarchie. Vous pouvez télécharger les fichiers MIB requis à l'aide du lien fourni ultérieurement dans cet article.

Événements Passerelle Horizon Edge que vous pouvez vérifier avec les interruptions SNMP

Une fois que vous avez activé et configuré le service SNMP pour le dispositif, Passerelle Horizon Edge prend en charge les interruptions SNMP pour les événements suivants.

- Actuellement, la surveillance des échecs de transfert de licence est prise en charge.

Chaque événement déclenche l'émission d'une interruption SNMP du dispositif vers le système de gestion du réseau.

Configuration de la surveillance SNMP pour la Passerelle Horizon Edge

Le processus de configuration SNMP se compose des étapes générales suivantes :

- Étape 1 : téléchargez les fichiers MIB VMware à utiliser par le système de gestion du réseau.
- Étape 2 : activez et configurez le service SNMP dans Horizon Universal Console.
- Étape 3 : utilisez Horizon Universal Console pour afficher l'ID du moteur Passerelle Horizon Edge.

Reportez-vous aux sections suivantes pour obtenir les conditions préalables et les détails de chaque étape.

Conditions préalables

- Déployez un dispositif Horizon Edge avec une licence Horizon Plus ou une licence universelle Horizon. Reportez-vous à la section Déploiement d'Horizon Edge dans votre fournisseur de capacité de ressources
- Vous devez disposer d'un récepteur d'interruptions SNMPv3 configuré qui peut recevoir des interruptions SNMP.
- Assurez-vous que la Passerelle Horizon Edge peut accéder au récepteur SNMP. En général, le port par défaut pour SNMP est 162.

Note La surveillance basée sur SNMP est prise en charge pour Passerelle Horizon Edge uniquement.

Étape 1 : télécharger les fichiers MIB et les OID VMware

La norme RFC 2578 de la structure des informations de gestion (SMI) est la syntaxe utilisée pour écrire des fichiers MIB (Management Information Base) pour des produits et des fonctions spécifiques. Ces fichiers MIB font l'objet d'un contrôle de version indépendamment du produit et peuvent être utilisés pour désigner les types d'événements et les informations liées aux données d'événement.

Pour télécharger ces fichiers MIB, accédez à l'article 1013445 de la base de connaissances VMware et téléchargez VMware-mibs-8.6.0NX-22397641.

Pour télécharger les identificateurs d'objets (OID) utilisés par les fichiers MIB, accédez à l'article 2054359 de la base de connaissances VMware.

Étape 2 : activer et configurer le service SNMP à l'aide d'Horizon Universal Console

Vous pouvez accéder aux paramètres du service SNMP par le biais d'Horizon Universal Console.

1 Dans Horizon Universal Console, sélectionnez **Intégrations** et cliquez sur **Gérer** dans la vignette SNMP.

2 Sur la page SNMP, cliquez sur **Ajouter**.

L'assistant **Ajouter SNMP** démarre.

3 Spécifiez les paramètres pour le nom de la configuration, le nom d'utilisateur et le niveau de sécurité comme décrit dans le tableau suivant.

Paramètre	Description
Version SNMP	Cette version prend uniquement en charge SNMPv3.
Nom de la configuration SNMPv3	Nom donné à l'utilisateur pour identifier la configuration du récepteur.
Nom d'utilisateur USM SNMPv3	Configurez l'utilisateur du modèle de sécurité basé sur l'utilisateur (USM) SNMPv3 qui peut accéder aux informations de surveillance SNMP. Le nom d'utilisateur doit comporter entre 8 et 31 caractères et contenir uniquement des lettres et des chiffres.
Niveau de sécurité SNMPv3	Spécifiez si vous voulez utiliser un algorithme d'authentification facultatif, avec ou sans algorithme de confidentialité, pour le service SNMP. L'authentification est utilisée pour garantir l'identité des utilisateurs. La confidentialité autorise le chiffrement des messages SNMPv3 pour garantir la confidentialité des données. L'authentification et la confidentialité sont facultatives. Cependant, vous devez activer l'authentification pour activer la confidentialité.

4 (Facultatif) Si vous avez spécifié un niveau de sécurité qui inclut l'authentification, configurez les détails de l'authentification comme décrit dans le tableau suivant.

Paramètre	Description
Algorithme d'authentification SNMPv3	Spécifiez l'algorithme d'authentification utilisé pour établir l'identité des utilisateurs SNMP.
Mot de passe d'authentification SNMPv3	Configurez le mot de passe requis par l'algorithme d'authentification pour établir l'identité des utilisateurs. Le mot de passe d'authentification doit comporter entre 8 et 31 caractères.
Confirmer le mot de passe d'authentification	Entrez de nouveau le mot de passe d'authentification.

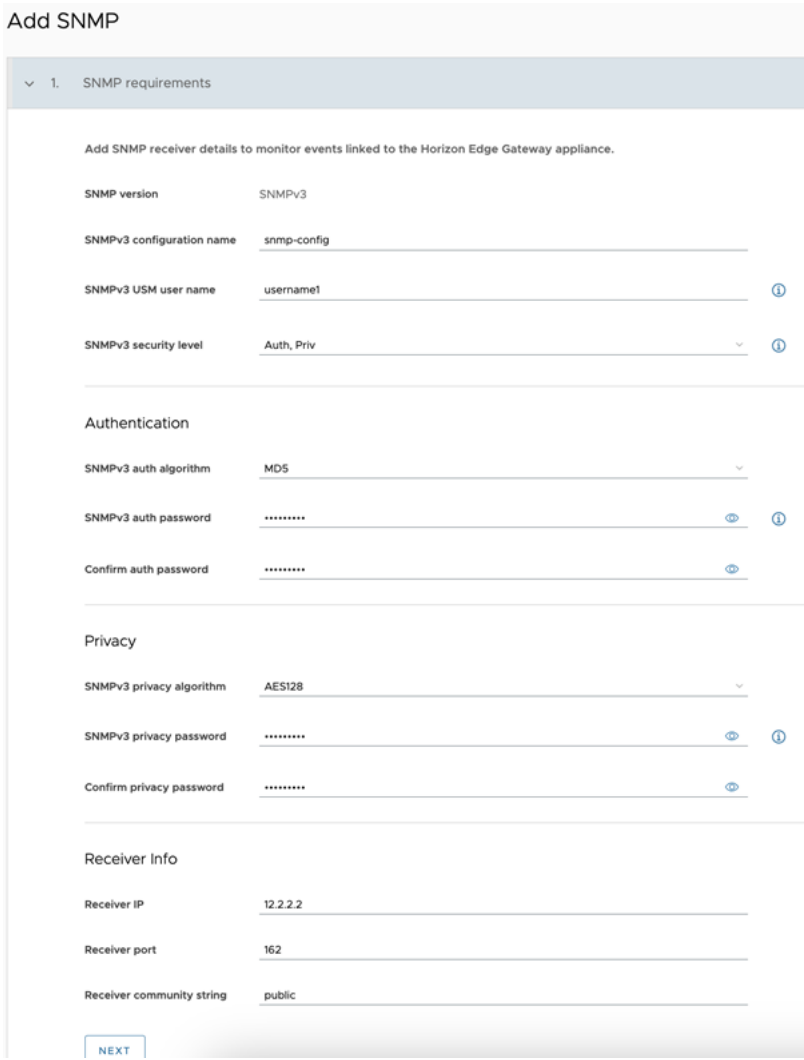
5 (Facultatif) Si vous avez spécifié le niveau de sécurité qui inclut à la fois l'authentification et la confidentialité, configurez les détails de confidentialité comme décrit dans le tableau suivant.

Paramètre	Description
Algorithme de confidentialité SNMPv3	Spécifiez l'algorithme de confidentialité utilisé pour chiffrer les messages SNMP.
Mot de passe de confidentialité SNMPv3	Configurez le mot de passe requis par l'algorithme de confidentialité pour générer une clé de chiffrement. Le mot de passe de confidentialité doit comporter entre 8 et 31 caractères.
Confirmer le mot de passe de confidentialité	Entrez de nouveau le mot de passe de confidentialité.

6 Spécifiez les détails de l'adresse IP et du port du récepteur SNMP pouvant recevoir des interruptions SNMP en provenance de la Passerelle Horizon Edge, comme décrit dans le tableau suivant, puis cliquez sur **Suivant**.

Paramètre	Description
Adresse IP du récepteur	Spécifiez l'adresse IP du système de gestion de réseau qui peut recevoir les interruptions SNMP.
Port du récepteur	Spécifiez le numéro de port utilisé par le système de gestion du réseau pour recevoir les interruptions.
Chaîne de communauté du récepteur	Entrez la chaîne de communauté utilisée par le système de gestion du réseau pour confirmer que les interruptions reçues proviennent d'Passerelle Horizon Edge.

La capture d'écran suivante fournit un exemple de formulaire Ajouter SNMP avec les paramètres configurés.

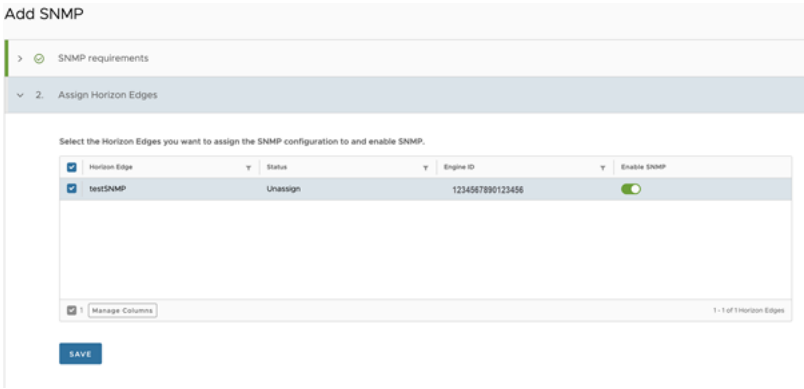


Si la configuration réussit, un message s'affiche et indique qu'une configuration SNMP est ajoutée.

7 Dans la section Attribuer les dispositifs Dispositifs Horizon Edge, sélectionnez le dispositif Horizon Edge à attribuer à la configuration SNMP.

Vous pouvez attribuer plusieurs dispositifs Dispositifs Horizon Edge à une seule configuration SNMP. Cependant, vous ne pouvez pas attribuer un dispositif Horizon Edge à plusieurs configurations SNMP. Lorsqu'un dispositif Horizon Edge est attribué à une configuration SNMP, il ne s'affiche plus dans la liste des dispositifs Dispositifs Horizon Edge.

Lorsque vous attribuez une configuration SNMP à un dispositif Horizon Edge, l'ID du moteur est créé.



8 Pour activer la surveillance SNMP des dispositifs Dispositifs Horizon Edge sélectionnés, assurez-vous que l'option **Activer SNMP** est activée.

Note L'état par défaut de l'option **Activer SNMP** est activé lors de l'association d'Dispositifs Horizon Edge.

9 Cliquez sur **Enregistrer**.

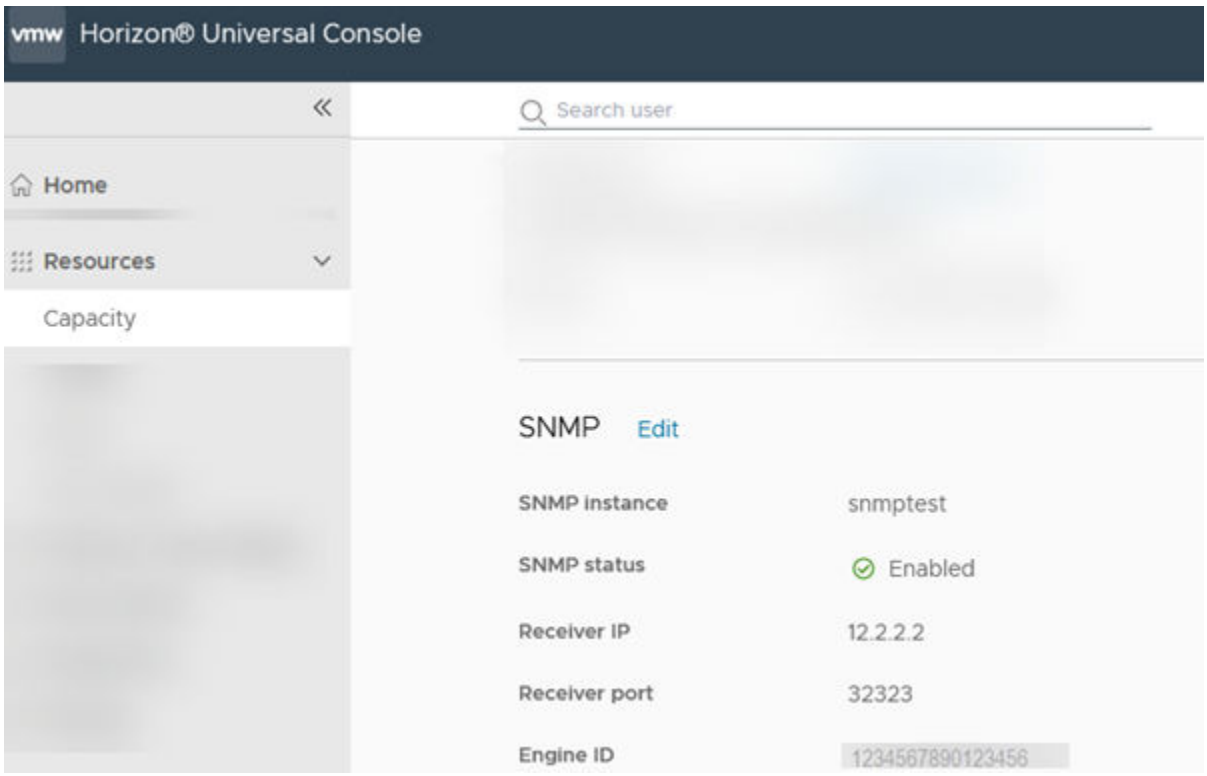
Étape 3 : obtenir l'ID du moteur SNMP pour une Passerelle Horizon Edge spécifique à l'aide d'Horizon Universal Console

Pendant le processus d'activation de SNMP, Passerelle Horizon Edge génère automatiquement un ID de moteur SNMP unique que votre système de gestion réseau doit utiliser. L'ID du moteur est utilisé avec une fonction de hachage pour générer des clés pour l'authentification et le chiffrement des messages SNMP v3.

Note Vous avez besoin de l'ID du moteur SNMP pour configurer le récepteur SNMP et identifier les messages d'interruption SNMP émis à partir de cette Passerelle Horizon Edge.

- Utilisez Horizon Universal Console pour accéder à l'ID du moteur SNMP d'un dispositif Horizon Edge.
  a Sélectionnez **Ressources > Capacité > .**
  b Cliquez sur le nom d'un dispositif Horizon Edge auquel vous avez attribué une configuration SNMP.
  c Faites défiler l'écran jusqu'à la section SNMP et recherchez la valeur ID du moteur.

  La capture d'écran suivante sert d'exemple d'ID du moteur SNMP généré automatiquement tel qu'il s'affiche dans Horizon Universal Console.



Étape suivante

Vous pouvez revenir à la page SNMP à tout moment pour modifier ou supprimer une configuration SNMP existante. Vous pouvez modifier une configuration SNMP pour modifier les détails du récepteur SNMP ou les associations SNMP. Pour supprimer une configuration SNMP, modifiez d'abord la configuration pour annuler l'attribution des Dispositifs Horizon Edge affectés.

Surveillance des licences d'abonnement Horizon pour les dispositifs Horizon 8 Edge

La licence d'abonnement Horizon repose sur une chaîne de communication opérationnelle entre le déploiement d'Horizon Edge, Horizon Connection Server et le service de licence Horizon Cloud. Le service de licence se synchronise avec le dispositif Horizon 8 Edge toutes les 24 heures. Des échecs de synchronisation de licence peuvent se produire, ce qui peut entraîner une interruption de service. Horizon Cloud Service - next-gen tente de vous informer des échecs de synchronisation de licence de différentes manières. L'utilisation de Horizon Universal Console pour surveiller l'état de synchronisation de vos licences d'abonnement et résoudre les problèmes de synchronisation constitue l'une des manières de rester informé.

Si l'un des liens de la chaîne de communication de licence n'est plus opérationnel, la synchronisation des licences échoue et le dispositif Horizon 8 Edge n'est pas conforme aux conditions générales de la licence d'abonnement. Toutefois, la licence d'abonnement reste valide et le dispositif Horizon Edge reste opérationnel pour vous permettre de rechercher et corriger

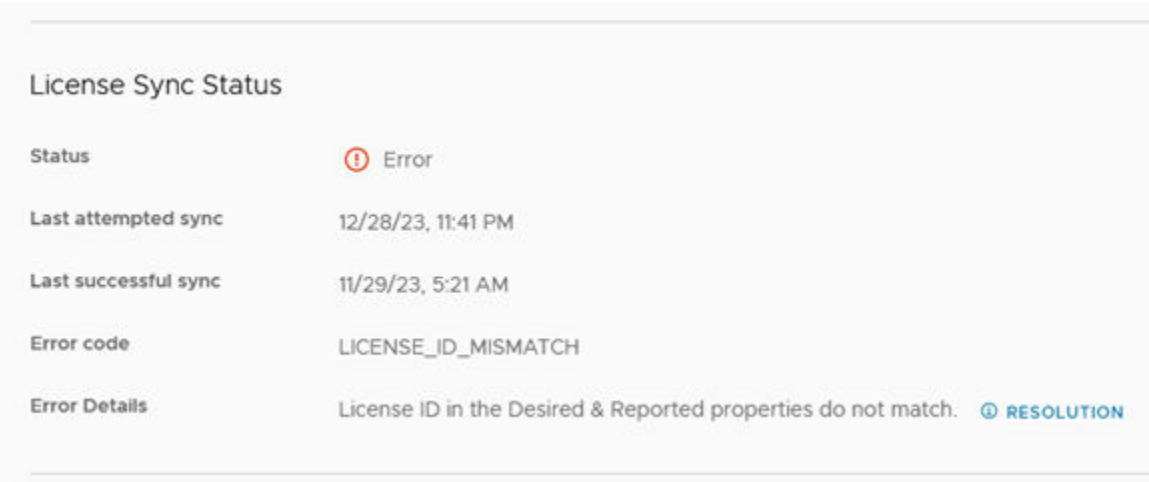
la cause de l'échec de la synchronisation. Si l'échec persiste pendant une période prolongée, les services vers le dispositif Horizon Edge sont interrompus et le dispositif Horizon Edge n'est plus opérationnel. Ensuite, les utilisateurs finaux ne peuvent pas se connecter à des applications et des postes de travail distants sur le dispositif Horizon Edge.

Les sections suivantes décrivent les différentes façons dont Horizon Cloud Service - next-gen vous fournit des informations sur l'état de synchronisation des licences.

État de synchronisation des licences d'abonnement sur la page Détails du dispositif Horizon Edge

Vous pouvez afficher l'état d'une synchronisation des licences d'abonnement sur la page de détails d'un dispositif Horizon 8 Edge spécifique. Pour les échecs de synchronisation des licences, vous pouvez utiliser les informations sur l'état de synchronisation des licences d'abonnement pour résoudre les problèmes.

Sélectionnez **Ressources > Capacité** et lorsque l'onglet **Dispositifs Horizon Edge** est sélectionné, cliquez sur le nom d'un dispositif Horizon 8 Edge et faites défiler la liste jusqu'à la section État de synchronisation des licences d'abonnement.



Note La section État de synchronisation des licences d'abonnement n'est disponible que pour les dispositifs Edge de type Horizon 8.

La section État de synchronisation des licences d'abonnement répertorie les types d'informations suivants.

État	L'état de la synchronisation des licences peut être l'un des suivants. ■ **Erreur** ■ **Réussi**
Dernière tentative de synchronisation	Date d'exécution de la tâche de synchronisation des licences la plus récente
Dernière synchronisation réussie	Date de la synchronisation réussie des licences la plus récente

Code d'erreur	Code d'erreur (le cas échéant).
Détails de l'erreur	Informations spécifiques sur l'erreur, notamment une info-bulle résolution.

État de synchronisation des licences d'abonnement dans les journaux d'activité de l'administrateur

Les journaux d'activité de l'administrateur incluent des informations sur l'état de synchronisation des licences.

Pour accéder à la page Journal d'activité, sélectionnez **Surveiller > Journal d'activité**. La page s'ouvre avec l'onglet Admin sélectionné. Reportez-vous à la section Surveillance de l'activité de l'administrateur et de l'utilisateur final sur la page Journal d'activité.

Notifications d'alerte de synchronisation des licences

Si un échec de synchronisation des licences se produit plusieurs jours à la suite, chaque dispositif Horizon 8 Edge affecté envoie des notifications à Horizon Universal Console sur l'échec de synchronisation des licences à partir du troisième jour. Reportez-vous à la section Notifications dans Horizon Cloud Service - next-gen.

E-mails d'alerte de synchronisation des licences

Si un échec de synchronisation des licences se produit plusieurs jours à la suite, le système envoie un e-mail vous informant de l'échec de synchronisation des licences d'abonnement à partir du troisième jour.

Gestion du logiciel Horizon Agent

Horizon Agent est le logiciel agent requis qui permet le couplage des VM avec Horizon Cloud. Vous devez gérer les agents pour vous assurer qu'ils sont à jour avec les nouvelles fonctionnalités et les nouveaux correctifs de bogues.

Sur les machines virtuelles, cet agent communique avec Horizon Cloud Service pour fournir des fonctionnalités telles que l'intermédiation, le contrôle des connexions, l'impression intégrée et l'accès à des périphériques USB connectés localement.

Maintien des versions d'Horizon Agent actualisées

Horizon Cloud utilise différentes méthodes pour vous informer que le logiciel Horizon Agent déployé sur les VM ne dispose pas de la version la plus actualisée.

Plusieurs pages d'Horizon Universal Console liées aux pools, aux groupes de pools et aux images vous informent lorsque l'instance d'Horizon Agent associée est obsolète. Il est recommandé de maintenir la version de l'agent à jour.

Étiquettes de la version d'Horizon Agent

Les étiquettes de la version d'Horizon Agent indiquent si la version de l'agent est à jour ou non sur une ressource (groupes de pools, pools ou images). Si l'agent n'est pas à jour, les étiquettes indiquent également le niveau d'obsolescence des agents.

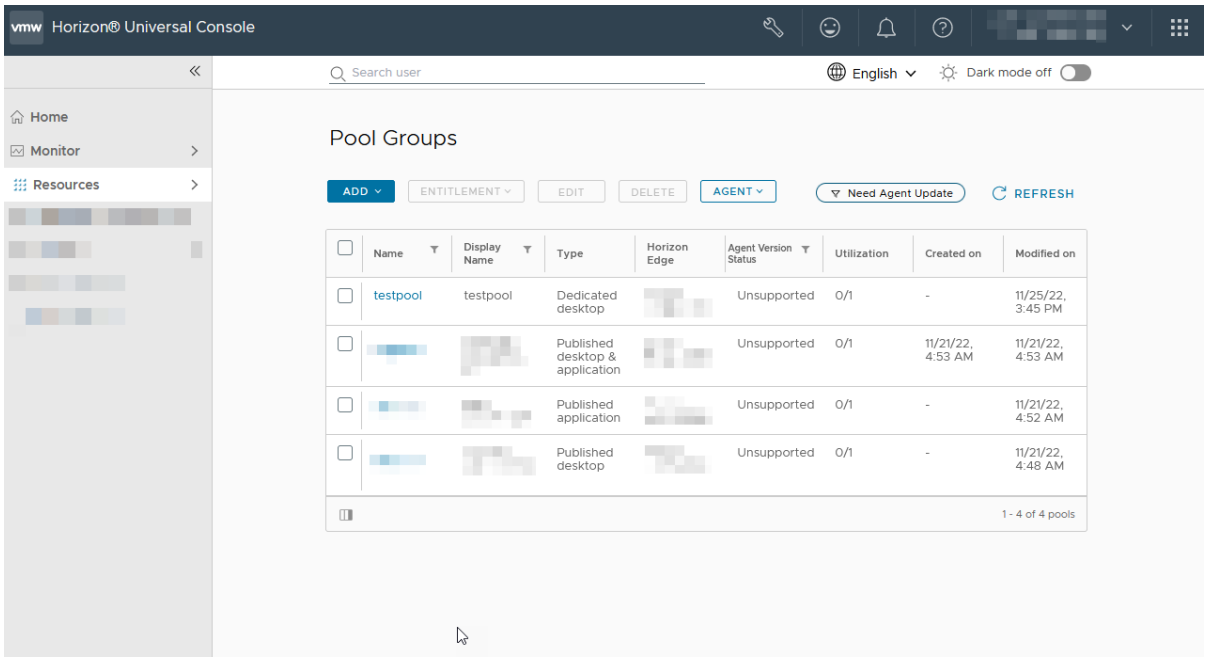
Étiquettes de la version d'Horizon Agent	Description
La dernière	La dernière version de l'agent est installée sur les VM.
Obsolète	Certaines VM comportent des agents obsolètes.
Non pris en charge	Certaines VM comportent des agents obsolètes et non pris en charge.
À risque	Certaines VM comportent des agents présentant des problèmes de sécurité ou de fonctionnalité critiques.

Exemple d'informations de la version d'Horizon Agent

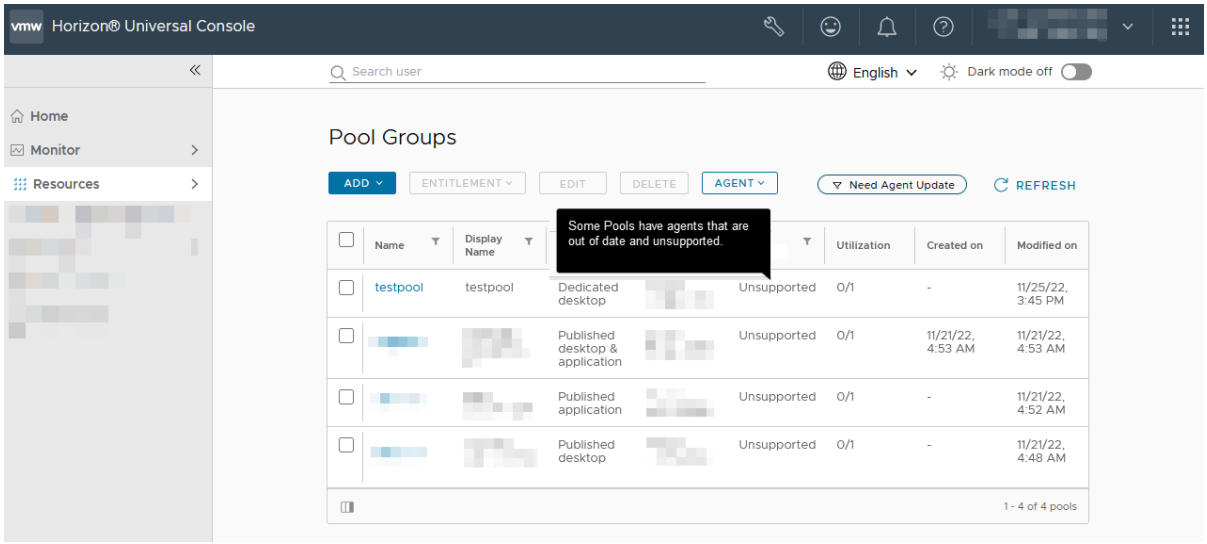
Les captures d'écran suivantes fournissent un exemple de présentation des informations de statistiques de version d'Horizon Agent. Cet exemple particulier concerne la page Groupes de pools.

Exemple de page Groupes de pools

La page Groupes de pools inclut la colonne État de la version de l'agent. Dans la capture d'écran qui suit, chacun des groupes de pools dispose d'une étiquette État de la version de l'agent Non prise en charge.



Passez la souris sur une étiquette État de la version de l'agent pour afficher la description, comme indiqué dans la capture d'écran suivante.



Mettre à jour le logiciel Horizon Agent sur les VM de postes de travail dédiés

Les mises à jour d'Horizon Agent peuvent inclure de nouvelles fonctionnalités et de nouveaux correctifs de bogues. Utilisez cette procédure pour mettre à jour les logiciels Horizon Agent installés sur vos VM de poste de travail dédié.

Note Lorsque votre environnement de nouvelle génération contient une migration de première génération qui n'est pas encore finalisée, le système empêche l'exécution de cette procédure de mise à jour de l'agent, même sur les groupes de pools qui ont été créés directement dans l'environnement de nouvelle génération. Dans ce scénario, lorsque vous cliquez sur **Mettre à jour l'agent**, la console affiche un message d'instruction sur la nécessité de finaliser la migration.

Pour mettre à jour les logiciels Horizon Agent installés sur vos VM de poste de travail dédié, utilisez Horizon Universal Console. Démarrez le processus de mise à jour de l'agent sur la page Groupes de pools et le focus du processus passe des groupes de pools aux pools. Activez ensuite la mise à jour de l'agent au niveau du pool pour que le système mette à jour les logiciels Horizon Agent sur vos VM de poste de travail dédié vers la dernière version disponible.

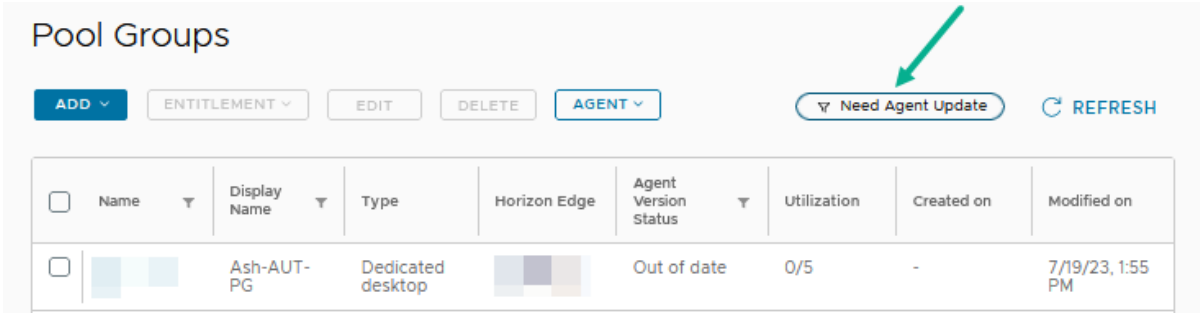
Attention Lorsque l'opération de mise à jour de l'agent est en cours, vous devez vous assurer qu'aucune autre activité planifiée ne peut entraîner d'opération de changement d'alimentation dans les VM de poste de travail du groupe de pools. Informez, par exemple, vos autres administrateurs qu'ils évitent de mettre manuellement hors ou sous tension l'une de ces VM de poste de travail. Vérifiez ensuite que les planifications de gestion de l'alimentation configurées dans ce groupe de pools n'entraînent pas la mise sous ou hors tension des postes de travail lors de l'exécution des tâches de mise à jour de l'agent. En cas d'opération de changement d'alimentation sur une machine virtuelle de poste de travail tandis que le système exécute ses tâches de mise à jour de l'agent sur la VM, des résultats imprévus peuvent se produire et laisser cette VM de poste de travail dans un état qui nécessite la récupération manuelle.

Il est recommandé de modifier le groupe de pools et de supprimer les planifications configurées de gestion de l'alimentation pour éliminer le risque d'opération de changement d'alimentation lors de l'exécution des tâches de mise à jour de l'agent.

Procédure

1 Dans Horizon Universal Console, accédez à la page **Groupes de pools**.

La capture d'écran suivante de la page **Groupes de pools** illustre l'option **Mise à jour de l'agent requise**.



2 (Facultatif) Pour vérifier que la dernière mise à jour de l'agent est disponible pour le filtre **Mise à jour de l'agent requise**, vous pouvez rechercher les mises à jour de l'agent pour les groupes de pools.

Note Une recherche des mises à jour peut prendre quelques minutes, selon le nombre de groupes de pools et de pools.

Horizon Cloud recherche automatiquement les mises à jour de l'agent tous les jours pour les postes de travail dans les groupes de pools. L'étiquette de l'action **Rechercher les mises à jour** affiche l'heure de la dernière analyse. Pour rechercher immédiatement les groupes de pools dans les agents, utilisez l'action **Rechercher les mises à jour** comme suit.

a Sélectionnez **Agent > Rechercher les mises à jour**.

Ce processus s'exécute en arrière-plan. L'état s'affiche sur la page Journal d'activité.

b Pour afficher la progression, accédez à la page Journal d'activité.

Pour plus d'informations sur le journal d'activité, reportez-vous à la section Surveillance de l'activité de l'administrateur et de l'utilisateur final sur la page Journal d'activité.

3 Pour filtrer la liste afin qu'elle se compose uniquement de groupes de pools qui contiennent des VM de poste de travail remplissant les conditions de mise à jour de l'agent, cliquez sur l'option **Mise à jour de l'agent requise**.

Si vous avez recherché les mises à jour à l'étape précédente, les données de cette liste incluent les mises à jour détectées lors de l'analyse. Sinon, la liste se compose de données calculées à partir d'analyses précédentes, telles que les analyses quotidiennes automatiques ou pour des événements spécifiques.

4 Sélectionnez un ou plusieurs groupes de pools.

5 Sélectionnez **Agent > Mettre à jour l'agent**.

Note Lorsque votre environnement contient une migration de première génération qui n'est pas encore finalisée, la console empêche l'exécution de l'assistant de mise à jour de l'agent.

L'assistant **Mettre à jour l'agent** démarre et présente une page qui fractionne les groupes de pools sélectionnés en une liste de pools correspondants, chacun d'eux contenant une ou plusieurs VM remplissant les conditions de mise à jour de l'agent.

6 Sélectionnez les pools dans la liste contenant les VM à mettre à jour, puis cliquez sur **Suivant**.

7 Remplissez le formulaire Détails et cliquez sur **Enregistrer**.

Option	Description
Ignorer les VM ayant des utilisateurs actifs	Sélectionnez cette option pour ignorer la mise à jour d'Horizon Agent pour les sessions actives ou déconnectées. Si cette option n'est pas sélectionnée, les utilisateurs connectés aux VM lorsque la mise à jour commence recevront un avertissement au bout de 5 minutes, puis seront déconnectés de force.
Délai d'expiration de la tâche	Définissez la période pendant laquelle le système doit continuer à mettre à jour automatiquement les agents. Pour exécuter des mises à jour uniquement pendant une période spécifique, vous pouvez définir une courte période, même si vous sélectionnez plusieurs modèles et VM. Un lot de VM peut prendre entre 20 et 60 minutes en fonction de l'état des VM et de tout autre délai d'attente et de nouvelles tentatives en cours. Par exemple, si vous disposez de plus de 600 VM à mettre à jour avec 30 VM en simultanéité, vous devez calculer la période comme suit : ■ Nombre de lots : 600/30 = 20 lots ■ Délai d'expiration de la tâche : 20 × 60 = 1 200 minutes Vous devez définir le délai d'expiration de la tâche sur 1 200 minutes, ce qui constitue une période beaucoup plus longue que celle généralement requise pour l'exécution des mises à jour. **Note** Le système ne tente pas de mettre à jour les VM qui rencontrent une erreur pendant le processus de mise à jour.
Simultanéité	Définissez une limite au nombre de VM sur lesquelles le système tente de mettre à jour l'agent simultanément. Ce paramètre fonctionne en parallèle avec le paramètre **Seuil d'échec**. Idéalement, conservez le paramètre **Simultanéité** sur une valeur inférieure ou égale au paramètre **Seuil d'échec**.
Seuil d'échec	Nombre de VM pour lesquelles la mise à jour de l'agent est autorisée à échouer avant l'arrêt du processus de mise à jour. La configuration de ce seuil évite les échecs en masse. Lorsque le processus de mise à jour s'arrête en raison de l'échec des mises à jour de l'agent de VM, vous pouvez observer un nombre de VM ayant échoué supérieur à la valeur **Seuil d'échec**. Si vous devez vous assurer qu'il y a moins d'échecs que le nombre spécifié pour le paramètre **Seuil d'échec**, définissez la valeur **Simultanéité** sur 1. Cela signifie également que le processus de mise à jour de l'agent prendra longtemps, car il mettra à jour une seule VM à la fois. Il est recommandé de définir **Simultanéité** et **Seuil d'échec** de manière appropriée pour obtenir des résultats optimaux.
Arguments de ligne de commande	Dans la zone de texte **Arguments de ligne de commande**, ajoutez toutes les options de ligne de commande qui peuvent être appropriées à cette mise à jour.

Étape suivante

Le processus de mise à jour de l'agent s'exécute en arrière-plan et l'état s'affiche sur la page Journal d'activité. Accédez à la page Journal d'activité pour afficher la progression. Pour plus d'informations sur le journal d'activité, reportez-vous à la section Surveillance de l'activité de l'administrateur et de l'utilisateur final sur la page Journal d'activité.

Mettre à jour Horizon Agent sur des postes de travail flottants et à plusieurs sessions

Vous pouvez mettre à jour Horizon Agent sur des postes de travail flottants et à plusieurs sessions en mettant à jour une image existante ou en créant une image avec la dernière version d'Horizon Agent et en l'attribuant au pool de postes de travail.

Les postes de travail flottants et à plusieurs sessions étant supprimés et recréés à la demande, ils ne conservent pas les données utilisateur sur le disque du système d'exploitation. Pour mettre à jour Horizon Agent sur chaque poste de travail du pool, mettez à jour l'image avec la dernière version et attribuez-la au pool. Lorsque vous appliquez l'image mise à jour à l'aide de marqueurs d'image au pool, le service recrée ces postes de travail.

Pour utiliser une image existante pour mettre à jour Horizon Agent, créez une version de l'image avec la dernière version d'Horizon Agent en publiant la nouvelle version de l'image.

Procédure

1. Clonez une nouvelle version de l'image. Reportez-vous à la section Cloner une version de l'image.
2. Mettez à jour les logiciels et les applications si nécessaire.
3. Publiez l'image avec la dernière version d'Horizon Agent : sélectionnez l'installation de l'agent et les fonctionnalités requises. Reportez-vous à la section Publication d'une image.

   La version de l'image publiée dispose du logiciel Horizon Agent le plus récent.
4. Validez la version et le marqueur de l'image dans le pool de test s'ils ne sont pas validés lors de la publication de l'image.
5. Choisissez un marqueur associé à des pools existants et mettez-le à jour vers cette version de l'image si vous prévoyez d'actualiser tous les pools utilisant ce marqueur avec cette version d'image. Si vous prévoyez d'actualiser les pools individuellement, vérifiez qu'il existe un marqueur pour cette version de l'image publiée afin de l'attribuer à un pool de postes de travail. Reportez-vous à la section Modifier une version de l'image.

   Une fois le marqueur mis à jour, le service actualise ce poste de travail avec les paramètres configurés et tous les postes de travail actualisés disposent des derniers agents.

Réinstaller le logiciel Horizon Agent sur des VM de poste de travail dédié

La fonctionnalité de réinstallation permet de désinstaller l'agent existant de la VM et de réinstaller le dernier logiciel agent. La fonctionnalité de réinstallation fournit un mécanisme de récupération pour les échecs de mise à jour de l'agent par l'installation forcée et dans des situations spéciales où vous devez désinstaller et réinstaller le logiciel agent, comme décrit dans les cas d'utilisation suivants.

Ces derniers illustrent dans quels cas vous pouvez effectuer une réinstallation de l'agent.

- Si la mise à jour de l'agent sur les VM, comme décrit dans la section Mettre à jour le logiciel Horizon Agent sur les VM de postes de travail dédiés, échoue systématiquement.
- Pour désinstaller et réinstaller un agent en raison de mises à jour du système d'exploitation ou de problèmes du pilote de périphérique.

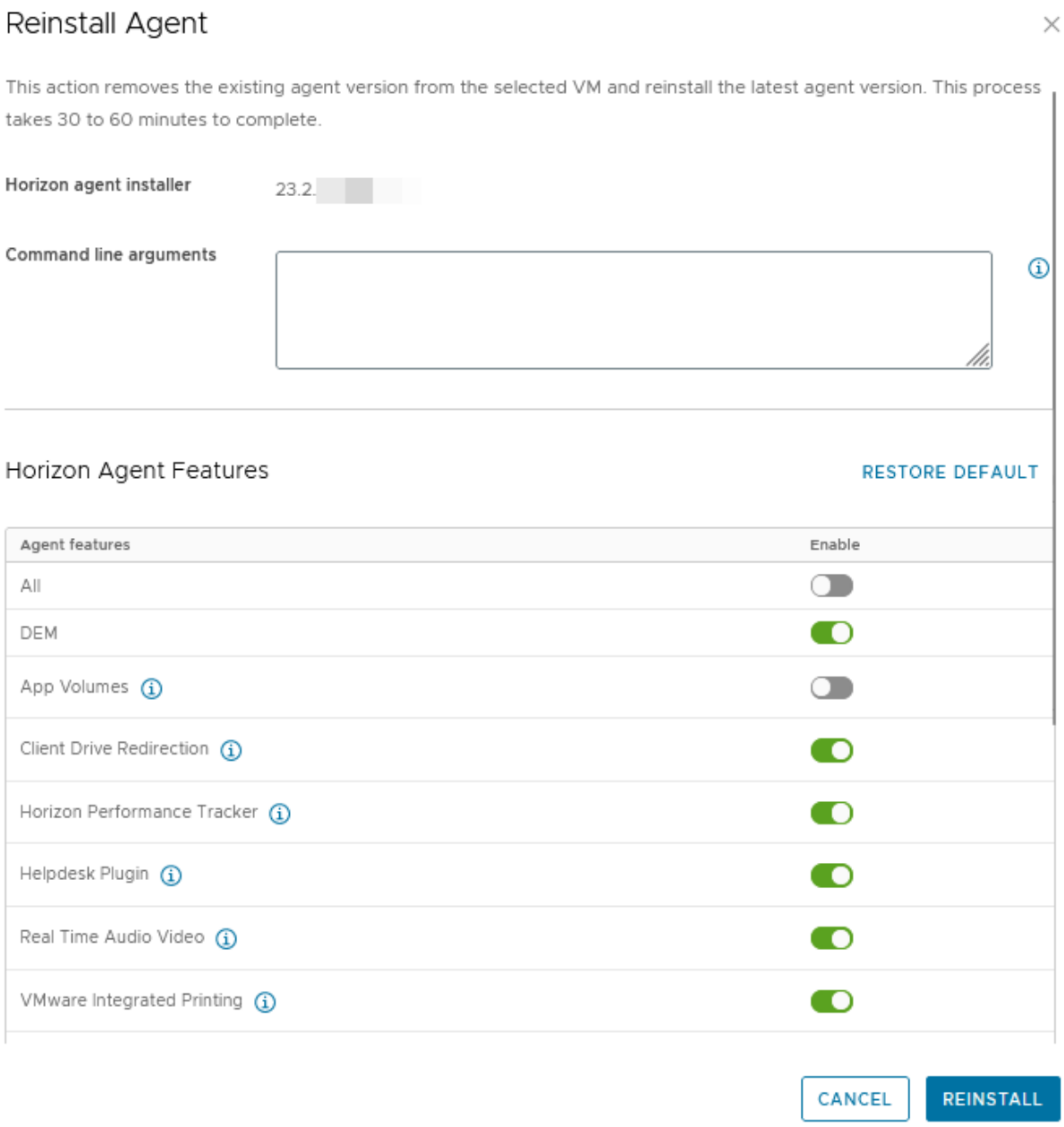
Note Lorsque votre environnement de nouvelle génération dispose d'une migration de première génération qui n'est pas encore finalisée, le système empêche l'exécution de cette procédure de réinstallation de l'agent. Après avoir cliqué sur **Agent > Réinstaller**, un message s'affiche sur la finalisation de la migration.

Procédure

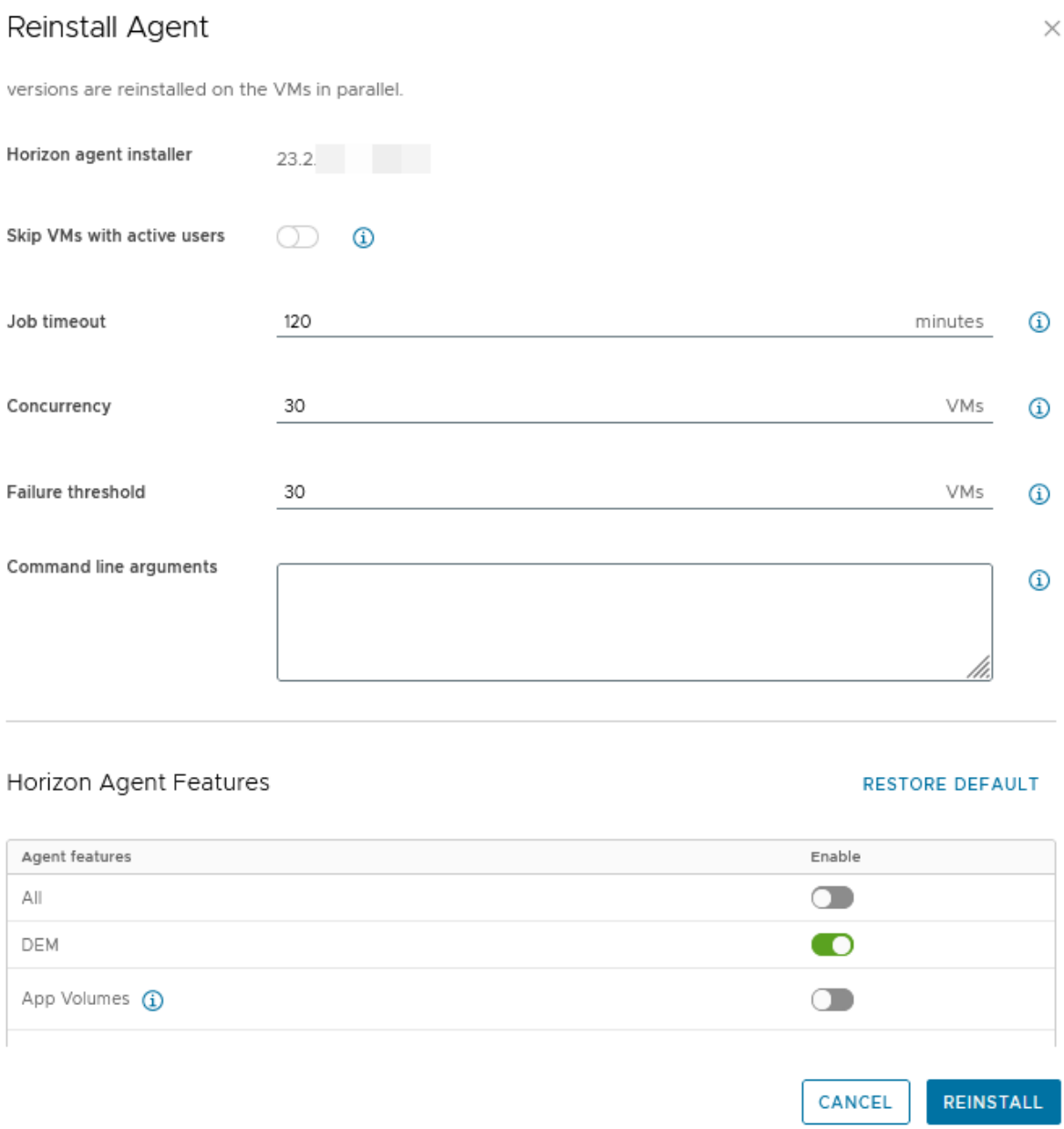
1. Dans Horizon Universal Console, accédez à la page **Groupes de pools**.
2. Sélectionnez des **VM**.
3. Sélectionnez une ou plusieurs machines virtuelles dans la liste.
4. Sélectionnez **Agent > Réinstaller**.

   La page Réinstaller l'agent s'ouvre. Cette page vous invite à fournir des informations. Les invites varient selon que vous avez sélectionné une ou plusieurs VM.

   Réinstaller la page Agent avec une seule VM sélectionnée



Réinstaller la page Agent avec plusieurs VM sélectionnées



5 Remplissez le formulaire Réinstaller l'agent et cliquez sur **Réinstaller**.

Fournissez les réponses appropriées aux invites suivantes qui s'appliquent. L'option **Arguments de ligne de commande** s'applique si vous avez sélectionné un ou plusieurs agents. Toutes les autres options s'appliquent uniquement lorsque vous avez sélectionné plusieurs agents.

Option	Description
Ignorer les VM ayant des utilisateurs actifs	Sélectionnez cette option pour ignorer la réinstallation d'Horizon Agent pour les sessions actives ou déconnectées. Si cette option n'est pas sélectionnée, les utilisateurs connectés aux VM lorsque la réinstallation commence recevront un avertissement au bout de 5 minutes, puis seront déconnectés de force.
Délai d'expiration de la tâche	Définissez la période pendant laquelle le système doit continuer à réinstaller automatiquement les agents. Pour exécuter des réinstallations uniquement pendant une période spécifique, vous pouvez définir une courte période, même si vous sélectionnez plusieurs modèles et VM. Un lot de VM peut prendre entre 20 et 60 minutes en fonction de l'état des VM et de tout autre délai d'attente et de nouvelles tentatives en cours. Par exemple, si vous disposez de plus de 600 VM à réinstaller avec 30 VM en simultanéité, vous devez calculer la période comme suit : ■ Nombre de lots : 600/30 = 20 lots ■ Délai d'expiration de la tâche : 20 × 60 = 1 200 minutes Vous devez définir le délai d'expiration de la tâche sur 1 200 minutes, ce qui constitue une période beaucoup plus longue que celle généralement requise pour l'exécution des réinstallations. **Note** Le système ne tente pas de réinstaller les VM qui rencontrent une erreur pendant le processus de réinstallation.
Simultanéité	Définissez une limite au nombre de VM sur lesquelles le système tente de réinstaller l'agent simultanément. Ce paramètre fonctionne en parallèle avec le paramètre **Seuil d'échec**. Idéalement, conservez le paramètre **Simultanéité** sur une valeur inférieure ou égale au paramètre **Seuil d'échec**.
Seuil d'échec	Nombre de VM pour lequel la réinstallation de l'agent est autorisée à échouer avant l'arrêt du processus de réinstallation. La configuration de ce seuil évite les échecs en masse. Lorsque le processus de réinstallation s'arrête en raison de l'échec des réinstallations de l'agent de VM, vous pouvez observer un nombre de VM ayant échoué supérieur à la valeur **Seuil d'échec**. Si vous devez vous assurer qu'il y a moins d'échecs que le nombre spécifié pour le paramètre **Seuil d'échec**, définissez la valeur **Simultanéité** sur **1**. Cela signifie également que le processus de réinstallation de l'agent prendra longtemps, car il réinstallera une seule VM à la fois. Il est recommandé de définir **Simultanéité** et **Seuil d'échec** de manière appropriée pour obtenir des résultats optimaux.
Arguments de ligne de commande	Dans la zone de texte **Arguments de ligne de commande**, ajoutez toutes les options de ligne de commande qui peuvent être appropriées à cette réinstallation.

Étape suivante

Le processus de réinstallation de l'agent s'exécute en arrière-plan. Vous pouvez afficher la progression du processus sur la page Journal d'activité. Reportez-vous à la section Surveillance de l'activité de l'administrateur et de l'utilisateur final sur la page Journal d'activité

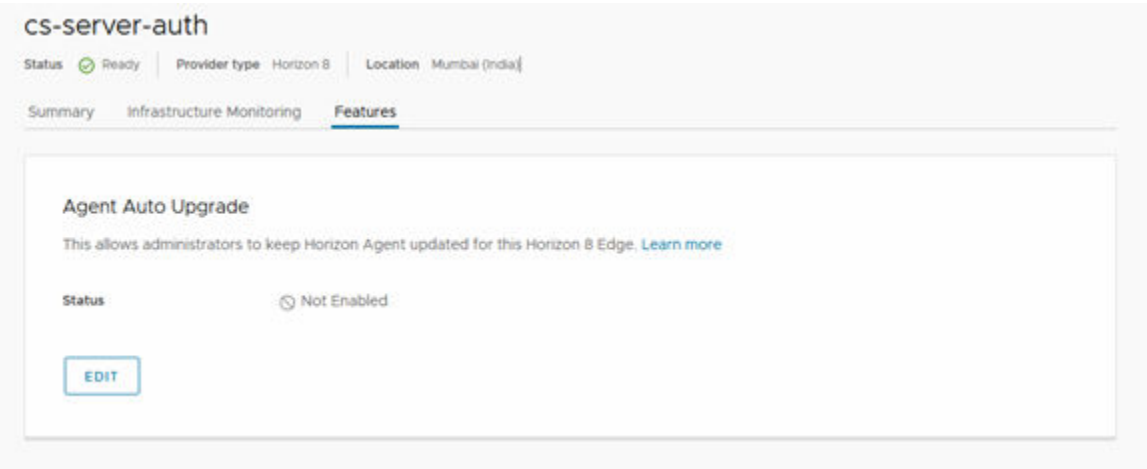
.

Gestion de la fonctionnalité de mise à niveau automatique de l'agent pour un dispositif Horizon 8 Edge

Avec Horizon Cloud Service - next-gen, lorsque vous disposez d'une licence Horizon Universal ou Horizon Plus et que vous déployez un dispositif Horizon Edge dans un environnement Horizon 8, vous pouvez utiliser Horizon Universal Console pour conserver l'instance d'Horizon Agent mise à jour pour le dispositif Horizon 8 Edge que vous spécifiez.

Lorsque vous disposez d'une licence Horizon Universal ou Horizon Plus, vous avez accès à l'onglet **Fonctionnalités** dans Horizon Universal Console, ce qui vous permet d'activer la fonctionnalité de mise à niveau automatique de l'agent. La fonctionnalité de mise à niveau automatique de l'agent dans Horizon 8 repose sur la configuration de la fonctionnalité de mise à niveau automatique de l'agent que vous activez dans Horizon Cloud Service - next-gen avec cette procédure.

Note La procédure suivante active la fonctionnalité. Vous pouvez ensuite gérer la mise à niveau de l'agent à partir d'Horizon Connection Server.



Conditions préalables

Assurez-vous que les conditions requises suivantes sont réunies.

- Obtenez l'une des licences suivantes :
  - Horizon Universal
  - Horizon Plus
- Déployez le dispositif Horizon 8 Edge pour Horizon Cloud Service - next-gen.
- La version d'Horizon Connection Server est 2312 ou ultérieure.

Procédure

1 Sélectionnez **Ressources > Capacité**.

2 Cliquez sur le nom d'un dispositif Horizon 8 Edge pour lequel vous souhaitez activer la fonctionnalité de mise à niveau automatique de l'agent.

3 Cliquez sur l'onglet **Fonctionnalités**.

4 Si l'état de la fonctionnalité est répertorié comme Non activé et que vous souhaitez l'activer, cliquez sur **Modifier**.

5 Cliquez sur l'option **État** pour activer la fonctionnalité.

6 Cliquez sur **Enregistrer**.

Résultats

La fonctionnalité de mise à niveau automatique de l'agent est désormais activée pour le dispositif Horizon 8 Edge.

Étape suivante

Gérez la mise à niveau automatique d'Horizon Agent à l'aide d'Horizon Console, comme indiqué dans la version appropriée de la rubrique Horizon 8, telle que Mettre à niveau Horizon Agent automatiquement.

Maintenance et mises à jour d'Horizon Edge dans Horizon Cloud Service - next-gen

Cette page décrit les principales informations à connaître sur la maintenance des composants logiciels qui constituent votre dispositif Horizon Edge déployé.

Lorsqu'une mise à jour de produit est à venir, y compris les produits d'infrastructure Horizon tels qu'Unified Access Gateway (UAG), la passerelle Edge, etc., vous recevrez un e-mail de notification.

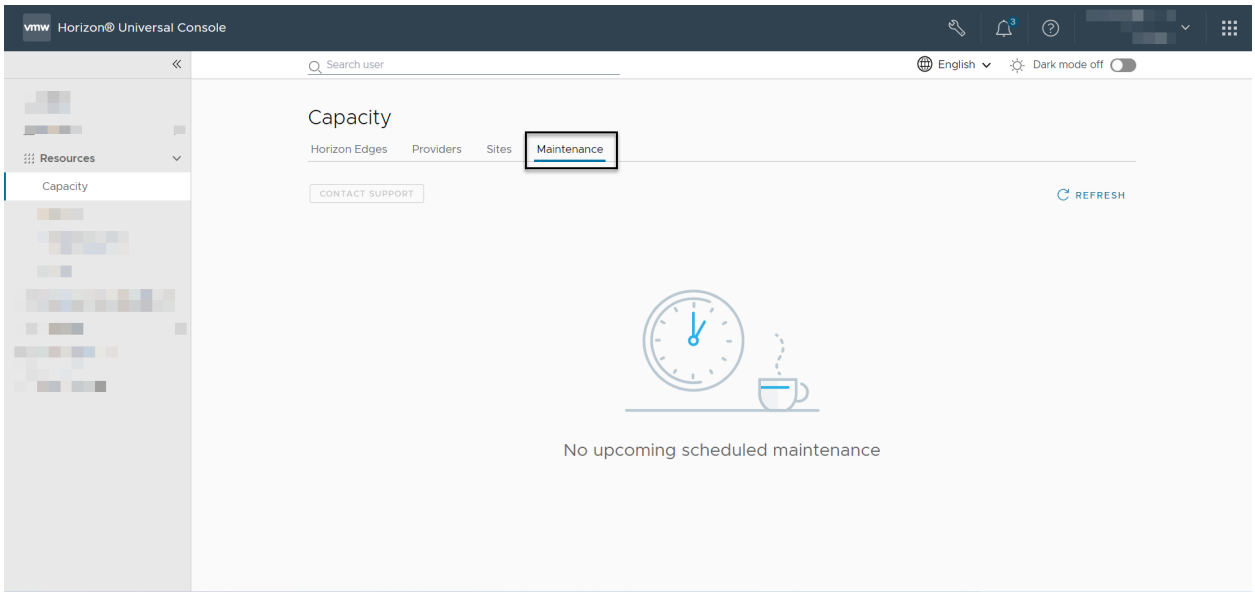
Vous recevez également des notifications par e-mail lorsque chaque phase du processus de mise à jour démarre, se termine, est replanifiée ou est annulée.

Note Les mises à jour de produits ne nécessitent aucune interruption de service et n'ont aucune incidence sur votre environnement ou vos charges de travail. Le report d'une mise à jour de produit peut entraîner l'exécution d'une version logicielle non prise en charge par Horizon Cloud Service, ce qui n'est pas recommandé.

Lorsque le processus de mise à jour de produit est terminé, vous recevez un e-mail récapitulatif de ce qui a été mis à jour.

Pour être sûr de recevoir ces notifications importantes par e-mail, ajoutez l'adresse e-mail *donotreply@vmware.com* à la liste autorisée de vos e-mails.

Unified Access Gateway, la passerelle Edge et les clusters sont mis à jour de manière continue. Pour afficher les informations relatives à la maintenance et à la mise à jour des produits dans Horizon Universal Console, sélectionnez **Ressources > Capacité > Maintenance**.



Si le délai de la maintenance planifiée ne vous convient pas, contactez le support en cliquant sur le bouton **Contacter le support** sur la page **Maintenance** pour effectuer une nouvelle planification.

Configuration de l'expérience à distance pour les utilisateurs Horizon Cloud Service - next-gen

7

Vous pouvez utiliser les informations suivantes pour configurer l'expérience à distance pour les utilisateurs finaux Horizon Cloud Service - next-gen.

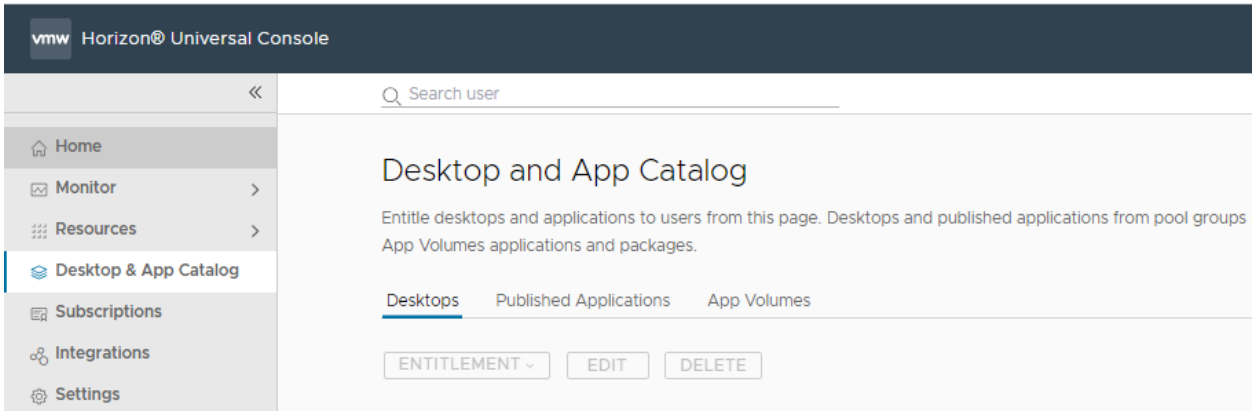
Lisez les sections suivantes :

- Autorisation de l'accès des utilisateurs finaux aux postes de travail et applications
- Attribuer des utilisateurs Horizon Cloud Service - next-gen à des machines virtuelles dans des groupes de pools à session unique dédiés
- Lancer un poste de travail avec Horizon Client
- Lancer un poste de travail à l'aide d'Horizon HTML Access, le client Web
- Lancer une application avec Horizon Client
- Lancer une application à l'aide d'Horizon HTML Access, le client Web
- Configuration des paramètres globaux d'Horizon Client
- Activation de la rampe d'accès au droit cloud d'Horizon pour accéder aux postes de travail Horizon 8 et Horizon Cloud on Azure

Autorisation de l'accès des utilisateurs finaux aux postes de travail et applications

Pour Horizon Cloud Service - next-gen, effectuez les étapes d'autorisation d'accès de vos utilisateurs finaux aux postes de travail et applications publiées à l'aide d'Horizon Universal Console et de la page **Catalogue de postes de travail et d'applications** de la console.

La capture d'écran suivante est une illustration de la page **Catalogue de postes de travail et d'applications** de la console.



Les étapes suivantes décrivent l'autorisation d'accès aux postes de travail et applications publiées qui sont des applications provenant de groupes de pools à sessions multiples.

Pour en savoir plus sur l'utilisation d'App Volumes dans votre environnement, commencez par Utilisation d'App Volumes.

Conditions préalables

Pour utiliser la page **Catalogue de postes de travail et d'applications** de la console afin d'autoriser l'accès de vos utilisateurs finaux aux postes de travail et applications publiées, vous devez disposer d'un groupe de pools qui fournit ces postes de travail et applications publiées pour votre environnement. Reportez-vous aux pages liées à partir de Créer un groupe de pools.

Procédure

1. Affichez la page **Catalogue de postes de travail et d'applications** en cliquant sur l'entrée **Catalogue de postes de travail et d'applications** du volet de navigation de gauche de la console.
2. Pour utiliser des droits d'accès aux postes de travail, cliquez sur **Postes de travail**.

   Les postes de travail des groupes de pools de votre environnement sont répertoriés dans l'onglet Postes de travail.

   Vous pouvez sélectionner un poste de travail répertorié et cliquer sur la liste **Droit** pour **Autoriser l'accès** des utilisateurs finaux à un poste de travail ou **Annuler l'autorisation d'accès** à ce dernier. Si vous cliquez sur **Autoriser l'accès**, la page **Autoriser l'accès aux postes de travail** décrite à l'étape suivante s'affiche.

   Dans cet onglet **Postes de travail**, vous pouvez également **Modifier** ou **Supprimer** votre sélection.
3. Lorsque vous autorisez l'accès à un poste de travail sélectionné sur la page **Autoriser l'accès aux postes de travail**, utilisez les **Types d'utilisateurs** pour spécifier **Utilisateurs** ou **Groupes d'utilisateurs** et **Rechercher des utilisateurs/groupes d'utilisateurs**, puis cliquez sur **Enregistrer**.

4 Pour utiliser les droits d'accès aux applications publiées, sur la page **Catalogue de postes de travail et d'applications**, cliquez sur l'onglet **Applications publiées**.

   Les applications publiées des groupes de pools de votre environnement sont répertoriées dans l'onglet **Applications publiées**.

   Vous pouvez sélectionner une application répertoriée et cliquer sur la liste **Droit** pour **Autoriser l'accès** ou **Annuler l'autorisation d'accès** des utilisateurs finaux à cette application. Si vous cliquez sur **Autoriser l'accès**, la page **Autoriser l'accès aux applications publiées** décrite à l'étape suivante s'affiche.

   Dans cet onglet, vous pouvez également **Modifier** ou **Supprimer** l'application publiée.

5 Lorsque vous attribuez l'accès à une application sélectionnée sur la page **Autoriser l'accès aux applications publiées**, utilisez les **Types d'utilisateurs** pour spécifier **Utilisateurs** ou **Groupes d'utilisateurs** et **Rechercher des utilisateurs/groupes d'utilisateurs**, puis cliquez sur **Enregistrer**.

Étape suivante

Lorsque vos utilisateurs finaux accèdent aux postes de travail et applications publiées, ils peuvent les lancer.

Lancement de postes de travail

- Lancer un poste de travail à l'aide d'Horizon HTML Access, le client Web
- Lancer un poste de travail avec Horizon Client

Lancement d'applications publiées

- Lancer une application à l'aide d'Horizon HTML Access, le client Web
- Lancer une application avec Horizon Client

Attribuer des utilisateurs Horizon Cloud Service - next-gen à des machines virtuelles dans des groupes de pools à session unique dédiés

Sur la page Groupes de pools, vous pouvez attribuer des utilisateurs à des groupes de pools à session unique dédiée.

Note Bien que vous puissiez attribuer plusieurs utilisateurs à un seul poste de travail, un seul utilisateur peut avoir une session sur une machine virtuelle individuelle à la fois. Configurez les paramètres Traitement du délai d'expiration de manière appropriée pour garantir la disponibilité de la machine virtuelle. Pour plus d'informations sur la configuration des paramètres de traitement du délai d'expiration, reportez-vous à la section Créer un groupe de pools à session unique.

Procédure

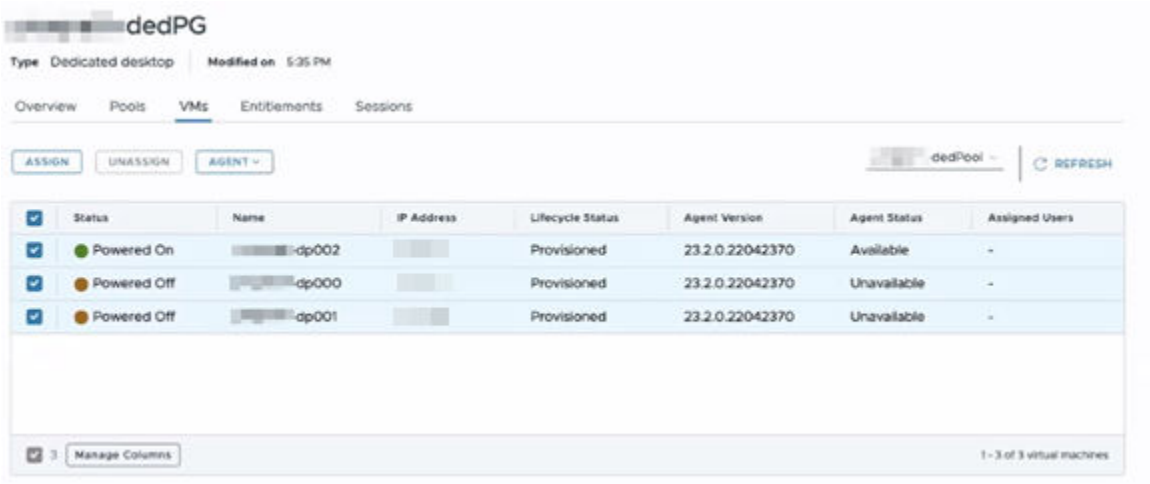
1 Dans la navigation latérale, sélectionnez **Ressources > Groupes de pools**.

2 Cliquez sur le nom d'un groupe de pools de postes de travail dédiés.

3 Cliquez sur l'onglet **VM**.

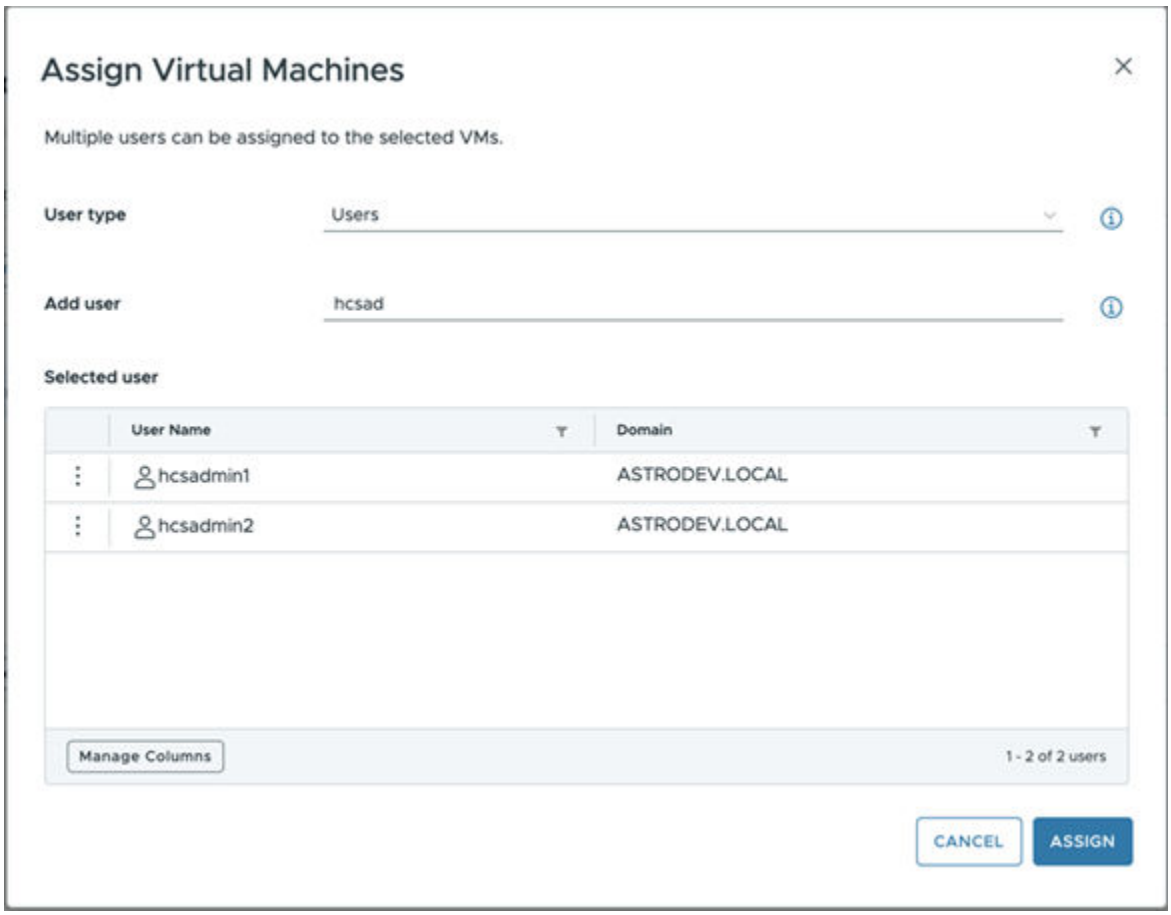
4 Au-dessus du tableau, sélectionnez un pool dans le menu déroulant à gauche du lien **ACTUALISER**.

5 Sélectionnez les VM auxquelles vous souhaitez attribuer des utilisateurs et cliquez sur **Attribuer**.



6 Dans la zone de texte **Ajouter un utilisateur**, entrez le nom d'utilisateur et cliquez dessus à partir des noms d'utilisateur qui s'affichent.

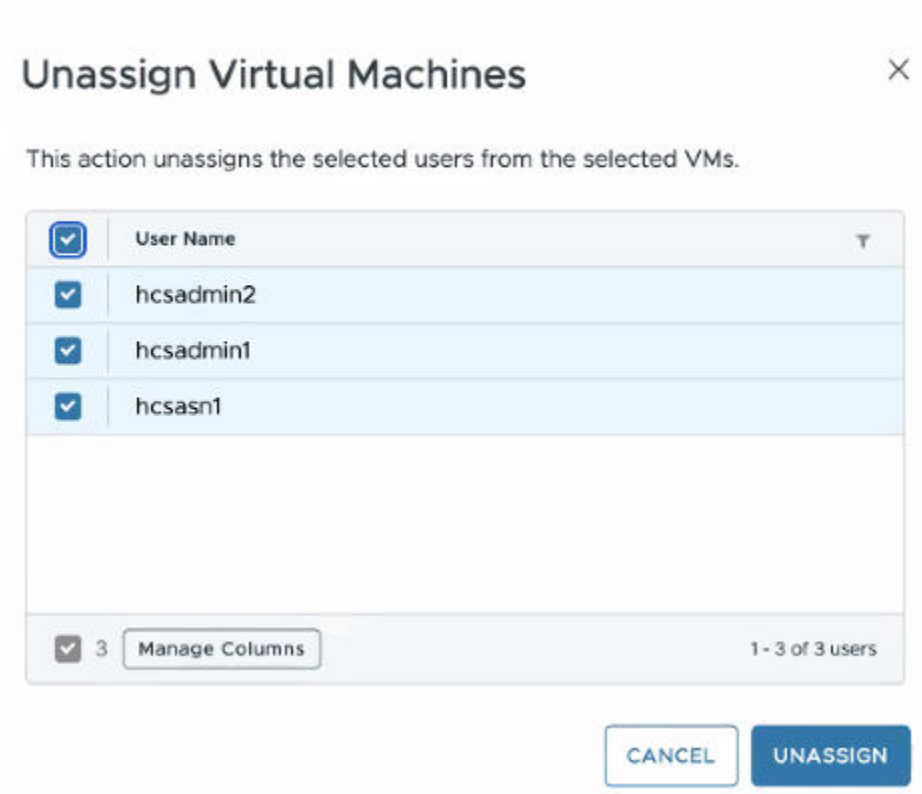
Vous pouvez répéter cette étape plusieurs fois pour ajouter d'autres utilisateurs.



7 Cliquez sur **ATTRIBUER**.

8 Pour annuler l'attribution d'utilisateurs, sélectionnez une ou plusieurs VM, cliquez sur **ANNULER L'ATTRIBUTION**, sélectionnez les utilisateurs spécifiques, puis cliquez à nouveau sur **ANNULER L'ATTRIBUTION**.

Lorsque vous sélectionnez plusieurs VM, l'écran affiche une liste consolidée de tous les utilisateurs attribués aux VM sélectionnées. La liste ne spécifie pas l'utilisateur associé à la VM. L'attribution de tous les utilisateurs sélectionnés sera annulée de toutes les VM, que l'annulation de l'attribution provienne d'une ou de plusieurs VM.



Lancer un poste de travail avec Horizon Client

Cette page de documentation décrit les étapes d'utilisation d'Horizon Client pour lancer un poste de travail virtuel fourni par votre environnement Horizon Cloud Service - next-gen.

Ces étapes incluent l'installation d'une instance d'Horizon Client en mode natif, pour le cas d'utilisation où vous n'en avez peut-être pas déjà installée sur votre système client local.

Conditions préalables

Avant que les utilisateurs finaux ne puissent lancer leurs postes de travail attribués, vérifiez que votre environnement dispose d'un des éléments suivants pour fournir les postes de travail.

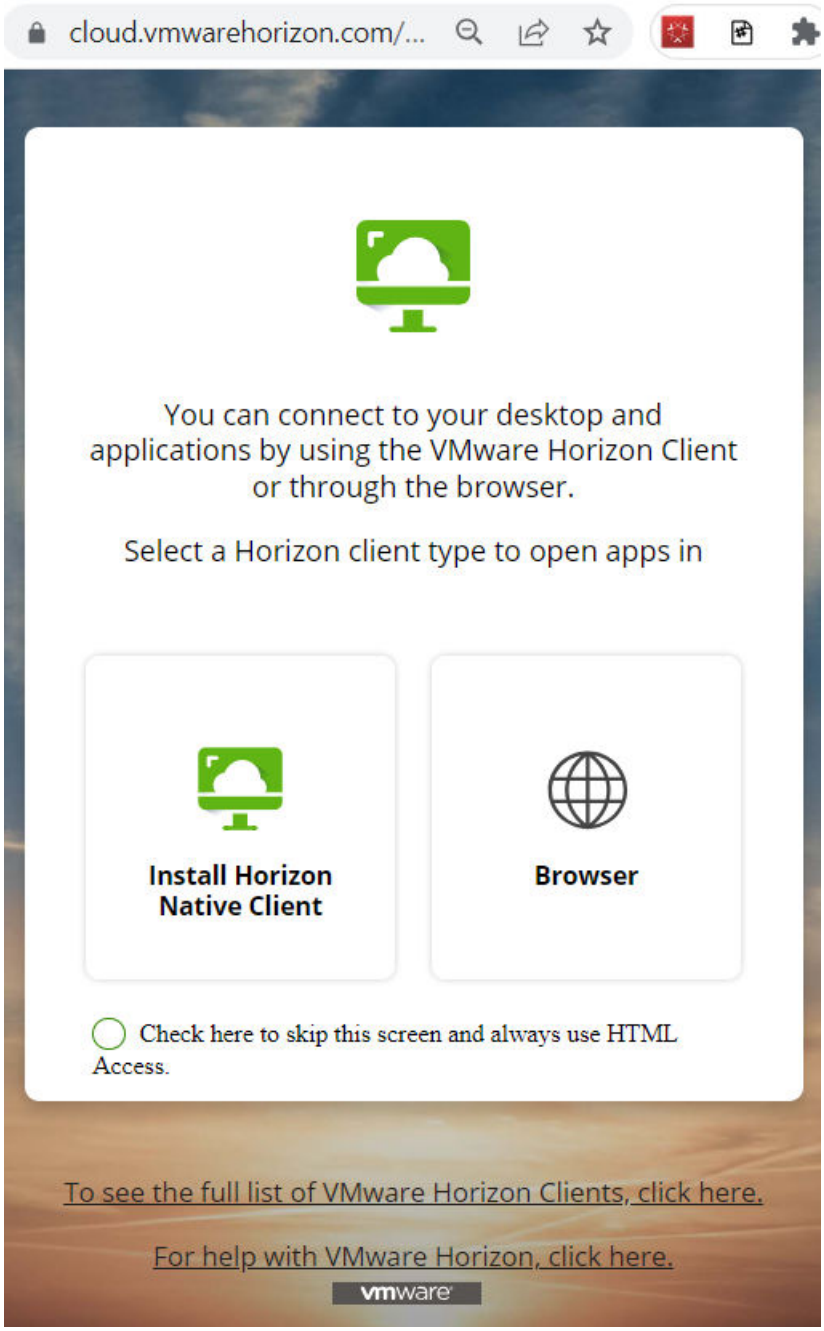
- Des images VDI ont été publiées pour un pool à session unique.
- Les images ont été publiées pour un pool à plusieurs sessions.

Vérifiez également que vos utilisateurs finaux utilisent des versions d'Horizon Client prises en charge pour un environnement Horizon Cloud Service - next-gen. Reportez-vous à la section client de la page Liste de vérification des conditions requises pour un dispositif Microsoft Azure Edge.

Procédure

1 Pour accéder à votre poste de travail attribué, lancez le portail Horizon à l'adresse https://cloud.vmwarehorizon.com/.

La capture d'écran suivante illustre le portail qui s'affiche lorsque vous pointez votre navigateur sur cette URL.



2 Si aucune instance d'Horizon Client n'a déjà été installée sur votre système natif, vous pouvez sélectionner l'option **Installer Horizon Client en mode natif** pour être dirigé automatiquement vers le site Customer Connect pour télécharger le client natif correspondant à votre système d'exploitation.

   Lorsque vous cliquez sur **Installer Horizon Client en mode natif**, le navigateur ouvre la page Customer Connect pour Télécharger les instances de VMware Horizon Client. Suivez les instructions à l'écran pour télécharger le programme d'installation du client natif qui correspond à votre système, puis installez le client natif.

3 Une fois installé, lancez Horizon Client.

   Le client affiche tous les sites Horizon actuellement configurés dans cette instance d'Horizon Client.

4 Dans l'ensemble des sites configurés affichés, recherchez celui qui porte la mention `cloud.vmwarehorizon.com` et double-cliquez dessus pour vous connecter au site.

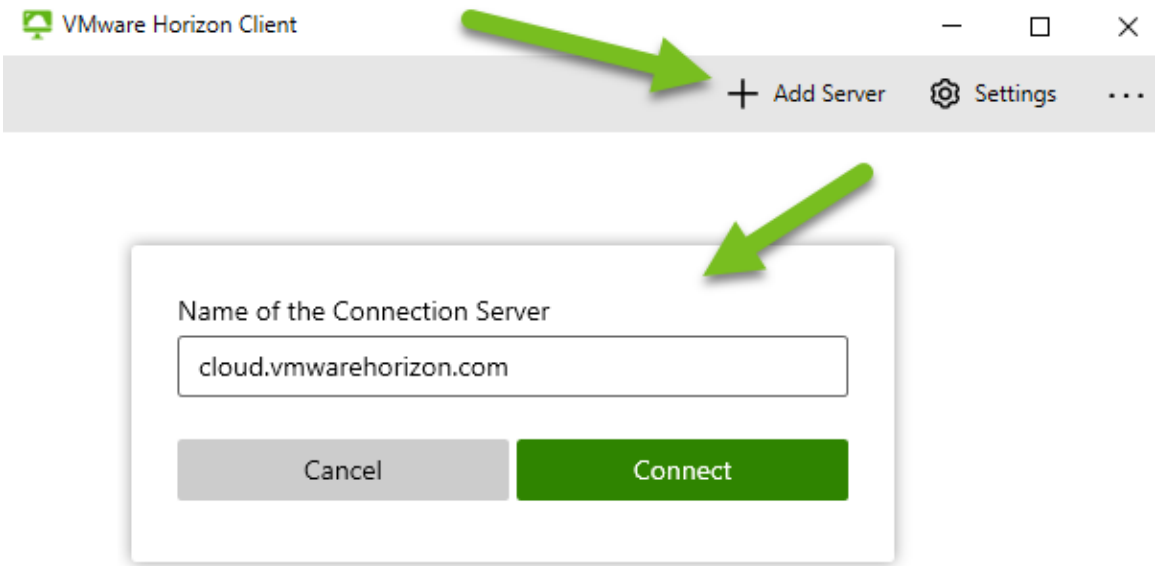
Note S'il s'agit d'une première installation de client ou du premier lancement d'un poste de travail ou d'une application à partir d'un environnement Horizon Cloud Service - next-gen, aucun site n'est encore configuré sur le client pour `cloud.vmwarehorizon.com`.

Dans ce cas, vous devez ajouter le site nommé `cloud.vmwarehorizon.com` à l'aide du bouton **Ajouter un serveur** du client.

a Si aucune icône portant la mention `cloud.vmwarehorizon.com` ne s'affiche, cliquez sur **Ajouter un serveur** pour l'ajouter.

Le client affiche un champ pour entrer `cloud.vmwarehorizon.com`.

La capture d'écran suivante illustre la séquence d'étapes d'utilisation d'Horizon Client pour Windows v2303. Si vous utilisez un autre client natif ou une autre version, il se peut que l'interface utilisateur soit différente de cette capture d'écran. La séquence de base est la même pour ajouter le nom du site (nom du serveur) et se connecter pour obtenir une icône de ce site dans votre client.

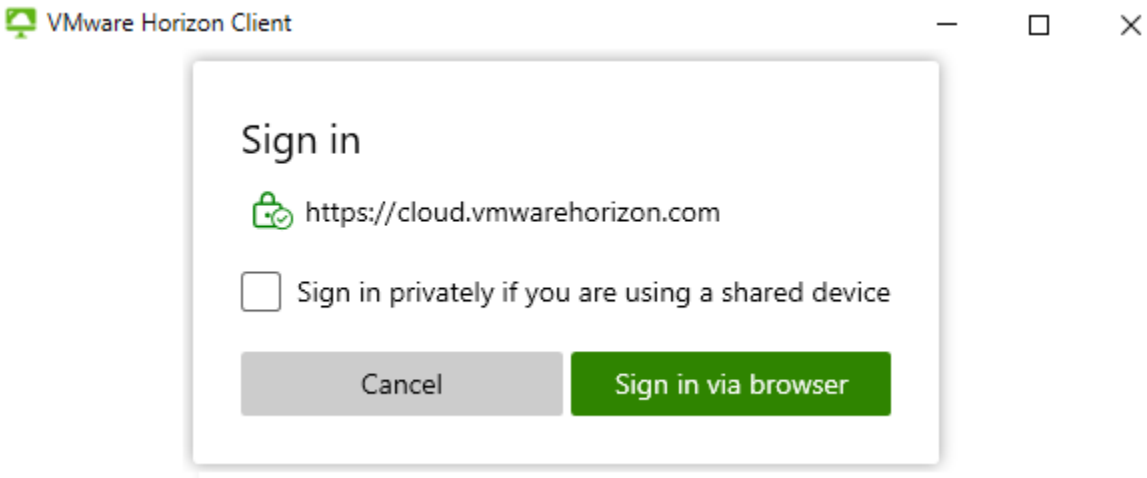


Cliquez ensuite sur **Se connecter** pour terminer l'ajout du site à Horizon Client.

5 Lorsque votre client affiche l'icône de `cloud.vmwarehorizon.com`, double-cliquez sur son icône pour vous connecter au site.

L'interface utilisateur qui s'affiche dépend du client natif que vous utilisez. Par exemple, Horizon Client pour Windows affiche une boîte de dialogue **Se connecter**, quant à Horizon Client pour Chrome, il n'existe pas de boîte de dialogue **Se connecter**.

La capture d'écran suivante illustre cette étape d'utilisation d'Horizon Client pour Windows v2303 spécifiquement.



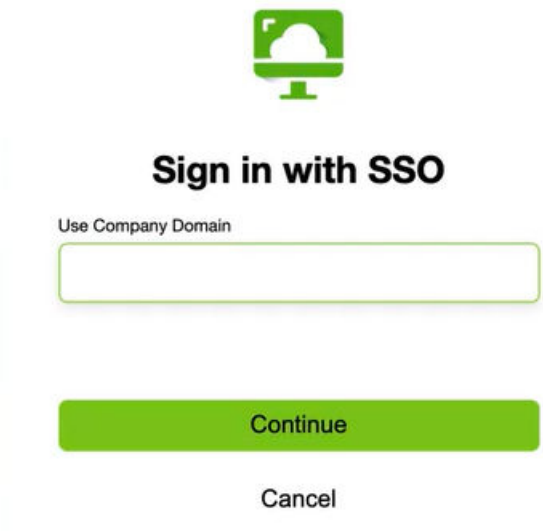
6 Connectez-vous en suivant les invites à l'écran, comme indiqué dans votre client.

Si le client que vous utilisez fournit l'option **Se connecter en mode privé si vous utilisez un périphérique partagé**, vous pouvez utiliser cette dernière pour empêcher le client de mettre en cache les informations sur votre périphérique.

Note Comme Horizon Client pour Chrome se connecte toujours en mode privé, ce client ne fournit pas l'option **Se connecter en mode privé si vous utilisez un périphérique partagé**. Lorsque vous cliquez sur l'icône du serveur dans Horizon Client pour Chrome, le client affiche l'interface utilisateur **Se connecter avec SSO** dans votre navigateur.

Lorsque vous suivez les invites à l'écran pour vous connecter, le système affiche l'interface utilisateur **Se connecter avec SSO** dans votre navigateur.

La capture d'écran suivante illustre l'interface utilisateur **Se connecter avec SSO**.



7 Dans **Se connecter avec SSO**, entrez le nom du domaine de la société associé à cet environnement Horizon Cloud Service - next-gen, puis cliquez sur **Continuer**.

   Dans Horizon Universal Console, les administrateurs peuvent consulter le nom configuré dans la configuration du fournisseur d'identité. Reportez-vous aux pages de Gestion des identités et des accès dans un environnement Horizon Cloud Service - next-gen.

   Lorsque vous cliquez sur **Continuer**, suivez les invites à l'écran. Le système vous dirige vers l'interface utilisateur de connexion de votre fournisseur d'identité. Connectez-vous avec vos informations d'identification attribuées pour ce fournisseur d'identité.

   Une fois la connexion du fournisseur d'identité terminée, l'écran de droit d'Horizon s'affiche dans votre client et répertorie les applications et postes de travail attribués.

8 Cliquez sur l'icône du poste de travail pour lancer ce dernier.

Lancer un poste de travail à l'aide d'Horizon HTML Access, le client Web

Cette page de documentation décrit les étapes d'utilisation de Horizon HTML Access, le client Web, pour lancer un poste de travail fourni par votre environnement Horizon Cloud Service - next-gen.

Conditions préalables

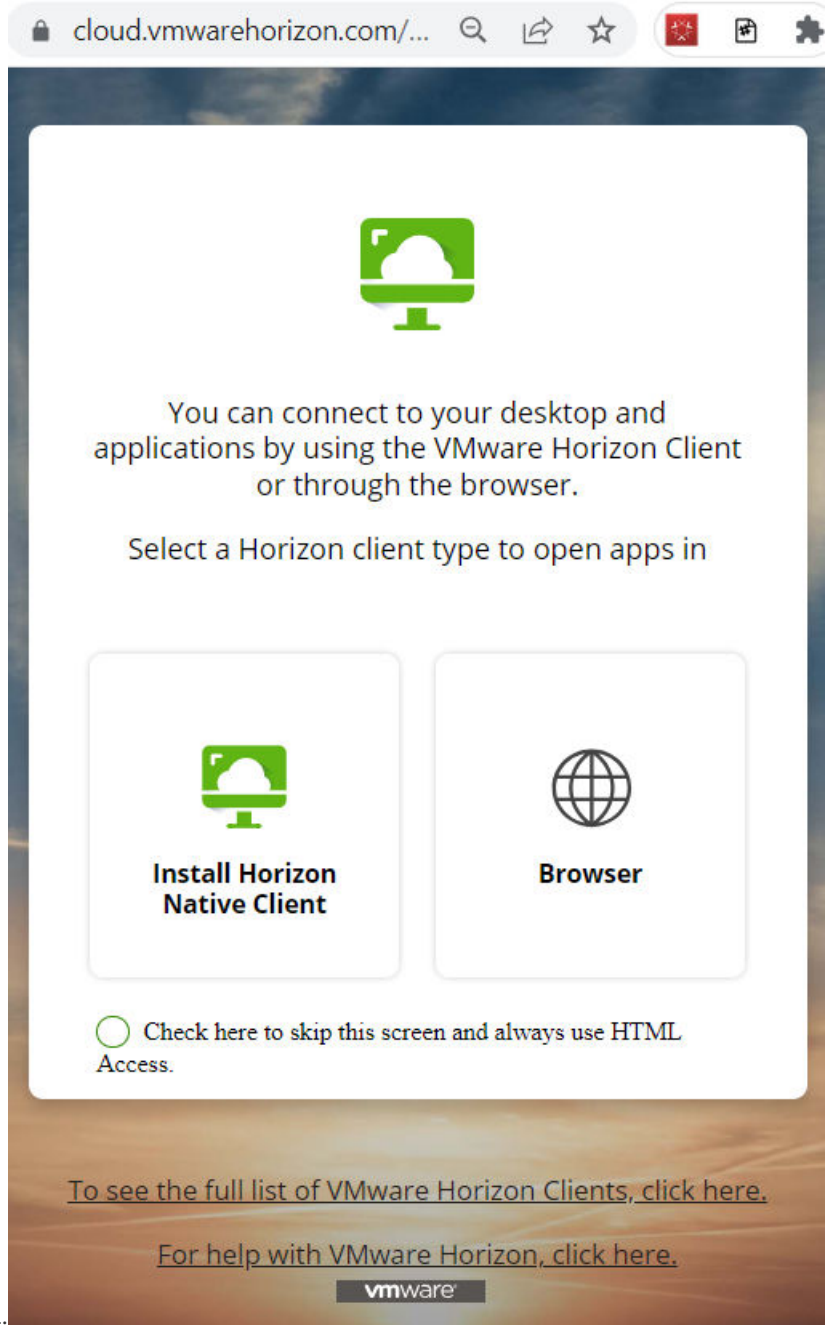
Avant que les utilisateurs finaux ne puissent lancer leurs postes de travail attribués, vérifiez que votre environnement dispose d'un des éléments suivants pour fournir les postes de travail.

- Des images VDI ont été publiées pour un pool à session unique.
- Les images ont été publiées pour un pool à plusieurs sessions.

Procédure

1 Pour accéder à votre poste de travail attribué, lancez le portail Horizon à l'adresse https://cloud.vmwarehorizon.com/.

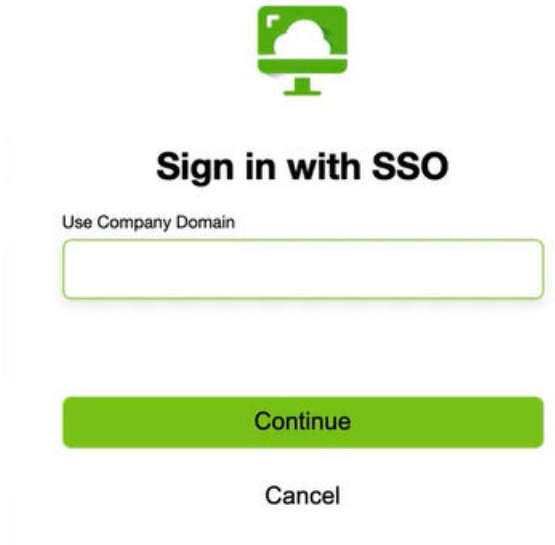
La capture d'écran suivante illustre le portail qui s'affiche lorsque vous pointez votre navigateur sur cette URL.



2 Cliquez sur **Navigateur** pour vous connecter à votre poste de travail à l'aide du client Web.

Lorsque vous cliquez sur **Navigateur**, le navigateur affiche l'interface **Se connecter avec SSO**.

La capture d'écran suivante illustre l'interface utilisateur **Se connecter avec SSO**.



3 Dans **Se connecter avec SSO**, entrez le nom du domaine de la société associé à cet environnement Horizon Cloud Service - next-gen, puis cliquez sur **Continuer**.

   Dans Horizon Universal Console, les administrateurs peuvent consulter le nom configuré dans la configuration du fournisseur d'identité. Reportez-vous aux pages de Gestion des identités et des accès dans un environnement Horizon Cloud Service - next-gen.

   Lorsque vous cliquez sur **Continuer**, suivez les invites à l'écran. Le système vous dirige vers l'interface utilisateur de connexion de votre fournisseur d'identité. Connectez-vous avec vos informations d'identification attribuées pour ce fournisseur d'identité.

   Une fois la connexion du fournisseur d'identité terminée, l'écran Droit d'Horizon s'affiche et répertorie vos applications et postes de travail attribués.

4 Pour lancer un poste de travail, cliquez sur son icône affichée.

Lancer une application avec Horizon Client

Cette page de documentation décrit les étapes d'utilisation d'Horizon Client pour lancer une application fournie par votre environnement Horizon Cloud Service - next-gen.

Ces étapes incluent l'installation d'une instance d'Horizon Client en mode natif, pour le cas d'utilisation où vous n'en avez peut-être pas déjà installée sur votre système client local.

Conditions préalables

Avant que les utilisateurs finaux ne puissent lancer les applications attribuées, vérifiez que vous avez autorisé l'accès de ces utilisateurs aux applications publiées à l'aide d'Horizon Universal Console.

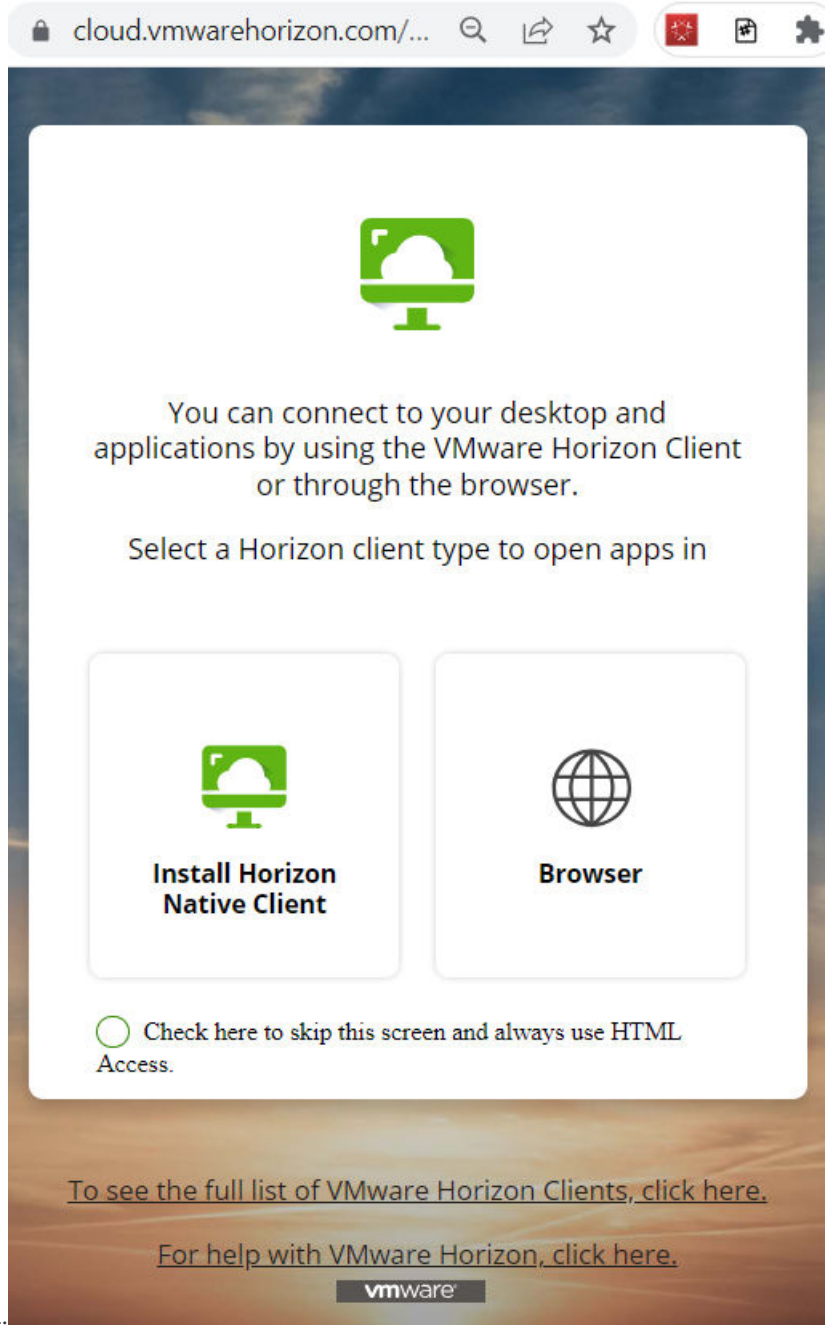
- Pour autoriser l'accès aux applications publiées à partir de groupes de pools à plusieurs sessions, reportez-vous à la page Autorisation de l'accès des utilisateurs finaux aux postes de travail et applications.

Vérifiez également que vos utilisateurs finaux utilisent des versions d'Horizon Client prises en charge pour un environnement Horizon Cloud Service - next-gen. Reportez-vous à la section client de la page Liste de vérification des conditions requises pour un dispositif Microsoft Azure Edge.

Procédure

1 Pour accéder à votre application attribuée, lancez le portail Horizon sur https://cloud.vmwarehorizon.com/.

La capture d'écran suivante illustre le portail qui s'affiche lorsque vous pointez votre navigateur sur cette URL.



2 Si aucune instance d'Horizon Client n'a déjà été installée sur votre système natif, vous pouvez sélectionner l'option **Installer Horizon Client en mode natif** pour être dirigé automatiquement vers le site Customer Connect pour télécharger le client natif correspondant à votre système d'exploitation.

   Lorsque vous cliquez sur **Installer Horizon Client en mode natif**, le navigateur ouvre la page Customer Connect pour Télécharger les instances d'Horizon Client. Suivez les instructions à l'écran pour télécharger le programme d'installation du client natif qui correspond à votre système, puis installez le client natif.

3 Une fois installé, lancez Horizon Client.

   Le client affiche tous les sites Horizon actuellement configurés dans cette instance d'Horizon Client.

4 Dans l'ensemble des sites configurés affichés, recherchez celui qui porte la mention `cloud.vmwarehorizon.com` et double-cliquez dessus pour vous connecter au site.

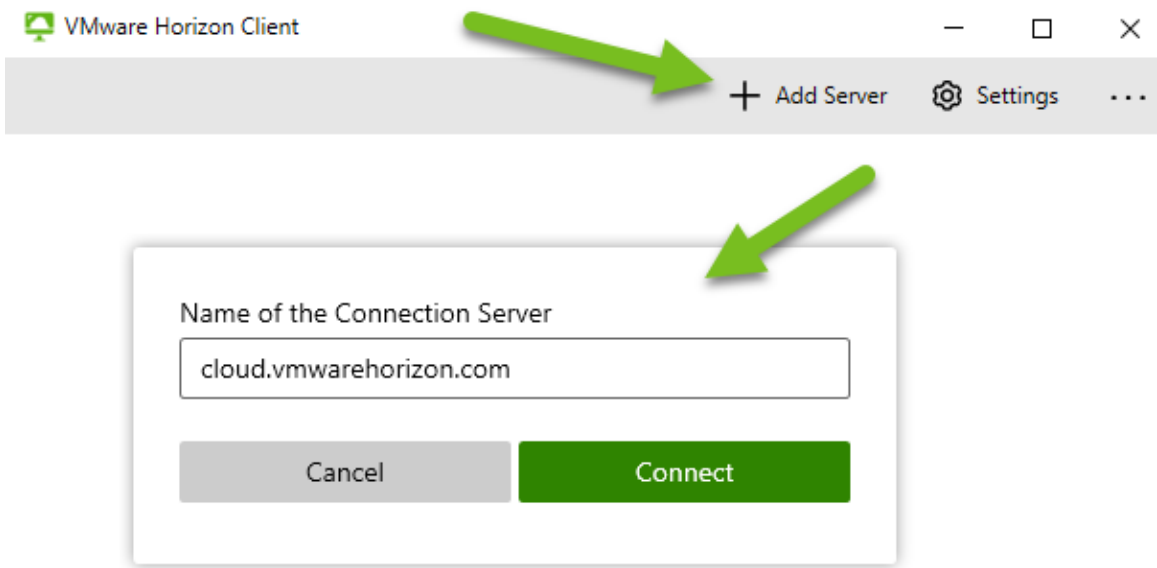
Note S'il s'agit d'une première installation de client ou du premier lancement d'une application ou d'un poste de travail à partir d'un environnement Horizon Cloud Service - next-gen, aucun site n'est encore configuré sur le client pour `cloud.vmwarehorizon.com`.

Dans ce cas, vous devez ajouter le site nommé `cloud.vmwarehorizon.com` à l'aide du bouton **Ajouter un serveur** du client.

a Si aucune icône portant la mention `cloud.vmwarehorizon.com` ne s'affiche, cliquez sur **Ajouter un serveur** pour l'ajouter.

Le client affiche un champ pour entrer `cloud.vmwarehorizon.com`.

La capture d'écran suivante illustre la séquence d'étapes d'utilisation d'Horizon Client pour Windows v2303. Si vous utilisez un autre client natif ou une autre version, il se peut que l'interface utilisateur soit différente de cette capture d'écran. La séquence de base est la même pour ajouter le nom du site (nom du serveur) et se connecter pour obtenir une icône de ce site dans votre client.

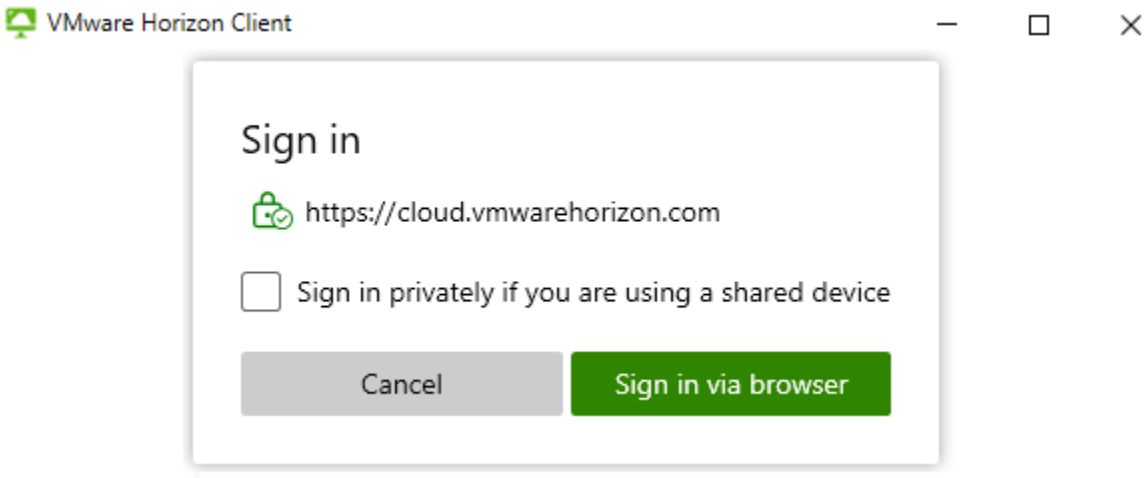


Cliquez ensuite sur **Se connecter** pour terminer l'ajout du site à Horizon Client.

5 Lorsque votre client affiche l'icône de `cloud.vmwarehorizon.com`, double-cliquez sur son icône pour vous connecter au site.

L'interface utilisateur qui s'affiche dépend du client natif que vous utilisez. Par exemple, Horizon Client pour Windows affiche une boîte de dialogue **Se connecter**, quant à Horizon Client pour Chrome, il n'existe pas de boîte de dialogue **Se connecter**.

La capture d'écran suivante illustre cette étape d'utilisation d'Horizon Client pour Windows v2303 spécifiquement.



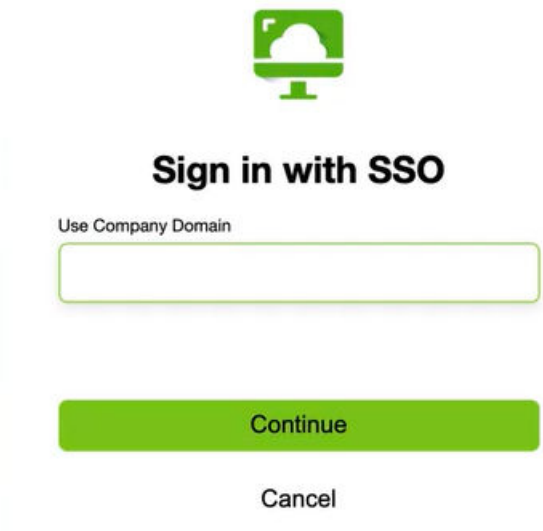
6 Connectez-vous en suivant les invites à l'écran, comme indiqué dans votre client.

Si le client que vous utilisez fournit l'option **Se connecter en mode privé si vous utilisez un périphérique partagé**, vous pouvez utiliser cette dernière pour empêcher le client de mettre en cache les informations sur votre périphérique.

Note Comme Horizon Client pour Chrome se connecte toujours en mode privé, ce client ne fournit pas l'option **Se connecter en mode privé si vous utilisez un périphérique partagé**. Lorsque vous cliquez sur l'icône du serveur dans Horizon Client pour Chrome, le client affiche l'interface utilisateur **Se connecter avec SSO** dans votre navigateur.

Lorsque vous suivez les invites à l'écran pour vous connecter, le système affiche l'interface utilisateur **Se connecter avec SSO** dans votre navigateur.

La capture d'écran suivante illustre l'interface utilisateur **Se connecter avec SSO**.



7 Dans **Se connecter avec SSO**, entrez le nom du domaine de la société associé à cet environnement Horizon Cloud Service - next-gen, puis cliquez sur **Continuer**.

   Dans Horizon Universal Console, les administrateurs peuvent consulter le nom configuré dans la configuration du fournisseur d'identité. Reportez-vous aux pages de Gestion des identités et des accès dans un environnement Horizon Cloud Service - next-gen.

   Lorsque vous cliquez sur **Continuer**, suivez les invites à l'écran. Le système vous dirige vers l'interface utilisateur de connexion de votre fournisseur d'identité. Connectez-vous avec vos informations d'identification attribuées pour ce fournisseur d'identité.

   Une fois la connexion du fournisseur d'identité terminée, l'écran de droit d'Horizon s'affiche dans votre client et répertorie les applications et postes de travail attribués.

8 Cliquez sur l'icône de l'application pour lancer cette dernière.

Lancer une application à l'aide d'Horizon HTML Access, le client Web

Cette page de documentation décrit les étapes d'utilisation d'Horizon HTML Access, le client Web, pour lancer une application fournie par votre environnement Horizon Cloud Service - next-gen.

Conditions préalables

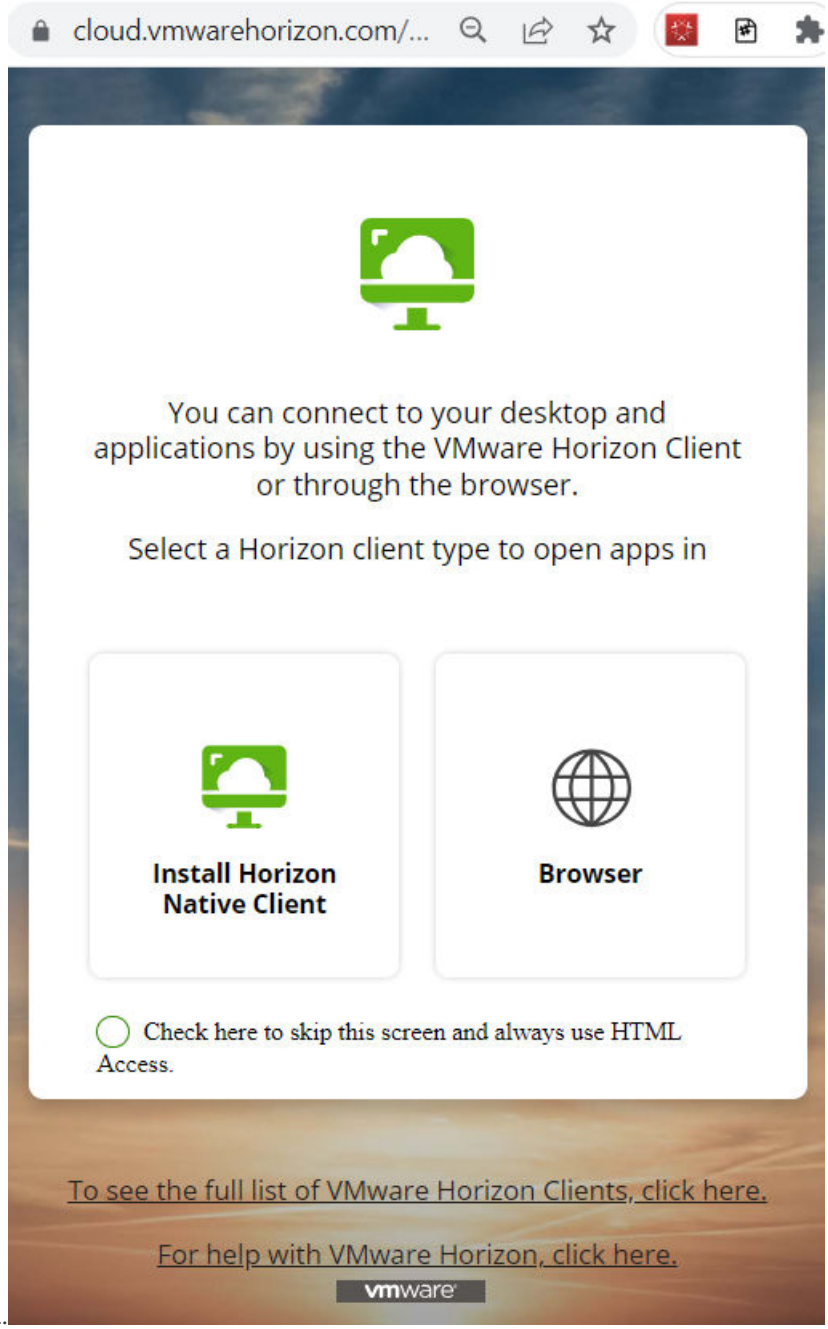
Avant que les utilisateurs finaux ne puissent lancer les applications attribuées, vérifiez que vous avez autorisé l'accès de ces utilisateurs aux applications à l'aide d'Horizon Universal Console.

- Pour autoriser l'accès aux applications publiées à partir de groupes de pools à plusieurs sessions, reportez-vous à la page Autorisation de l'accès des utilisateurs finaux aux postes de travail et applications.

Procédure

1 Pour accéder à votre application attribuée, lancez le portail Horizon sur https://cloud.vmwarehorizon.com/.

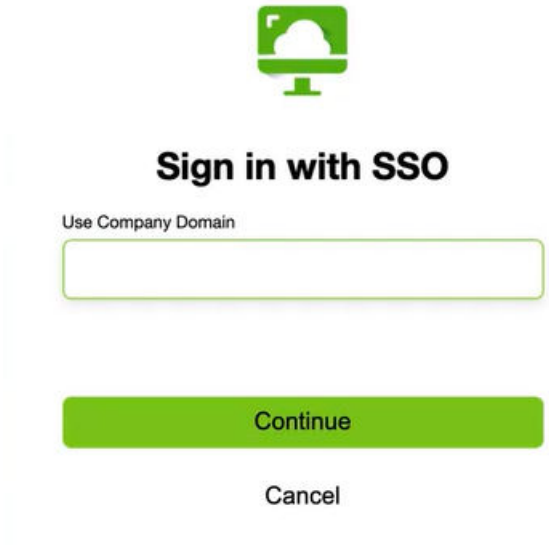
La capture d'écran suivante illustre le portail qui s'affiche lorsque vous pointez votre navigateur sur cette URL.



2 Cliquez sur **Navigateur** pour vous connecter à votre application à l'aide du client Web.

Lorsque vous cliquez sur **Navigateur**, le navigateur affiche l'interface **Se connecter avec SSO**.

La capture d'écran suivante illustre l'interface utilisateur **Se connecter avec SSO**.



3 Dans **Se connecter avec SSO**, entrez le nom du domaine de la société associé à cet environnement Horizon Cloud Service - next-gen, puis cliquez sur **Continuer**.

   Dans Horizon Universal Console, les administrateurs peuvent consulter le nom configuré dans la configuration du fournisseur d'identité. Reportez-vous aux pages de Gestion des identités et des accès dans un environnement Horizon Cloud Service - next-gen.

   Lorsque vous cliquez sur **Continuer**, suivez les invites à l'écran. Le système vous dirige vers l'interface utilisateur de connexion de votre fournisseur d'identité. Connectez-vous avec vos informations d'identification attribuées pour ce fournisseur d'identité.

   Une fois la connexion du fournisseur d'identité terminée, l'écran Droit d'Horizon s'affiche et répertorie vos applications et postes de travail attribués.

4 Cliquez sur l'icône de l'application pour lancer cette dernière.

Configuration des paramètres globaux d'Horizon Client

Vous pouvez configurer les paramètres globaux d'Horizon Client qui s'appliquent à tous les utilisateurs finaux dans cet environnement de locataire d'Horizon Cloud Service - next-gen.

Configurer le message de préouverture de session dans Horizon Cloud Service - next-gen

Vous pouvez personnaliser un message visible par les utilisateurs finaux avant de se connecter à Horizon Client.

Procédure

1 Connectez-vous à Horizon Cloud Service - next-gen.

2 Cliquez sur **Paramètres** dans la barre de navigation.

3 Cliquez sur **Gérer** sur la vignette **Paramètres du client**.

4 Sur la page **Paramètres du client**, cliquez sur l'onglet **Messages personnalisés**, puis sur **Modifier**.

5 Basculez le bouton pour inclure le **message de préouverture de session**.

6 Ajoutez le champ **Message de préouverture de session**. Vous pouvez également rebasculer le bouton pour désactiver le **message de préouverture de session**.

Configurer les informations de marque dans Horizon Cloud Service - next-gen

Vous pouvez personnaliser l'URL à laquelle vos utilisateurs finaux accèdent pour se connecter à vos postes de travail et applications.

Conditions préalables

Déterminez l'URL ou le sous-domaine à utiliser. Les détails suivants s'appliquent à l'URL ou au sous-domaine que vous utilisez.

- Cette URL ou ce sous-domaine doit être unique sur le service Horizon Client. Vous recevez une erreur si l'URL ou le sous-domaine est utilisé(e) par un autre locataire. Si vous pensez qu'une URL ou un sous-domaine que vous possédez est utilisé(e) par un autre locataire n'appartenant pas à votre organisation, adressez une demande de support pour nous en informer.
- Le sous-domaine des URL personnalisées doit comporter au moins 1 caractère et 63 caractères au maximum.
- Les URL personnalisées ne doivent contenir que des lettres, des chiffres et des tirets (-).
- Certaines chaînes ne sont pas autorisées ou sont réservées par le système. Cette catégorie de chaîne inclut des mots génériques tels que `book`, des termes bien connus appartenant à des entreprises, tels que `Gmail` et `protocol.coding`, ainsi que des termes open source tels que `php` et `sql`. Le système interdit également une catégorie de modèle de ces chaînes comme `mail0`, `mail1`, `mail2`, etc.
- Les URL ou les sous-domaines appartenant à une autre organisation ou enfreignant les droits d'auteur ou les marques commerciales que vous ne possédez pas sont supprimés.

Procédure

1 Connectez-vous à Horizon Cloud Service - next-gen.

2 Cliquez sur **Paramètres** dans la barre de navigation.

3 Cliquez sur **Gérer** sur la vignette **Paramètres du client**.

4 Sur la page **Paramètres du client**, cliquez sur l'onglet **Informations de marque**.

5 Pour fournir un **Sous-domaine d'accès client personnalisé**, procédez comme suit

a Dans la section **Sous-domaine d'accès client personnalisé**, spécifiez un sous-domaine pour personnaliser l'URL d'accès client que les utilisateurs finaux utilisent pour se connecter à vos postes de travail et applications.

b Cliquez sur **Modifier** pour **Activer le sous-domaine d'accès client personnalisé** en sélectionnant l'option.

Le champ **Activer le sous-domaine d'accès client personnalisé** est désactivé et l'option disponible est **Non** par défaut. Ce n'est qu'après avoir cliqué sur **Modifier** que l'option est activée et que vous pouvez la sélectionner.

c Ajoutez un **Sous-domaine d'accès client personnalisé**.

L'application de la configuration et de la modification du sous-domaine client personnalisé peut prendre jusqu'à 10 minutes.

6 Pour fournir une **URL d'accès client personnalisée**, procédez comme suit.

a Dans la section **URL d'accès client personnalisée**, spécifiez un nom de domaine complet pour personnaliser l'URL que les utilisateurs finaux utilisent pour se connecter à vos postes de travail et applications.

Note Vous devez configurer une association d'alias en créant un enregistrement CNAME sur votre serveur DNS qui mappe votre nom de domaine complet personnalisé au point de terminaison fourni.

b Pour configurer l'URL, cliquez sur **Configurer**.

c Spécifiez l'**URL d'accès client personnalisée**.

d Cliquez sur **Parcourir** pour parcourir et charger un **certificat** valide pour l'URL d'accès client personnalisée entrée précédemment au format `PFX`.

e Ajoutez un **Mot de passe** pour le certificat. Cliquez sur **Enregistrer**.

L'application de la configuration et de la modification du sous-domaine client personnalisé peut prendre jusqu'à 10 minutes.

Configurer des plages réseau pour identifier les utilisateurs Horizon Cloud Service - next-gen internes

Cette rubrique explique comment définir les plages de votre réseau interne en spécifiant les adresses IP publiques NAT de sortie sur le pare-feu ou le routeur du bureau ou du centre de données à partir duquel vos instances d'Horizon Client se connectent. La définition de votre réseau interne de cette manière permet au broker d'appliquer des stratégies propres au réseau, telles que l'autorisation de connexions directes à des postes de travail à partir d'Horizon Client, en contournant Unified Access Gateway.

Pour définir votre réseau interne pour le broker, utilisez l'onglet **Plages réseau** de la page **Paramètres du client** et spécifiez toutes les plages d'adresses NAT de sortie qui correspondent au trafic de vos utilisateurs finaux internes.

Le broker reconnaît les instances d'Horizon Client qui se connectent à partir des plages spécifiées d'adresses NAT de sortie sur le routeur ou pare-feu de bureau ou de centre de données provenant de votre réseau interne. Les utilisateurs qui se connectent à partir d'adresses IP publiques comprises dans ces plages sont considérés comme des utilisateurs internes. Les utilisateurs qui se connectent à partir d'adresses IP publiques en dehors de ces plages sont considérés comme des utilisateurs externes.

Important Si la configuration de votre réseau change et si l'une des plages d'adresses spécifiées est désactivée, vous devez supprimer manuellement les plages inutilisées de la liste Plages réseau. Le broker ne détecte pas si une plage d'adresses est utilisée et ne supprime pas automatiquement des plages de la liste.

Conditions préalables

Identifiez les adresses NAT (traduction d'adresse réseau) de sortie sur votre routeur ou pare-feu de bureau ou de centre de données qui correspondent au trafic de vos utilisateurs finaux internes.

Procédure

1. Connectez-vous à Horizon Cloud Service - next-gen.
2. Cliquez sur **Paramètres** dans la barre de navigation.
3. Cliquez sur **Gérer** sur la vignette **Paramètres du client**.
4. Sur la page **Paramètres du client**, cliquez sur l'onglet **Plages réseau**.

   La page **Plages réseau** affiche une liste des plages d'adresses IP publiques correspondant au trafic de vos utilisateurs finaux internes.
5. Pour ajouter une plage d'adresses NAT de sortie à la liste, cliquez sur **Ajouter**.
6. Sélectionnez un type de plage, entrez une adresse ou une plage pour ce type, puis cliquez sur **Enregistrer**.

Option	Description
CIDR	Sélectionnez **CIDR** et entrez une plage entre les plages autorisées de /1 et de /32, telle que 192.168.70.10/32.
Adresse IP unique	Sélectionnez **Adresse IP unique** et entrez une adresse IP, telle que 192.168.70.10.
Plage d'adresses IP	Sélectionnez **Plage d'adresses IP** et entrez une plage d'adresses IP, telle que 192.168.70.10-192.168.72.32.

7. Continuez à ajouter davantage de plages d'adresses NAT de sortie à la liste jusqu'à ce que vous ayez défini l'étendue complète de votre trafic réseau interne.

Étape suivante

Vous pouvez utiliser les contrôles de l'onglet Plages réseau pour **Supprimer** une plage de la liste.

Note Avant de supprimer une plage de la liste, prenez en compte les points suivants :

- Lorsque vous supprimez une plage d'adresses NAT de sortie, le broker considère que cette plage fait partie du réseau externe.
- Si vous supprimez toutes les plages de la liste, le broker traite tous les utilisateurs comme des utilisateurs externes. Par conséquent, les stratégies appliquées aux utilisateurs internes ne prendront plus effet.

Activation de la rampe d'accès au droit cloud d'Horizon pour accéder aux postes de travail Horizon 8 et Horizon Cloud on Azure

Le paramètre global Rampe d'accès au droit cloud d'Horizon permet aux utilisateurs d'accéder aux postes de travail Horizon 8 et Horizon Cloud on Azure avec leurs informations d'identification à partir d'une seule instance d'Horizon Client pour Windows, évitant ainsi d'utiliser plusieurs URL, déconnexions ou une authentification supplémentaire sur le cloud.

Conditions préalables

- Vérifiez que vous avez enregistré un fournisseur d'identité (IDP) pris en charge, Microsoft Entra ID ou VMware Workspace ONE Access (sur site/cloud), dans votre locataire VMware Horizon Cloud Service - next-gen. Le fournisseur d'identité enregistré facilite la synchronisation des identités d'utilisateur Active Directory sur site avec ce fournisseur d'identité.
- Veillez à exécuter Horizon Connection Server version 2312 ou ultérieure.
- Vérifiez que vous avez déployé le dispositif Horizon 8 Edge pour connecter votre espace Horizon 8 au plan de contrôle Horizon Cloud Service - next-gen.
- Dans la console Horizon Universal Console, avec Microsoft Azure comme fournisseur de capacité, créez un pool, déployez des instances de poste de travail et attribuez des droits.
- Dans Horizon Console, créez des pools Horizon 8 et attribuez des droits pour l'architecture Cloud Pod ou locale.
- Vérifiez que vos utilisateurs finaux exécutent Horizon Client 2312 pour Windows ou version ultérieure.

Fonctionnement de la rampe d'accès au droit cloud d'Horizon

La fonctionnalité de rampe d'accès au droit cloud d'Horizon utilise le Serveur de connexion comme mécanisme d'intermédiation pour accorder aux utilisateurs l'accès à des postes de travail Horizon Cloud on Azure. Vous pouvez utiliser Microsoft Entra ID ou Workspace ONE Access (sur site/cloud) comme fournisseur d'identité (IDP) pour votre locataire VMware Horizon Cloud Service - next-gen.

Votre choix de fournisseur d'identité facilite la synchronisation des comptes d'utilisateurs, des appartenances à des groupes et d'autres objets d'annuaire depuis Active Directory sur site vers le fournisseur d'identité basé sur le cloud. Cette synchronisation garantit que les utilisateurs disposent d'une authentification cohérente, qu'ils accèdent à des ressources sur site ou basées sur le cloud.

Si vous utilisez Workspace ONE Access comme fournisseur d'identité, un connecteur est déployé pour synchroniser les comptes d'utilisateurs et les appartenances à des groupes avec la plate-forme Workspace ONE Access.

Lorsqu'un utilisateur se connecte à une instance du Serveur de connexion, ce dernier valide les droits d'accès de cet utilisateur à tous les postes de travail Horizon Cloud on Azure. Horizon Client affiche ensuite ces postes de travail avec les postes de travail Horizon 8 dans la même fenêtre de sélection des postes de travail et applications. De cette manière, les utilisateurs peuvent accéder à leurs droits Horizon Cloud on Azure directement via le Serveur de connexion ou le nom de domaine complet Unified Access Gateway. Une URL distincte n'est plus requise pour le portail VMware Horizon Cloud Service - next-gen.

Chaque droit Horizon 8 affiché dans la fenêtre de sélection peut être un droit local ou un droit global. Les droits Horizon 8 et les droits Horizon Cloud on Azure s'affichent sous forme de postes de travail individuels dans la fenêtre de sélection et l'utilisateur doit sélectionner le poste de travail auquel se connecter. À ce stade, la rampe d'accès au droit cloud d'Horizon ne prend pas en charge la capacité de définir une stratégie de connexion entre les droits Horizon 8 et Horizon Cloud on Azure.

Important Notez les limitations de fonctionnalités suivantes :

- Actuellement, seul Horizon Client 2312 pour Windows ou version ultérieure est pris en charge pour cette fonctionnalité. La prise en charge sera disponible à l'avenir pour d'autres instances d'Horizon Client.
- Si vous configurez des messages de restriction du client à partir d'Horizon Console et d'Horizon Universal Console, ces messages ne s'affichent pas simultanément sur le client. Au lieu de cela, le premier message s'affiche momentanément avant d'être remplacé par le second.

Vous pouvez activer la rampe d'accès au droit cloud d'Horizon au niveau de l'espace Horizon 8 et au niveau de l'utilisateur. Par défaut, elle est désactivée pour tous les utilisateurs. Un administrateur doit activer cette fonctionnalité, comme décrit dans les sections suivantes de cette page.

Activer la rampe d'accès au droit cloud d'Horizon dans le plan de contrôle Horizon Cloud

Effectuez la première partie du processus d'activation de la fonctionnalité à l'aide de la console Horizon Universal Console.

1 Connectez-vous à la console Horizon Universal Console.

2 Sur la page **Accueil**, cliquez sur **Dispositifs Horizon Edge** sur la vignette **Dispositifs Horizon Edge**.

3 Dans l'onglet **Dispositifs Horizon Edge** de la page **Capacité**, cliquez sur le nom d'une instance d'Horizon Edge avec un **Type de fournisseur Horizon 8** vers sa page de détails du dispositif **Horizon Edge**.

4 Dans la vignette **Rampe d'accès au droit cloud**, cliquez sur **Activer**.

   La console Horizon Universal Console transfère la configuration vers la passerelle Passerelle Horizon Edge pour un déploiement d'Horizon 8 sur site, où il transfère à son tour la configuration vers Horizon Connection Server et active la fonctionnalité de rampe d'accès au droit cloud d'Horizon dans Horizon Console.

5 Passez à la section suivante de cette page pour ajouter des droits d'utilisateur dans Horizon Console.

Ajouter des droits d'accès à la rampe d'accès au droit cloud d'Horizon dans Horizon Console

Après avoir activé la fonctionnalité de rampe d'accès au droit cloud d'Horizon dans le plan de contrôle Horizon Cloud, vous devez configurer les droits d'accès à la **rampe d'accès au droit cloud d'Horizon** dans Horizon Console pour les utilisateurs et les groupes appropriés.

1 Connectez-vous à Horizon Console.

2 Dans **Paramètres généraux**, vérifiez que le paramètre **Rampe d'accès au droit cloud** est activé.

   Note Si le paramètre ne s'affiche pas, vérifiez la connectivité réseau entre la passerelle Passerelle Horizon Edge, la console Horizon Universal Console et Horizon Connection Server.

3 Accédez à **Utilisateurs et groupes > Rampe d'accès au droit cloud** et cliquez sur **Ajouter**.

4 Ajoutez les utilisateurs et les groupes qui doivent accéder à des postes de travail Horizon Cloud on Azure.

Dépannage de votre plan de contrôle Horizon et de votre environnement Horizon Cloud Service - next-gen

8

Des instructions de dépannage sont souvent fournies dans l'interface utilisateur du produit et dans la rubrique de la documentation applicable pour le plan de contrôle Horizon et Horizon Cloud Service - next-gen.

Vous pouvez également utiliser les ressources suivantes pour faciliter le dépannage :

- Articles sur le support fournisseur, les communautés et la base de connaissances (KB) pour Horizon Cloud Service dans VMware Customer Connect.
- Blogs, vidéos et articles de marketing technique pour Horizon Cloud Service dans la Digital Workspace Tech Zone.

Si vous rencontrez des problèmes ou des erreurs lors de votre workflow de déploiement du dispositif Edge, les pages suivantes décrivent plusieurs problèmes et leur solution de dépannage ou les étapes de correction :

- Horizon 8 Edge est bloqué dans l'état Connexion en attente
- Erreur « Les informations d'identification d'Horizon Connection Server fournies sont incorrectes »
- Erreur de délai d'expiration du Serveur de connexion
- Tout fonctionnait auparavant contrairement à maintenant
- Afficher l'ancien flux dans lequel les détails d'Horizon Connection Server sont requis lors de la création du fournisseur

Lisez les sections suivantes :

- Diagnostic de Dispositifs Horizon Edge : connectivité Active Directory pour les déploiements Microsoft Azure
- Horizon 8 Edge est bloqué dans l'état Connexion en attente
- Erreur « Les informations d'identification d'Horizon Connection Server fournies sont incorrectes »
- Erreur de délai d'expiration du Serveur de connexion
- Tout fonctionnait auparavant contrairement à maintenant

- Afficher l'ancien flux dans lequel les détails d'Horizon Connection Server sont requis lors de la création du fournisseur

Diagnostic de Dispositifs Horizon Edge : connectivité Active Directory pour les déploiements Microsoft Azure

Vous pouvez effectuer un diagnostic à la demande sur votre Dispositifs Horizon Edge. Le diagnostic d'Active Directory est pris en charge. Si vous détectez un problème avec Active Directory lié aux dispositifs Dispositifs Horizon Edge, vous pouvez utiliser Horizon Universal Console pour diagnostiquer le problème, en particulier sur la page **Surveiller > Diagnostic**. Ensuite, vous pouvez accéder directement à la configuration d'Active Directory pour déterminer ce qui empêche une connexion appropriée et la corriger.

Configurez Active Directory pour Microsoft Azure au début du déploiement. Reportez-vous aux sections Conditions requises pour l'identité de machine et Configuration de votre domaine Active Directory. S'il existe un problème de configuration avec Active Directory, vous pouvez exécuter un test sur la page Diagnostic d'Horizon Universal Console qui effectue les opérations suivantes.

- Teste la connectivité Active Directory (qui peut correspondre à une ou plusieurs instances) à Dispositifs Horizon Edge.
- Vérifie les informations d'identification du domaine (domaine principal, domaine auxiliaire et SSO) d'Active Directory.

Accéder à la page **Diagnostic**

Lorsque vous détectez un problème avec Active Directory, consultez la page Diagnostic à des fins d'analyse plus approfondie.

Pour accéder à la page Diagnostic, dans Horizon Universal Console, sélectionnez **Surveiller > Diagnostic**.

Note Vous pouvez afficher des informations historiques sur les erreurs liées à Active Directory sur la page **Accueil > Dispositifs Horizon Edge présentant des erreurs d'infrastructure**. Reportez-vous à la section Données de surveillance des ressources : erreurs.

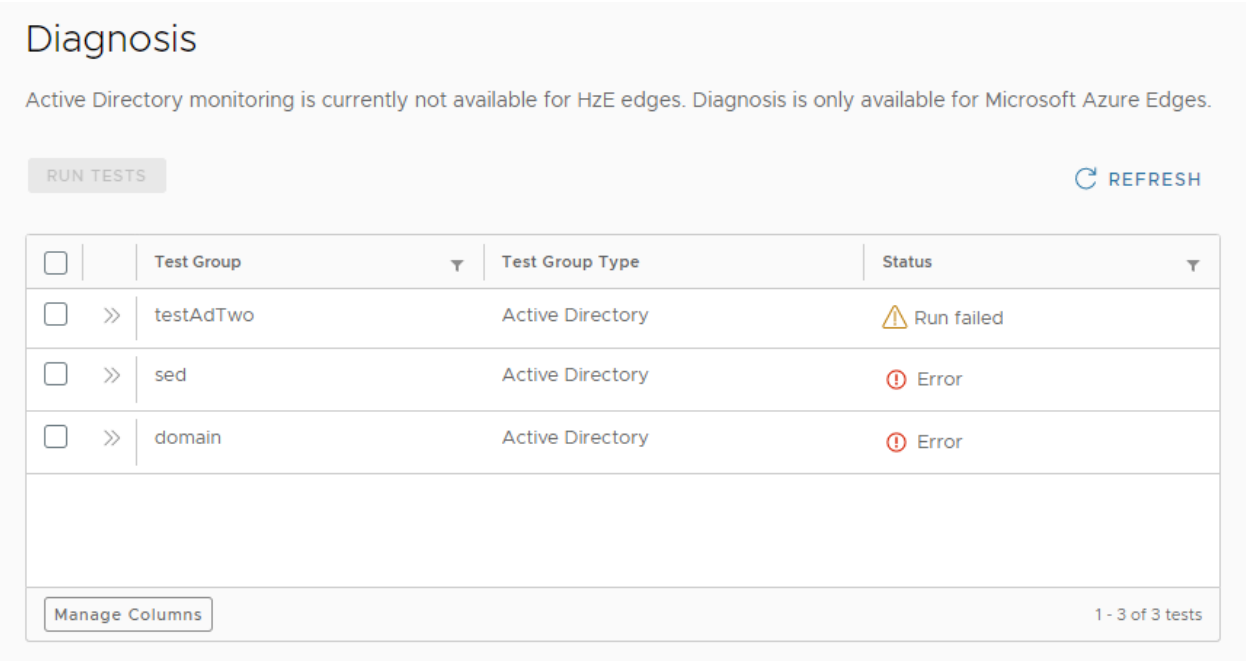
Afficher la page Diagnostic

La page Diagnostic répertorie toutes les instances d'Active Directory trouvées, le cas échéant.

Lorsque des groupes de tests (instances d'Active Directory) sont répertoriés, les informations suivantes sont spécifiées.

- Nom de chaque groupe de tests
- État de diagnostic global d'un groupe de tests.

L'état de diagnostic global fournit une présentation de la connectivité entre Active Directory et tous les dispositifs Microsoft Azure Edge. Si un ou plusieurs dispositifs Microsoft Azure Edge sont dans un état d'erreur, celui-ci indique **Erreur**. Pour vérifier l'état de chaque dispositif Microsoft Azure Edge, vous devez développer le groupe de tests.



Exécuter des tests

Sur la page Diagnostic, vous pouvez exécuter des tests de diagnostic sur l'un des groupes de tests répertoriés sur tous les dispositifs Microsoft Azure Edge.

1 Cochez la case en regard du nom du groupe de tests que vous souhaitez tester.

2 Cliquez sur **Exécuter des tests**.

Les tests s'exécutent pour chaque groupe de tests sélectionné.

Vérifiez les résultats de la connectivité Active Directory

Sur la page Diagnostic, vous pouvez examiner l'état de chaque groupe de tests un par un.

Les descriptions d'état suivantes sont utiles pour distinguer les types d'état.

Réussite

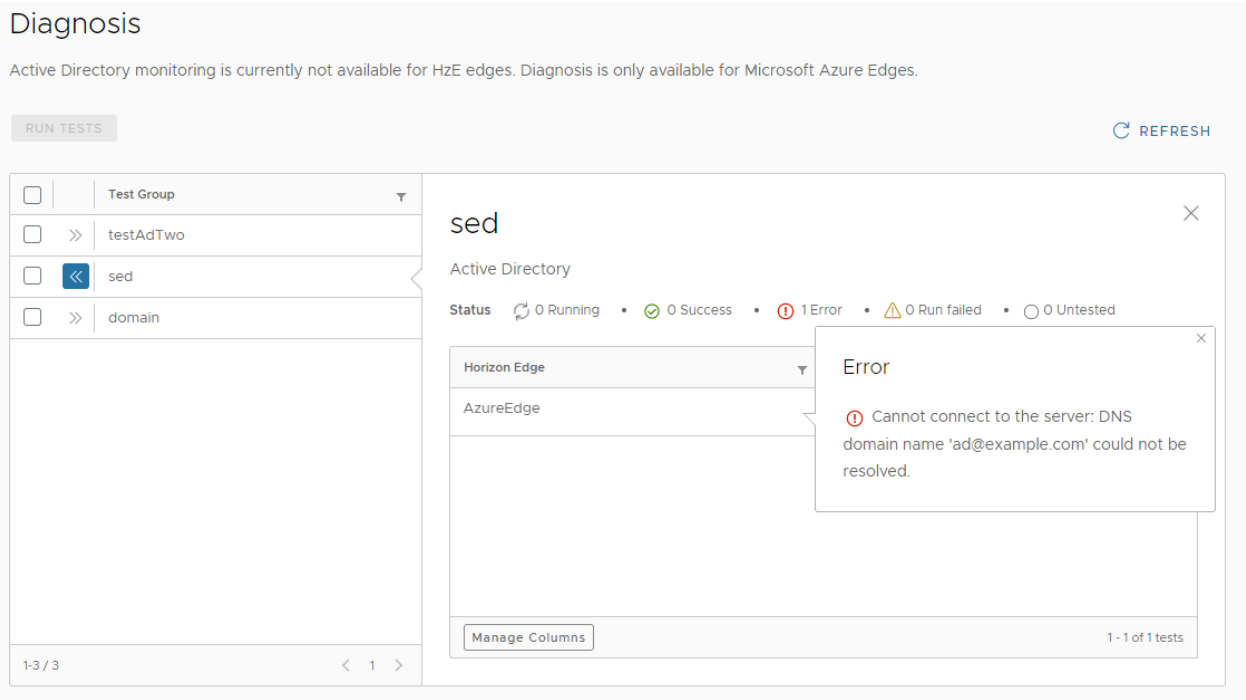
Connectivité réussie (aucune erreur de connectivité).

Erreur

Il existe des problèmes de connectivité. Le message d'erreur explique la cause exacte de l'erreur. Utilisez les informations du message d'erreur pour apporter les modifications requises à la configuration d'Active Directory.

Échec de l'exécution

Le test ne s'est pas terminé. Réexécutez le test.



1 Cliquez sur la flèche à deux pointes en regard d'un groupe de tests à vérifier.

Un volet s'ouvre et affiche l'état de diagnostic de chaque dispositif Microsoft Azure Edge de ce groupe de tests.

2 Pour vérifier une erreur, cliquez sur **Erreur** dans la colonne État du dispositif Horizon Edge pour lequel vous souhaitez afficher le message d'erreur.

Il existe différents types de messages d'erreur. Voici un exemple de message d'erreur concernant le compte de liaison principal, qui indique que vous devez vérifier les informations d'identification entrées pour le compte de liaison principal : `Error connecting to AD server using Primary Bind Account`

3 Utilisez les informations spécifiées dans le message d'erreur pour vous aider à résoudre le problème lorsque vous accéderez ultérieurement à la configuration d'Active Directory.

Horizon 8 Edge est bloqué dans l'état Connexion en attente

Problème

Horizon 8 Edge est bloqué dans l'état **Connexion en attente**.

Cause

Le code de couplage n'a pas été fourni lors du déploiement de la passerelle Passerelle Horizon Edge dans VMware vCenter. Le code de couplage est requis pour créer l'espace de noms Kubernetes dans la passerelle Passerelle Horizon Edge qui dispose des modules requis pour marquer le dispositif Edge dans d'autres états (cela peut prendre parfois entre 15 et 20 minutes). Le code de couplage est présent sur le deuxième écran de VMware vCenter, au-dessous du mot de passe racine.

Si le code de couplage est fourni correctement, vérifiez l'appel d'API edge-deployments. L'appel d'API edge-deployments doit être semblable à l'exemple suivant :

```
admin/v2/edge-deployments/63da2d9216884348cf96a0f5?include_reported_status=true
```

Dans l'interface utilisateur, elle est appelée lorsque la page de détails d'un déploiement du dispositif Edge est ouverte. Assurez-vous que **view-cs-module** se trouve sous **registeredModules** et dans **reportedStatus > moduleConnectionDetails**, **view-cs-module** doit être présent et être dans l'état **CONNECTED**.

Pour plus d'informations, reportez-vous à la section https://kb.vmware.com/s/article/92056.

Solution

Assurez-vous que **view-cs-module** se trouve sous **registeredModules** et dans **reportedStatus > moduleConnectionDetails**, **view-cs-module** doit être présent et être dans l'état **CONNECTED**.

Effectuez également les tâches suivantes.

1. Assurez-vous que la passerelle Passerelle Horizon Edge est correctement déployée et qu'elle est dans l'état sous tension. En cas de problème de déploiement, vérifiez la mise en réseau, le stockage, etc.
2. Utilisez les versions `2.3.1.0` ou ultérieures d'OVA de la passerelle Passerelle Horizon Edge pour spécifier une clé publique pour que l'utilisateur `ccadmin` se connecte. Les anciennes versions d'OVA présentent un problème lors de l'initialisation de Kubernetes lorsque la clé publique est spécifiée pour l'utilisateur `ccadmin`.
3. Exécutez le script de diagnostic en mode de débogage. Pour plus d'informations, reportez-vous à l'article https://kb.vmware.com/s/article/92056. Dans la section **Cluster Kubernetes**, un espace de noms créé lors de la première mise sous tension de la passerelle Passerelle Horizon Edge doit s'afficher.
    a. Si ce n'est pas le cas et si l'espace de noms n'est pas créé, cela peut être dû au fait que le réseau n'a pas été configuré correctement à l'étape 2, ou que le code de couplage n'a pas été fourni lors de la création de la passerelle Edge lors du déploiement d'OVA de la passerelle Edge.

Vous pouvez configurer le code de couplage après le déploiement du dispositif de passerelle Passerelle Horizon Edge, s'il n'a pas été fourni lors du déploiement du dispositif de passerelle Passerelle Horizon Edge. Copiez le code de couplage à partir d'Horizon Universal Console et exécutez la commande suivante pour configurer le code de couplage après le déploiement du dispositif de passerelle Passerelle Horizon Edge `/opt/vmware/bin/pair-edge .sh '<Pairing_Code_Copied_From_Horizon_Universal_Console>`.

b Si l'espace de noms est créé et que le dispositif Edge est toujours bloqué dans l'état En attente de connexion, cela peut être dû à des problèmes de connectivité réseau ou à des URL de cloud inaccessibles à partir du dispositif Edge (cela peut provenir de la configuration du proxy ou d'autres problèmes liés au réseau), voire à la mise à jour de la configuration du proxy dans le dispositif Edge.

c Ensuite, si l'espace de noms est créé, il faut entre 15 et 20 minutes pour que le dispositif Edge s'affiche dans l'état `Non configuré`, comme indiqué dans l'interface utilisateur ou `POST_PROVISIONING_CONFIG_IN_PROGRESS` dans l'API. Si cela se produit, vous devriez être en mesure de configurer le Serveur de connexion.

Si cela ne se produit toujours pas, exécutez le script de diagnostic et sous la section **Cluster Kubernetes**, attendez que l'espace `view-cs-module` soit en cours d'exécution. Exécutez le script de diagnostic en mode de débogage. Pour plus d'informations, reportez-vous à l'article https://kb.vmware.com/s/article/92056.

Erreur « Les informations d'identification d'Horizon Connection Server fournies sont incorrectes »

Problème

Le client obtient une erreur, par exemple, `VIEW_INCORRECT_CS_CREDENTIALS`

Cause

Cela se produit probablement en raison des détails d'Horizon Connection Server incorrects fournis.

Solution

Assurez-vous que les conditions suivantes sont réunies :

Le nom d'utilisateur et le mot de passe du Serveur de connexion doivent être corrects. Le nom de domaine complet doit correspondre à l'URL réelle, par exemple `https://cs83.hzeccad.com` et non à l'adresse IP du Serveur de connexion. Exemple de détails d'Horizon Connection Server :

```
{
    "providerDetails": {
        "data": {
            "domain": "hzeccad.com",
            "viewPodURL": "https://cs83.hzeccad.com",
            "username": "Administrator",
```

```
            "password": "*******",
            "thumbprint": "E4:3B:70:DE:AF:0F:44:F8:6E:87:0C:F1:F6:2D:09:2F:A5:E3:4A:4B"
        }
    }
}
```

Note Dans cet exemple, ********* représente votre mot de passe réel.

Erreur de délai d'expiration du Serveur de connexion

Problème

Vous obtenez une erreur, par exemple, `Impossible de valider les informations d'identification du Serveur de connexion, car la demande à ce dernier a expiré.`

Cause

Horizon Connection Server est surchargé.

Solution

1 Assurez-vous que le Serveur de connexion n'est pas surchargé.

2 Cette erreur peut également se produire si des détails d'Horizon Connection Server incorrects sont fournis. Réessayez donc ultérieurement.

Tout fonctionnait auparavant contrairement à maintenant

Problème

Tout fonctionnait auparavant contrairement à maintenant.

Cause

Les détails d'Horizon Connection Server ont été mis à jour dans VMware vCenter et non dans Horizon Cloud Service - next-gen.

Solution

Assurez-vous que les détails du Serveur de connexion sont mis à jour dans VMware vCenter et non dans Horizon Cloud Service - next-gen. Vérifiez également la date d'expiration du certificat et assurez-vous que l'empreinte numérique n'a pas été modifiée.

Afficher l'ancien flux dans lequel les détails d'Horizon Connection Server sont requis lors de la création du fournisseur

Problème

Le client observe l'ancien flux dans lequel les détails d'Horizon Connection Server sont requis lors de la création du fournisseur ou constate l'échec de l'API ci-dessous.

```
domain:  SG_ADMIN
code:    PROVIDER_INSTANCE_CREDENTIALS_ERROR
message: Credential service error for Provider Instance
details: Cannot create a provider instance without any sensitive data!
```

Cause

Il se peut que les indicateurs de fonctionnalités `astro-cs-sync-validation` pour l'interface utilisateur et `cs-sync-flag` pour l'API soient désactivés pour le client.

Solution

Vous pouvez les vérifier dans l'appel d'API public-flag. S'ils sont désactivés, le client observe l'ancien flux, ce qui nécessite les détails d'Horizon Connection Server à l'étape fournisseur. Assurez-vous donc que ces indicateurs de fonctionnalité sont activés pour l'organisation du client.

Meilleures pratiques et recommandations afin d'utiliser Horizon Cloud Service - next-gen

9

Explorez ces meilleures pratiques utiles et les workflows suggérés pour vous aider à optimiser les avantages des fonctionnalités d'Horizon Cloud Service - next-gen dans votre organisation.

Lisez les sections suivantes :

- Conseils d'utilisation de la console Horizon Universal Console et de votre locataire
- Utilisation du bouton Aide pour accéder à la documentation et au support
- Partage de vos commentaires sur le produit
- Utilisation des cookies et outils d'analyse tiers
- Fermeture d'une page

Conseils d'utilisation de la console Horizon Universal Console et de votre locataire

La console Horizon Universal Console affiche dynamiquement des éléments pour les fonctionnalités en fonction des conditions les plus récentes de votre locataire.

Ces conditions incluent des éléments tels que ce que votre abonnement permet, ce que vos services complémentaires achetés permettent, les types de déploiements du dispositif Edge dans votre locataire, etc. Pour connaître les types d'éléments régis par votre abonnement, reportez-vous à la Matrice de comparaison des abonnements Horizon. Vous ne verrez pas d'éléments dans Horizon Universal Console pour les fonctionnalités que votre abonnement ne prend pas en charge ou pour les fonctionnalités fournies par des services complémentaires achetés pour une utilisation avec des instances d'Horizon Universal Subscription.

Utilisez les rubriques suivantes pour en savoir plus sur les fonctionnalités de la console Horizon Universal Console.

Utilisation du bouton Aide pour accéder à la documentation et au support

Le bouton Aide permet d'explorer la documentation d'Horizon Cloud Service - next-gen et des produits associés pour trouver les réponses aux questions et accéder à Customer Connect pour obtenir une assistance, ouvrir des tickets et afficher l'historique de vos tickets.

Conditions préalables

Le processus d'intégration est terminé.

Procédure

1. Connectez-vous à Horizon Universal Console.
2. Cliquez sur le bouton **Aide** sur la page d'accueil.
3. Entrez vos mots-clés dans le champ de recherche pour rechercher des rubriques pertinentes et connexes.

   Les liens de document associés à la page actuelle s'affichent dans une liste lorsque vous cliquez sur le bouton d'aide. Par exemple, si vous vous trouvez sur la page des pools et que vous cliquez sur le bouton d'aide, tous les liens de document connexes associés aux pools sont répertoriés dans le panneau d'aide.
4. Cliquez sur **AFFICHER PLUS DANS LES DOCUMENTS** pour accéder à la page Documentation.
5. Cliquez sur la vignette **Créer une demande de support** pour accéder à **Customer Connect** pour ouvrir un ticket de support.
6. Cliquez sur **Afficher toutes mes demandes de support** pour afficher la liste de toutes vos demandes de support.
7. Cliquez sur **FOURNIR UN COMMENTAIRE SUR VOTRE EXPÉRIENCE DE SUPPORT** pour fournir vos commentaires.

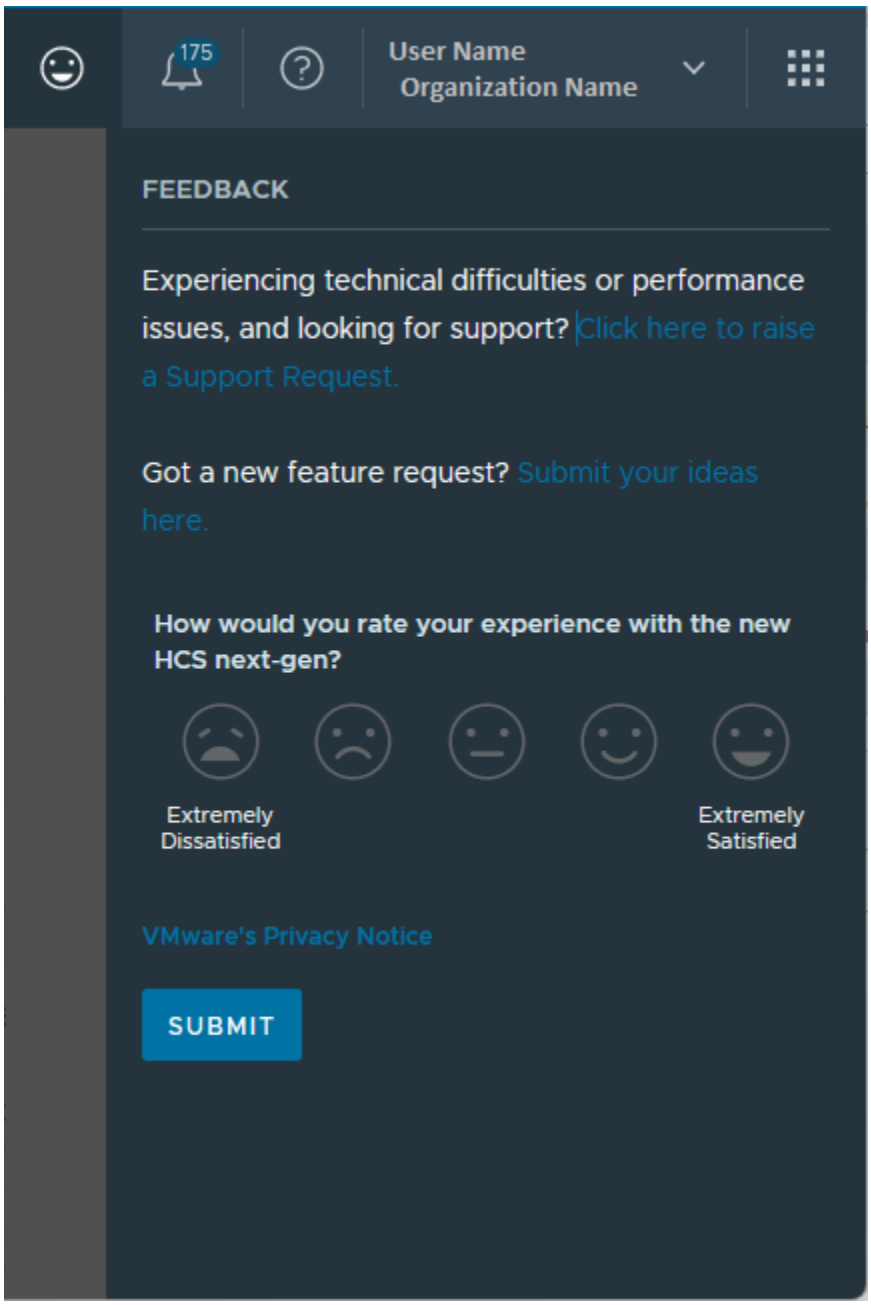
Partage de vos commentaires sur le produit

Les commentaires sur les produits sont une fonctionnalité qui vous permet de partager vos commentaires pour nous aider à améliorer le produit que vous utilisez.

Vous pouvez partager des commentaires de deux manières :

- À tout moment, vous pouvez cliquer sur l'icône Commentaires  en haut de la console pour ouvrir le panneau Commentaires, qui s'ouvre sur le côté droit de la console.
- Le panneau Commentaires peut s'afficher lorsque vous vous connectez à la console. Le panneau s'ouvre au centre de la console.

La capture d'écran suivante est celle du panneau Commentaires qui s'affiche lorsque vous cliquez sur l'icône Commentaires.



Une fois le panneau Commentaires ouvert, vous pouvez prendre les mesures suivantes.

Générez une demande de support.

Si vous n'êtes pas connecté à Customer Connect lorsque vous cliquez sur le lien permettant d'effectuer une demande de support, vous êtes dirigé vers la page Customer Connect pour le faire.

Une fois connecté, vous êtes dirigé vers la page Support, sur laquelle vous pouvez choisir parmi différentes options de support.

Envoyez une idée.

Si vous n'êtes pas connecté à Customer Connect lorsque vous cliquez sur le lien permettant de partager une idée, vous êtes dirigé vers Customer Connect pour le faire.

Une fois connecté, vous êtes dirigé vers le portail de demandes de fonctionnalités dans lequel vous êtes invité à sélectionner un espace de travail, par exemple **Horizon**, et à partager une idée pour cet espace de travail.

Évaluez le produit.

Lorsque vous sélectionnez l'une des icônes **Évaluer votre expérience**, le panneau se développe pour vous permettre de fournir des commentaires spécifiques et d'indiquer si vous êtes prêt à participer à un entretien de suivi.

Utilisation des cookies et outils d'analyse tiers

Horizon Cloud collecte des données pour observer et améliorer l'expérience client et à d'autres fins.

Horizon Cloud collecte les données conformément aux Avis de confidentialité VMware. Certaines de ces données sont collectées à l'aide de cookies et d'une technologie similaire telle que Pendo.

Pendo est un outil tiers intégré à Horizon Cloud, qui collecte des cookies pour déterminer comment les fonctionnalités du produit sont utilisées en suivant les interactions et l'utilisation des fonctionnalités par les administrateurs.

Fermeture d'une page

Dans Horizon Cloud Service - next-gen, si vous tentez de fermer une page sans terminer le workflow, vous recevrez une notification vous informant de rester sur la page au risque de perdre vos données.

Procédure

1. Si vous cliquez sur **Précédent** ou sur un lien avant de terminer toutes les étapes de la page, une boîte de dialogue s'affiche pour vous rappeler que vos modifications risquent d'être perdues si vous quittez cette page. Cliquez sur **Annuler** pour rester sur la page ou sur **Quitter** pour quitter la page.
2. Si vous cliquez sur **Actualiser** pour actualiser la page avant de terminer toutes les étapes de la page, une boîte de dialogue s'affiche pour vous rappeler que vos modifications risquent d'être perdues si vous quittez cette page. Cliquez sur **Recharger** pour actualiser la page ou sur **Annuler** pour rester sur la page.
3. Si vous tentez de fermer l'onglet ou la fenêtre avant de terminer toutes les étapes de la page, une boîte de dialogue s'affiche pour vous rappeler que vos modifications seront perdues si vous quittez cette page. Cliquez sur **Quitter** pour quitter la page ou sur **Annuler** pour rester sur la page.

Documentation d'Horizon Plus 10

La page Documentation d'Horizon Plus décrit comment démarrer avec l'utilisation du service.

E-mail de bienvenue

VMware envoie un e-mail de bienvenue au compte d'administrateur pour confirmer l'évaluation ou l'achat de la licence. L'e-mail confirme l'inscription et contient un lien d'invitation pour utiliser l'accès à VMware Horizon Cloud.

VMware Horizon® Cloud Service™ fait partie de la solution Anywhere Workspace globale.

Le service de licence Horizon Cloud dans VMware Horizon® Cloud Service™ - next-gen s'assure que les administrateurs informatiques peuvent accéder aux fonctionnalités par type de licence acheté et les exploiter.

Reportez-vous à la Matrice de comparaison des abonnements VMware Horizon pour obtenir une comparaison des fonctionnalités de licence d'abonnement Horizon, qui classe globalement les licences sous la forme Durée et SaaS. Les fonctionnalités répertoriées ne s'appliquent pas toutes actuellement à VMware Horizon® Cloud Service™ - next-gen.

Note L'e-mail de bienvenue ne contient pas d'informations sur le type de licence acheté. Vous pouvez obtenir ces informations à partir de votre compte VMware Customer Connect™. Pour devenir un utilisateur de Customer Connect, reportez-vous à l'article 2007005 de la base de connaissances.

Une fois le processus d'intégration terminé, vous pouvez suivre vos licences Horizon à partir d'Horizon Universal Console. À ce stade, lorsque vous avez accès uniquement au plan de contrôle Horizon de nouvelle génération, contactez le support VMware pour qu'il vous envoie les clés perpétuelles. Pour plus d'informations, reportez-vous à la section Utiliser Horizon Universal Console pour suivre vos licences Horizon.

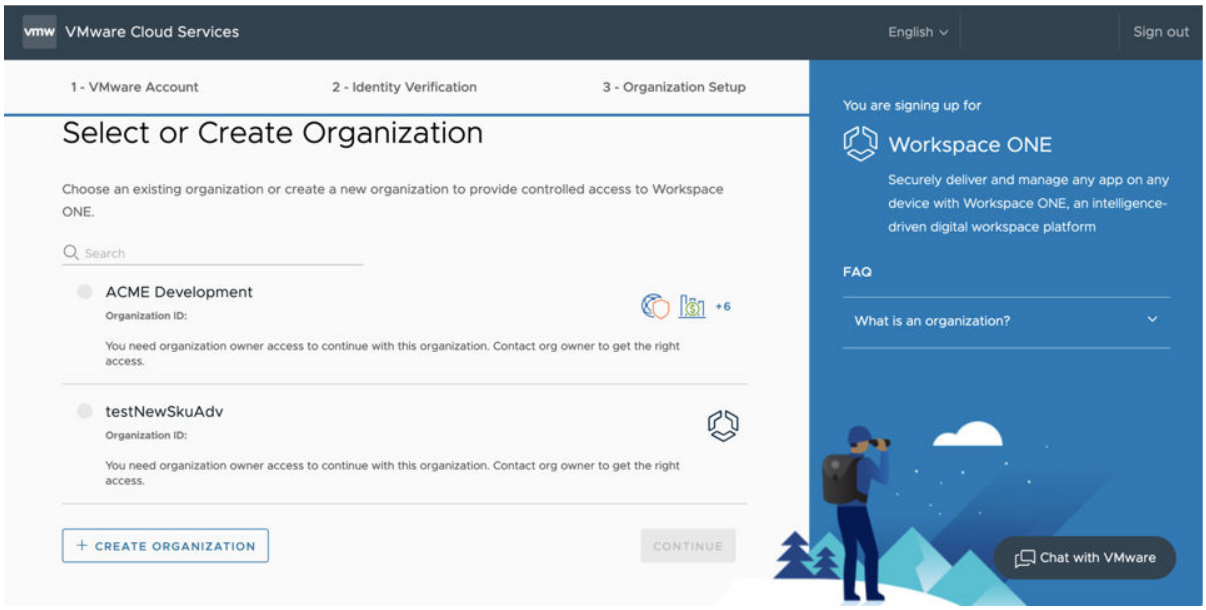
Connectez-vous à la console VMware Cloud Services.

Note Pour plus d'informations sur les VMware Cloud™ Services, reportez-vous à la documentation du produit VMware Cloud Services. D'autres noms de VMware Cloud services s'affichent dans la documentation et les produits VMware, par exemple « Plate-forme VMware Cloud Services » (CSP) et « Plate-forme d'engagement de VMware Cloud Services ».

1 Créez un compte VMware Cloud services.

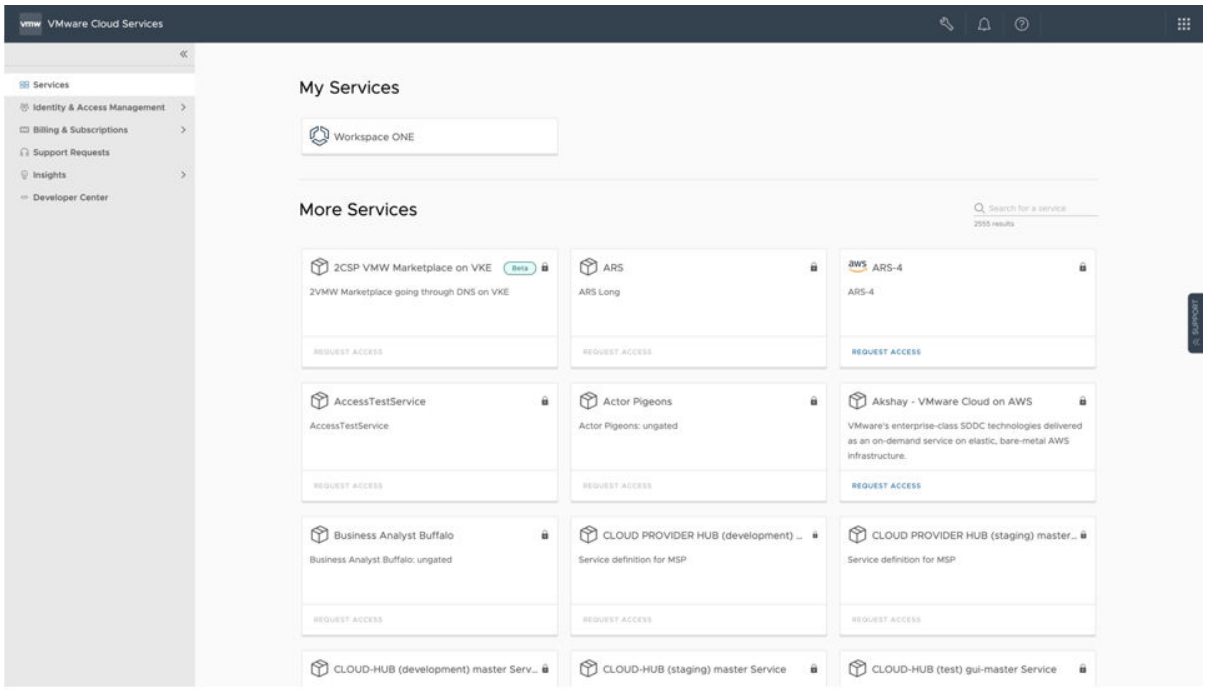
Les instructions commencent par votre e-mail de bienvenue. Cliquez sur le lien dans l'e-mail, créez un compte VMware Cloud services et utilisez votre ID de VMware pour vous connecter à VMware Cloud services.

La console VMware Console Cloud Services s'ouvre sur la page Configuration de l'organisation.



2 Entrez un nom d'organisation de votre choix et cliquez sur **Créer une organisation et terminer l'inscription**.

La console VMware Cloud services s'affiche et indique tous les services dont vous disposez



3 Cliquez sur votre nom dans le coin supérieur droit, puis sur **Afficher l'organisation**.

Revenez à la console VMware Console Cloud Services dans laquelle vous pouvez désormais attribuer les rôles requis.

À propos de l'ajout d'autres utilisateurs et de l'attribution de rôles

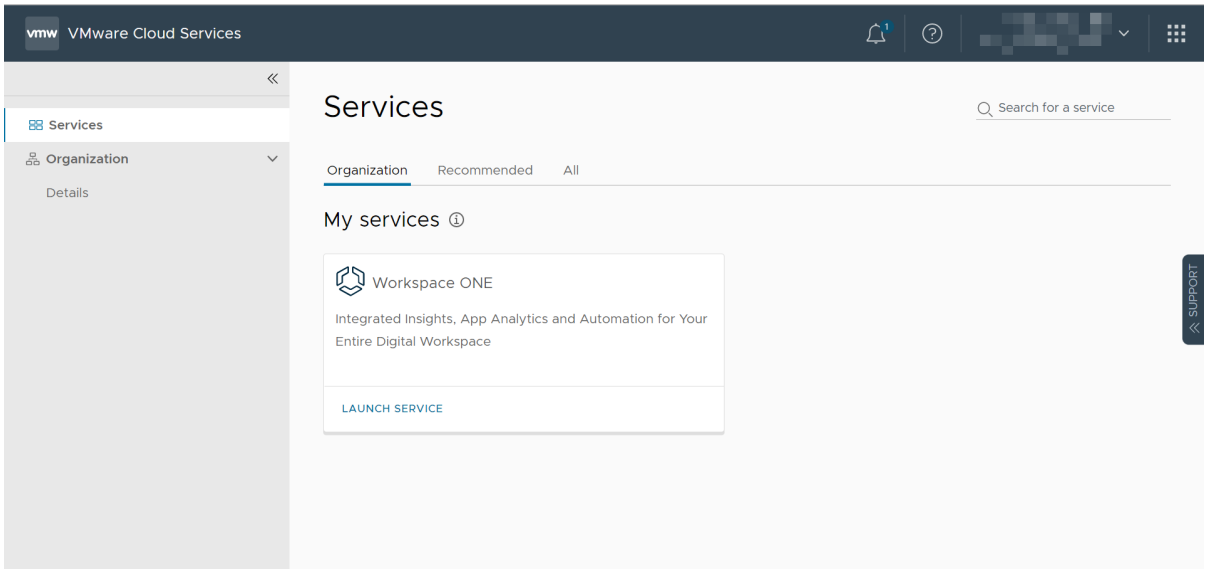
Lorsque vous utilisez le lien de l'e-mail de bienvenue pour récupérer l'invitation, le rôle Administrateur vous est automatiquement attribué. Le rôle Administrateur vous octroie des autorisations complètes pour l'interface utilisateur et les API d'Horizon Universal Console que vous devez intégrer. Vous pouvez fournir à d'autres utilisateurs administratifs des droits d'accès à Horizon Universal Console. Pour plus d'informations, reportez-vous à la section Attribution de rôles administratifs aux utilisateurs Horizon Universal Console

Utiliser la console VMware Console Cloud Services pour lancer Workspace ONE

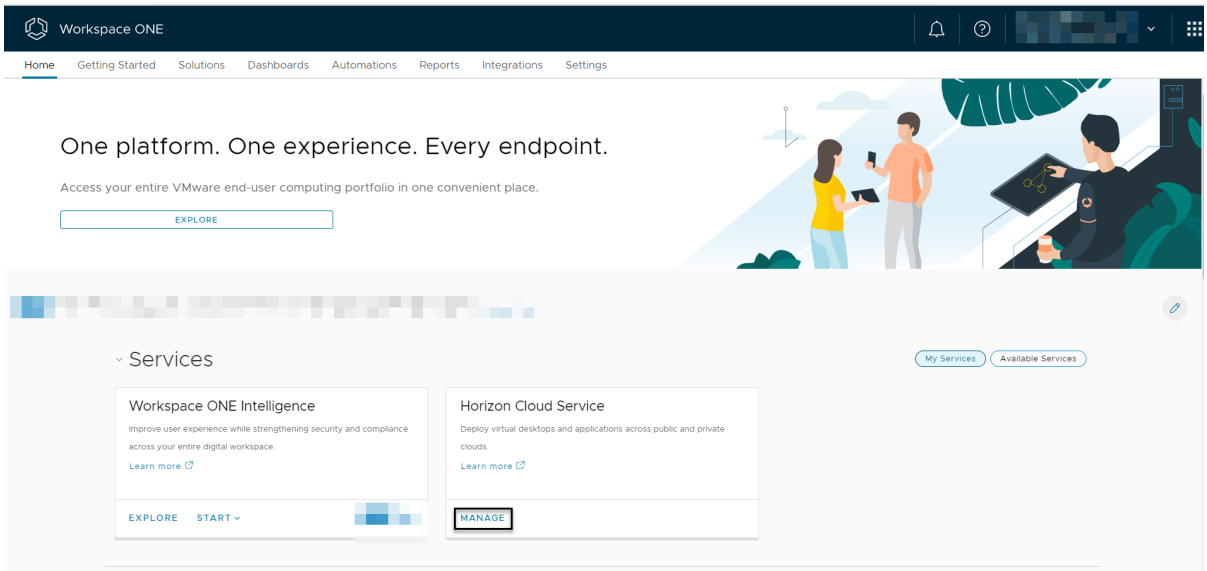
Pour lancer Horizon Cloud, procédez comme suit.

1 Dans le volet de gauche, cliquez sur **Services**.

2 Cliquez sur **Lancer le service** pour Workspace ONE.

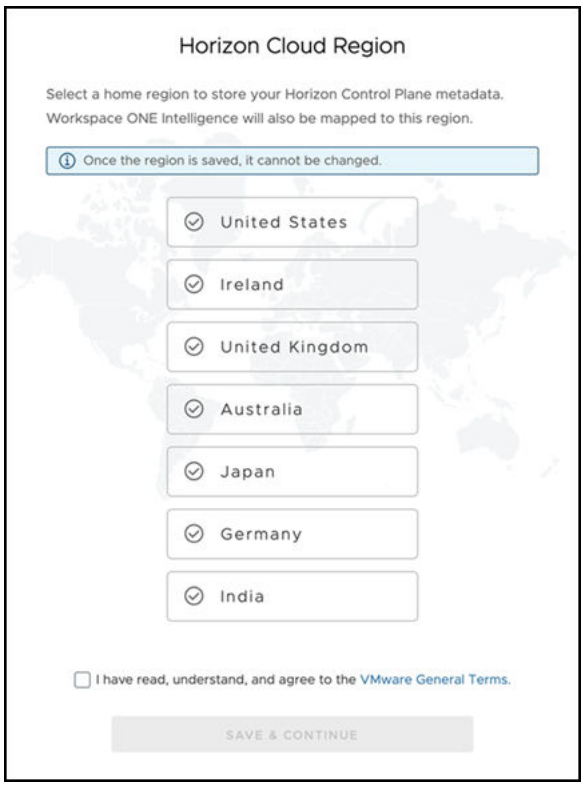


3 Cliquez sur **Gérer** sur la vignette **Horizon Cloud Service** pour lancer Horizon Universal Console.



Utiliser Horizon Universal Console pour sélectionner votre région Horizon Cloud

Après avoir lancé la console, vous êtes invité à sélectionner votre région. Pour respecter les principes d'intégrité des données, vous devez sélectionner la région dans laquelle résident vos ressources et leurs métadonnées. Une fois que vous avez sélectionné la région, vous ne pouvez plus la modifier.



1 Sélectionnez votre région Horizon Cloud.

2 Cochez la case pour accepter les conditions d'utilisation.

3 Cliquez sur **Enregistrer et continuer** pour accéder à la page Démarrage avec Horizon Universal Console.

Note À ce stade, Horizon Universal Console peut afficher une bannière en haut de l'écran indiquant que la synchronisation de la licence est en cours. Dans ce cas, la console n'affiche pas toutes les fonctionnalités activées par votre licence spécifique tant que la synchronisation n'est pas terminée et que vous n'avez pas actualisé votre navigateur. Une fois la synchronisation terminée, Horizon Universal Console affiche les éléments appropriés à votre licence.

Lisez les sections suivantes :

- Démarrage et déploiement d'Horizon Plus avec Horizon Cloud Service - next-gen
- Surveillance de la disponibilité de vos ressources Horizon Edge - Horizon Plus
- Configuration de la surveillance d'Horizon 8 Edge avec Splunk Enterprise

Démarrage et déploiement d'Horizon Plus avec Horizon Cloud Service - next-gen

Cette page de documentation décrit les étapes de workflow Horizon Universal Console **Ajouter un dispositif Horizon Edge** pour le cas d'utilisation dans lequel vous disposez de l'abonnement Horizon Plus, avez déjà terminé les étapes de connexion à Horizon Universal Console et de

sélection de votre région Horizon Cloud. Vous devez à présent connecter votre espace Horizon 8 au plan de contrôle Horizon Cloud Service - next-gen.

Introduction

Le déploiement d'un dispositif Horizon 8 Edge consiste à déployer un dispositif Passerelle Horizon Edge dans la plate-forme de virtualisation souhaitée, à coupler ce dispositif avec le plan de contrôle de nouvelle génération et à configurer les détails de l'instance d'Horizon Connection Server de l'espace Horizon 8 pour votre dispositif Horizon 8 Edge.

Note Intégrez chaque espace Horizon 8 comme dispositif Horizon Edge individuel.

Ce processus de bout en bout comporte plusieurs étapes.

1 Démarrez ce processus dans Horizon Universal Console.

2 À mi-parcours, déployez un dispositif OVA dans votre environnement vSphere (non fédéré). Vous devez utiliser les informations de code de couplage que le système crée dans la première partie du processus dans les champs de l'interface utilisateur Déployer le modèle OVF lorsque vous déployez le fichier OVA.

   Note Un déploiement d'OVA/OVF d'Passerelle Horizon Edge est uniquement disponible pour les fournisseurs Horizon 8 disposant d'une architecture intégrée à SDDC ou d'un type de capacité de centre de données privé. Pour les fournisseurs Horizon 8 disposant d'une architecture fédérée, reportez-vous à la procédure correspondant à votre type de capacité spécifique décrite dans la section Configuration des déploiements fédérés d'Horizon 8 avec Horizon Cloud Service - next-gen.

3 Ensuite, après la mise sous tension du dispositif, revenez à Horizon Universal Console pour vérifier que l'état du couplage est réussi et effectuez les étapes restantes dans cette console pour ajouter les détails de l'espace Horizon 8.

Avant de commencer

Consultez ces VMware Tech Zone videos :

VMware Tech Zone a créé quatre vidéos qui présentent les meilleures pratiques clés pour le déploiement d'un dispositif Horizon 8 Edge.

- Déploiement du dispositif Passerelle Horizon Edge - Configuration DNS sur https://via.vmw.com/tchzmno5209.
- Déploiement du dispositif Passerelle Horizon Edge - Vérificateur d'URL sur https://via.vmw.com/tchzmno5210.
- Déploiement du dispositif Passerelle Horizon Edge - Configuration du fournisseur et du dispositif sur https://via.vmw.com/tchzmno5211.
- Déploiement du dispositif Passerelle Horizon Edge à partir d'OVA sur https://via.vmw.com/tchzmno5212.

Les titres sont fournis ci-dessus pour faciliter la recherche des vidéos.

Vérifiez que vous ou votre équipe informatique avez terminé les éléments répertoriés suivants.

- Examinez la page Liste de vérification des conditions requises pour le déploiement d'un dispositif Horizon 8 Edge et assurez-vous que ces conditions requises sont remplies.
- Examinez les éléments préparatoires décrits sur les pages liées de la page Déploiements des dispositifs Horizon 8 Edge et vérifiez que ces éléments sont terminés.
- Déterminez le nom de domaine complet (FQDN) que vous utiliserez pour le dispositif Passerelle Horizon Edge déployé. L'assistant d'interface utilisateur vous demande d'entrer ce nom de domaine complet.
- Si l'instance d'Horizon Connection Server impliquée dans ce dispositif Horizon Edge dispose d'un certificat auto-signé, assurez-vous que vous connaissez l'empreinte digitale du certificat pour l'étape de vérification de l'assistant.

Démarrage de l'assistant Ajouter un dispositif Horizon Edge

Déployez un dispositif Horizon Edge à l'aide de l'assistant **Ajouter un dispositif Horizon Edge** de la console.

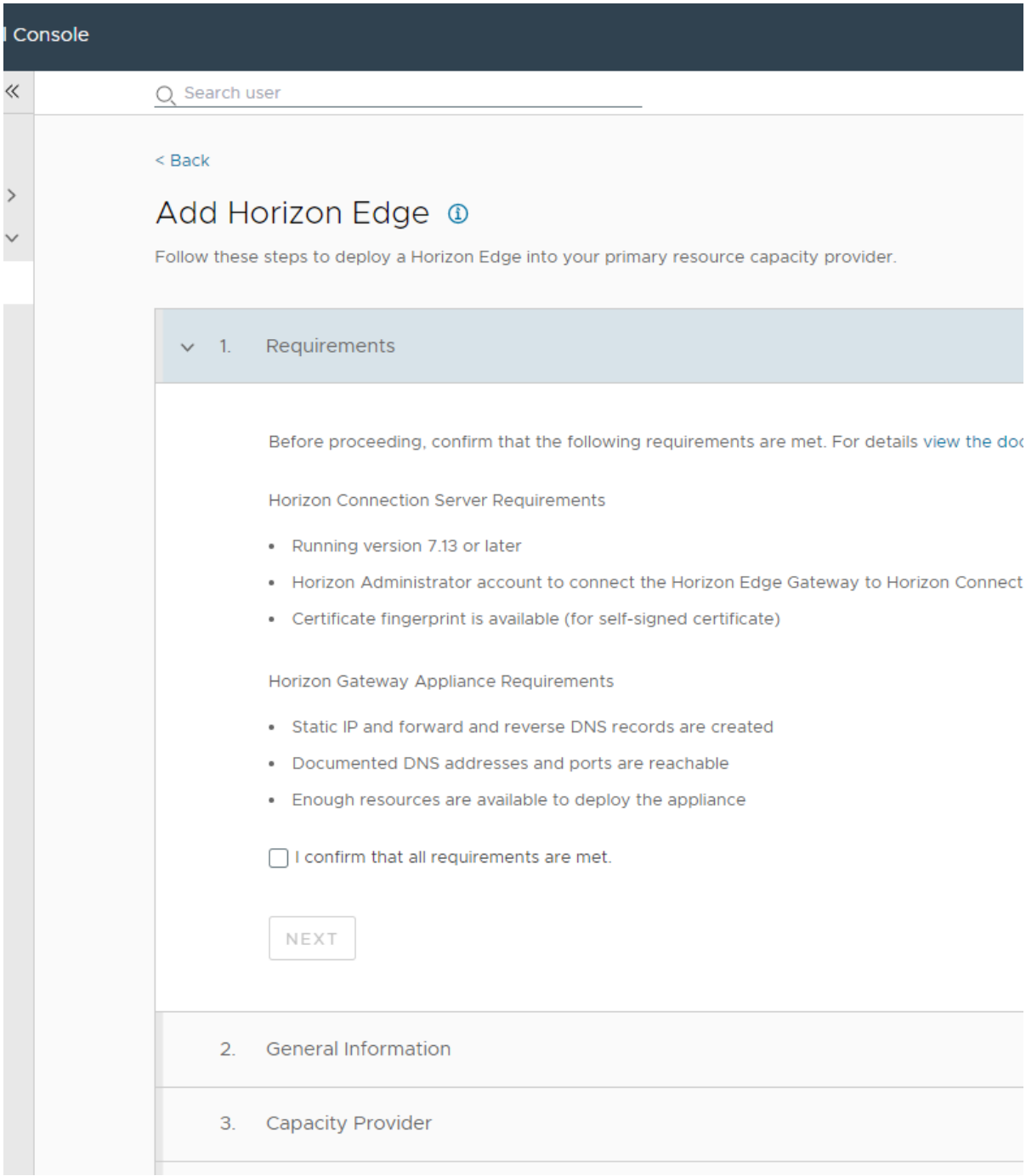
La console rend l'assistant **Ajouter un dispositif Horizon Edge** disponible à partir de différents points d'entrée. Votre point de départ dans la console pour cette étape varie généralement selon que votre environnement est vierge ou qu'il existe un dispositif Horizon Edge.

- Si vous venez de terminer immédiatement les étapes décrites sur la page Documentation d'Horizon Plus, il n'existe aucun dispositif Dispositifs Horizon Edge dans votre environnement et la console affiche son écran d'accueil. Dans ce cas, démarrez l'assistant **Ajouter un dispositif Horizon Edge** de la console en cliquant sur **Démarrer**.
- Si votre environnement dispose déjà d'au moins un dispositif Horizon Edge, la page Capacité contient une grille qui répertorie le dispositif Horizon Edge existant. Dans ce scénario, accédez à **Ressources > Capacité** et commencez à ajouter un autre dispositif Horizon Edge à partir de là.

Démarrage de l'assistant Ajouter un dispositif Horizon Edge

1 Démarrez l'assistant **Ajouter un dispositif Horizon Edge** de la console, à partir de l'écran d'accueil si votre environnement ne dispose d'aucun dispositif Horizon Edge ou sur la page Capacité si vous disposez d'un dispositif Horizon Edge existant.

   La console affiche son assistant **Ajouter un dispositif Horizon Edge** à partir de l'étape 1.



À ce stade, les étapes de l'assistant sont les mêmes que celles documentées à la page Déploiement d'un dispositif Horizon 8 Edge.

2 Effectuez les étapes en suivant la procédure décrite à la page Déploiement d'un dispositif Horizon 8 Edge.

Points importants lors du déploiement du fichier OVA dans votre environnement vSphere

Lorsque vous utilisez l'outil **Déployer le modèle OVF** pour déployer le fichier OVA dans votre environnement, gardez à l'esprit ces points importants. Ces éléments sont cruciaux à un déploiement de bout en bout réussi.

Note Un déploiement d'OVA/OVF d'Passerelle Horizon Edge est uniquement disponible pour les fournisseurs Horizon 8 disposant d'une architecture intégrée à SDDC ou d'un type de capacité de centre de données privé. Pour les fournisseurs Horizon 8 disposant d'une architecture fédérée, reportez-vous à la procédure correspondant à votre type de capacité spécifique décrite dans Configuration des déploiements fédérés d'Horizon 8 avec Horizon Cloud Service - next-gen.

Important

- À l'étape **Déployer et coupler la passerelle Horizon Edge**, un champ intitulé **Code de couplage** s'affiche. Ce code de couplage est crucial à la réussite du processus de bout en bout. Vous devez utiliser ce code de couplage dans l'interface utilisateur **Déployer le modèle OVF** lorsque vous déployez le dispositif dans votre environnement vSphere.
- Notez également que l'interface utilisateur **Déployer le modèle OVF** utilise une étiquette différente pour ce code (**Chaîne de connexion** dans l'interface utilisateur **Déployer le modèle OVF**).
- Lorsque vous copiez le code de couplage à partir de l'étape de l'assistant, vous devez utiliser l'icône de copie, car la console n'affiche pas la chaîne complète de code de couplage. La chaîne de code est plus longue que les éléments affichés par la console. Par conséquent, vous n'obtiendrez pas la chaîne de code complète en mettant uniquement le texte affiché en surbrillance et en le copiant.
- Dans l'étape **Personnaliser le modèle** de l'interface utilisateur **Déployer le modèle OVF**, dans le champ **Chaîne de connexion**, vous devez entrer la chaîne **Code de couplage** que vous avez copiée à l'étape précédente, à partir de l'assistant **Ajouter un dispositif Horizon Edge**.
- Même si au moment de la rédaction de ce document, le texte à l'écran indique que le champ **Chaîne de connexion** est facultatif, notez que la saisie du code de couplage est une étape cruciale à un déploiement réussi du dispositif Passerelle Horizon Edge.

Pour obtenir l'illustration pas à pas du déploiement du dispositif Passerelle Horizon Edge à l'aide de l'interface utilisateur **Déployer le modèle OVF**, reportez-vous à la Tech Zone video Déployer le dispositif Horizon Edge à partir d'OVA.

Pour obtenir des captures d'écran de l'interface utilisateur **Déployer le modèle OVF** qui illustrent ces points importants, reportez-vous à la page Déploiement d'un dispositif Horizon 8 Edge.

Résultats

En cas de réussite, la console ferme l'interface utilisateur de l'assistant et affiche la page de détails de ce dispositif Horizon Edge récemment ajouté.

Note En fonction du trafic réseau, le système peut prendre une minute pour terminer la mise à jour des indicateurs de l'état de la connectivité sur la page de détails.

Pour obtenir une illustration de la page de détails, reportez-vous à la page Détails du dispositif Horizon Edge ou en bas de la page Déploiement d'un dispositif Horizon 8 Edge.

Si vous souhaitez modifier ultérieurement les détails de ce dispositif Horizon Edge ou le supprimer, accédez à la page **Capacité**, sélectionnez le dispositif Horizon Edge dans la liste et utilisez l'action appropriée (**Modifier** ou **Supprimer**).

Surveillance de la disponibilité de vos ressources Horizon Edge - Horizon Plus

Si vous disposez d'une licence Horizon Plus, VMware® Horizon Availability Monitoring™ fournit un client que vous pouvez installer et utiliser pour tester la santé de vos ressources Horizon Edge. Ces tests peuvent vous aider à détecter et à résoudre rapidement les problèmes avant qu'ils ne s'aggravent. Par exemple, vous pouvez utiliser le client Horizon Availability Monitoring pour tester les connexions et effectuer d'autres actions, sur divers composants, tels que VMware Horizon® Connection Server™, votre annuaire Active Directory, les dispositifs de passerelle Horizon, les postes de travail et les applications publiées.

Après avoir configuré le client Horizon Availability Monitoring, vous pouvez utiliser Horizon Universal Console pour configurer des tests qui exécutent des contrôles de santé sur votre environnement Horizon Edge.

Note La fonctionnalité Horizon Availability Monitoring ne s'applique qu'aux dispositifs Dispositifs Horizon Edge qui résident dans votre locataire.

Les étapes générales du processus Horizon Availability Monitoring sont les suivantes.

1 Sélectionnez le type de client.

   - Sélectionnez le type de client **Installable** pour télécharger, installer et configurer le client Horizon Availability Monitoring sur votre propre système Windows, ce qui inclut le couplage du client avec Horizon Universal Console.
   - Sélectionnez le type de client **Cloud** pour configurer le client Horizon Availability Monitoring dans le cloud.

2 Utilisez Horizon Universal Console pour créer et exécuter l'un des types de tests suivants à partir du client Horizon Availability Monitoring.

Dans la liste suivante, chaque test nécessite progressivement un meilleur accès à votre environnement Horizon Edge, ce qui vous oblige à fournir une plus grande quantité d'informations liées à l'accès.

Attention Pour les tests en général, y compris les tests d'Horizon Availability Monitoring, il est recommandé d'utiliser un compte de test plutôt qu'un compte d'utilisateur normal lorsque vous êtes invité à fournir des informations d'identification (nom d'utilisateur et mot de passe).

Test de connectivité

Un résultat réussi s'ensuit lorsque le test de connectivité valide le chemin réseau entre le client et le dispositif Unified Access Gateway.

Le test de connectivité s'exécute du client Horizon Availability Monitoring vers le dispositif Unified Access Gateway.

La condition préalable à ce test est la suivante.

- Obtenez l'URL vers le dispositif Horizon Edge, qui constitue la cible du test de connectivité.

  Pour Horizon, il s'agit de l'URL d'Horizon Connection Server, qui est utilisée par Horizon Client.

Test d'authentification

Un résultat est réussi lorsque le test d'authentification confirme qu'une instance d'Horizon Connection Server est active en s'authentifiant sur Active Directory.

Le test d'authentification s'exécute depuis le client Horizon Availability Monitoring, vers le déploiement d'Horizon Edge, puis vers les dispositifs de passerelle Horizon (Unified Access Gateway et Passerelle Horizon Edge) et vers Horizon Connection Server.

Les conditions préalables à ce test sont les suivantes.

- Obtenez l'URL vers le dispositif Horizon Edge, qui constitue la cible du test de connectivité.

  Pour Horizon, il s'agit de l'URL d'Horizon Connection Server, qui est utilisée par Horizon Client.

- Obtenez les informations d'identification disponibles pour le compte de test que vous utiliserez pour ce test d'Horizon Availability Monitoring.

Test de lancement des ressources

Un résultat réussi s'ensuit lorsque le test de lancement des ressources initie un poste de travail ou une application de publication sélectionné.

Le test de lancement des ressources s'exécute à partir du client Horizon Availability Monitoring, via le déploiement d'Horizon Edge, jusqu'au poste de travail.

Les conditions préalables à ce test sont les suivantes.

- Obtenez l'URL vers le dispositif Horizon Edge, qui constitue la cible du test de connectivité.

  Pour Horizon, il s'agit de l'URL d'Horizon Connection Server, qui est utilisée par Horizon Client.
- Obtenez les informations d'identification disponibles pour le compte de test que vous utiliserez pour ce test d'Horizon Availability Monitoring.
- Disposez du nom du poste de travail ou de l'application publiée que vous souhaitez lancer dans le cadre du test.

Lancement simulé

Le lancement simulé utilise la passerelle Horizon Edge comme destination et simule un lancement de session sans consommer une application ou un poste de travail réel. Vous pouvez tester et surveiller le chemin de connexion du poste de travail avec un module d'agent simulé incorporé dans le déploiement du dispositif Edge.

Le lancement simulé valide le flux de connexion du poste de travail impliquant le client simulé, le service de connexion, UAG et le module Edge.

La condition préalable à ce test est la suivante :

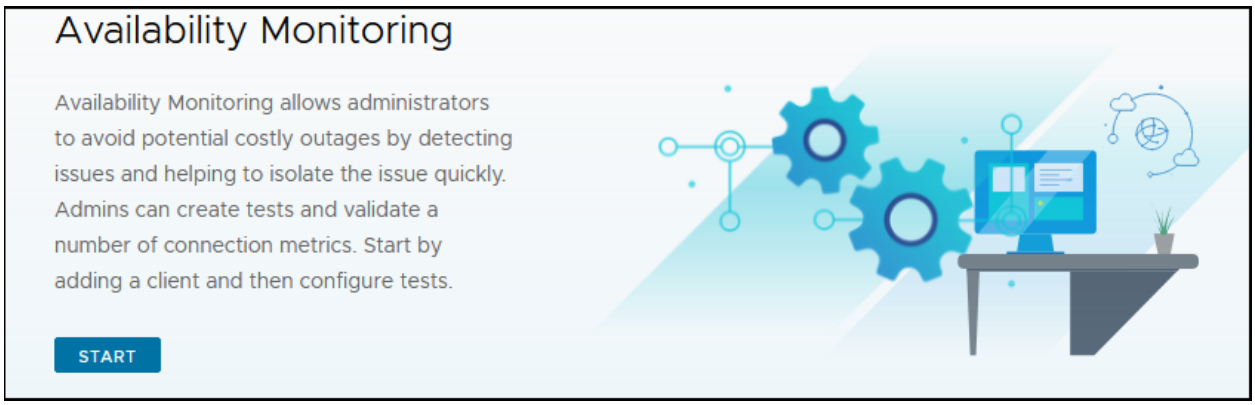
- Vous devez avoir déployé la capacité du dispositif Edge et UAG.

Configurer le test Horizon Availability Monitoring initial

Configurez les tests d'Horizon Availability Monitoring sur la page Horizon Availability Monitoring d'Horizon Universal Console. L'apparence de la page Horizon Availability Monitoring change après la première configuration. Cette rubrique décrit la configuration initiale du client Horizon Availability Monitoring jusqu'à la configuration du premier test. Pour les configurations suivantes, les étapes sont semblables, bien que l'apparence de l'interface diffère légèrement.

Note La fonctionnalité Horizon Availability Monitoring ne s'applique qu'aux dispositifs Dispositifs Horizon Edge qui résident dans votre locataire.

Pour accéder à la page Horizon Availability Monitoring, sélectionnez **Surveiller > Disponibilité**. Avant de configurer votre premier test d'Horizon Availability Monitoring, la page Surveillance de la disponibilité s'affiche comme suit.



La tâche suivante illustre les étapes requises pour configurer votre premier test, où la page Surveillance de la disponibilité ressemble à l'image précédente.

Conditions préalables

Disposez des informations requises pour le type de test que vous effectuerez. Reportez-vous à l'explication précédente des types de test **Connectivité**, **Authentification**, **Lancement des ressources** et **Lancement simulé**.

Procédure

1. À l'aide d'Horizon Universal Console, dans le menu de gauche, sélectionnez **Surveiller** > **Disponibilité**.
2. Cliquez sur **Démarrer**.

   L'assistant Horizon Availability Monitoring s'ouvre, en commençant par la première étape, qui consiste à ajouter le client Horizon Availability Monitoring.

   Pour la création initiale d'un test d'Horizon Availability Monitoring, créez un client et un test. Une fois l'assistant terminé, vous pouvez créer des clients et des tests supplémentaires.
3. Sélectionnez et configurez le type de client, soit le type de client **Installable**, soit le type de client **Cloud**.

   Type de client installable

   Client que vous devez télécharger et installer à un emplacement réseau sur un système Windows. Ce type de client est le choix optimal lorsque vous souhaitez simuler un test à partir du même emplacement réseau à partir duquel se trouvent les utilisateurs de poste de travail.

   Type de client cloud

Un client hébergé par VMware dans le cloud. Ce type de client est le choix optimal lorsque des utilisateurs accèdent au poste de travail depuis Internet. En tant qu'administrateur, vous n'avez pas besoin d'entretenir la machine qui héberge l'agent.

- Pour télécharger, installer et configurer le client Horizon Availability Monitoring sur un système Windows, procédez comme suit.
  a Pour l'option **Sélectionner un type**, sélectionnez **Installable**.
  b Cliquez sur **Télécharger** pour permettre à votre navigateur de télécharger le bundle client, qui est un module Windows Installer (fichier `.msi`).
  c Cliquez sur l'icône de copie en regard du code de couplage pour copier le code.
  d Déplacez le module Windows Installer vers un dossier du système Windows à partir duquel vous exécuterez le client Horizon Availability Monitoring.
  e Sur le système Windows, démarrez et terminez l'installation du module Windows Installer.
    - Si vous souhaitez un nom de client plus convivial, renommez le client.
    - Entrez le code de couplage dans la zone de texte appropriée lorsque vous y êtes invité.

      La page Démarrer la surveillance de la disponibilité affiche l'état mis à jour du processus de couplage, tel que Couplage terminé.

  f Cliquez sur **Suivant**.
- Pour configurer le client Horizon Availability Monitoring dans le cloud, procédez comme suit.
  a Pour l'option **Sélectionner un type**, sélectionnez **Cloud**.
  b Dans la zone de texte **Nom**, entrez un nom pour le client.
  c Dans le menu déroulant **Région**, sélectionnez une région.

    Le menu déroulant **Région** inclut toutes les régions disponibles de votre environnement.

4 Sélectionnez et enregistrez le type de test.

Reportez-vous aux explications précédentes des types de test **Connectivité**, **Authentification**, **Lancement des ressources** et **Lancement simulé**.

5 Fournissez les informations demandées et enregistrez le test.

La quantité d'informations que la page vous invite à fournir augmente pour chaque type de test que vous configurez du test **Connectivité** au test **Authentification**, puis au test **Lancement des ressources** et enfin au test **Lancement simulé**.

Invites applicables à tous les types de test	Description
Type	Sélectionnez le type de test à effectuer.
Nom	Créez un nom pour le test.
Client	Sélectionnez le client à partir duquel exécuter le test. Pour le test initial, ce client est celui que vous avez ajouté à la première étape de l'assistant Horizon Availability Monitoring. Lorsque vous créerez des clients à l'avenir, vous pourrez configurer ce test en remplaçant le client par un autre ou en ajoutant des clients. **Note** Plusieurs clients peuvent utiliser le même test.
Intervalle	Sélectionnez la fréquence d'exécution du test. Le test s'exécute en continu à l'intervalle que vous sélectionnez jusqu'à la modification de l'intervalle ou de la suppression du test.
URL	URL du dispositif Horizon Edge qui sert de cible de test.

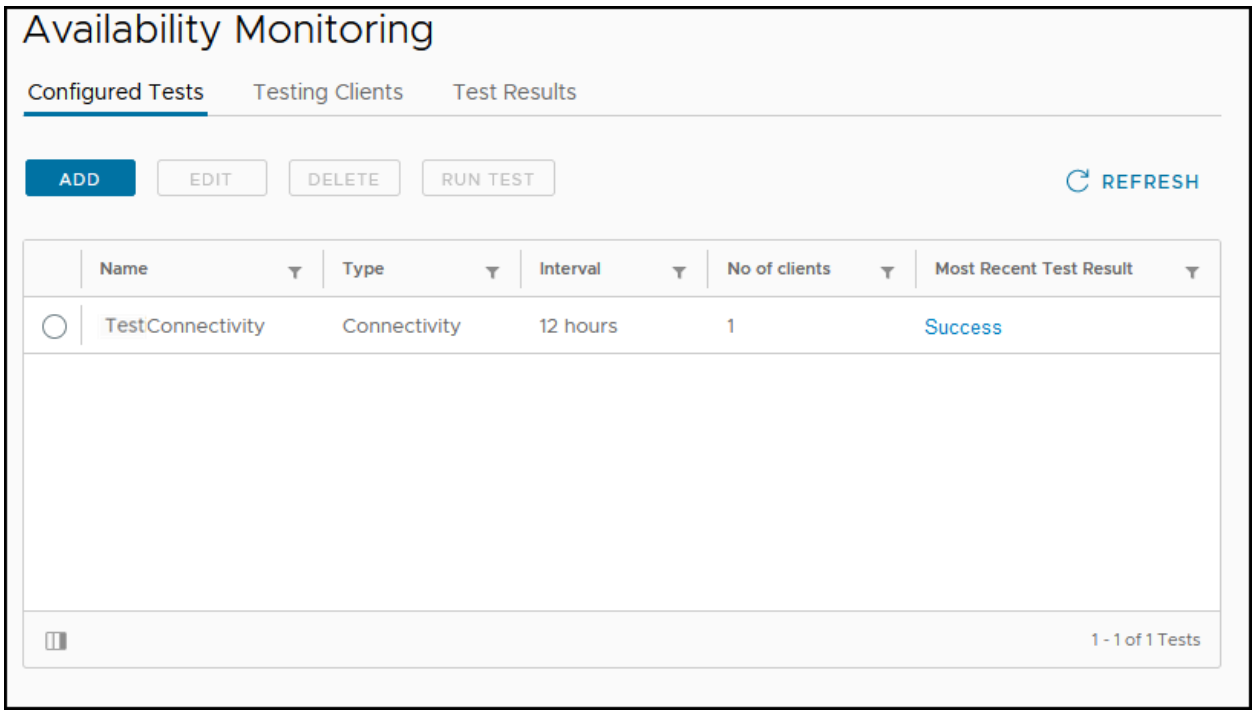
Invites supplémentaires applicables aux types de test d'authentification et de lancement des ressources	Description
Nom d'utilisateur	Entrez le nom d'utilisateur du compte de test pour ce test d'Horizon Availability Monitoring.
Mot de passe	Entrez le mot de passe du compte de test pour ce test d'Horizon Availability Monitoring.
Domaine (facultatif)	Domaine du dispositif Horizon Edge qui sert de cible de test.

Invite supplémentaire applicable au type de test de lancement des ressources	Description
Nom du pool	Fournissez le nom du poste de travail ou de l'application à lancer.

Invite supplémentaire applicable au type de test de lancement simulé	Description
Horizon Edge	Sélectionnez le dispositif Edge qui servira de destination pour le test HST.
Adresse d'Unified Access Gateway	L'adresse d'Unified Access Gateway.
Vérifier SSL	Activez ou désactivez **Vérifier SSL**. Lorsque cette option est activée, le test vérifie l'existence et l'authenticité d'un certificat d'identité de serveur.

Résultats

La page Surveillance de la disponibilité réapparaît avec une apparence mise à jour, présentant des informations sur vos tests, clients et résultats configurés. Ce sera l'apparence permanente de la page à l'avenir.



Actions d'Horizon Availability Monitoring que vous pouvez effectuer

Une fois que vous avez créé le test initial d'Horizon Availability Monitoring, vous pouvez effectuer plusieurs actions différentes sur la page Surveillance de la disponibilité qui vous permettent d'utiliser la fonctionnalité Horizon Availability Monitoring pour tester la santé de votre déploiement d'Horizon Edge.

Vous pouvez effectuer les actions suivantes, dont la plupart sont identiques ou semblables aux étapes de configuration du test initial d'Horizon Availability Monitoring. Reportez-vous à la section Configurer le test Horizon Availability Monitoring initial.

Note En cas d'échec d'un test d'Horizon Availability Monitoring, une notification s'affiche sur la page **Notifications**, accessible depuis l'icône en forme de cloche ( ) située dans le coin supérieur droit de n'importe quelle page.

Action	Description
Filtrer les informations sur la page Surveillance de la disponibilité.	Dans chaque onglet de la page Surveillance de la disponibilité, vous pouvez utiliser les filtres de colonne pour présenter les informations de la manière la plus adaptée à vos besoins.
Ajoutez, modifiez, supprimez ou exécutez des tests configurés.	Sélectionnez **Disponibilité > Tests configurés** pour effectuer l'une des actions suivantes. ■ Ajoutez un autre test d'Horizon Availability Monitoring. ■ Modifiez un test configuré existant, par exemple, pour ajouter ou modifier des clients ou pour modifier l'intervalle de test. Selon le type de test, vous pouvez également modifier les informations d'identification du compte de test ou modifier le nom du pool. ■ Supprimez un test configuré existant, par exemple, lorsque le test n'est plus utile. ■ Exécutez manuellement un test configuré existant, par exemple, lorsque vous souhaitez exécuter le test maintenant au lieu d'attendre la prochaine exécution planifiée du test.
Ajoutez, modifiez ou supprimez des clients de test.	Sélectionnez **Disponibilité > Test des clients** pour effectuer l'une des actions suivantes. ■ Ajoutez de nouveaux clients de test. Pour le type de client Installable, vous pouvez uniquement ajouter un nouveau client de test à un autre système Windows. **Note** Un seul client Horizon Availability Monitoring est pris en charge à la fois sur un système d'exploitation donné. ■ Modifiez un client de test existant. Pour le type de client Installable, vous pouvez installer un nouveau client et effectuer un nouveau couplage avec l'enregistrement du client d'origine si le système Windows qui héberge le client échoue et nécessite une réinstallation. ■ Supprimez un client de test existant, par exemple, lorsque le client n'est plus utile.
Afficher les résultats du test.	Sélectionnez **Disponibilité > Résultats du test** pour afficher une liste de résultats du test. La liste inclut 30 jours de résultats du test. Sur la page, vous pouvez afficher une liste de résultats du test, par exemple, vous pouvez afficher les tests qui ont réussi et ceux qui ont échoué, le cas échéant. Dépannez un test ayant échoué en tenant compte du type de test qui a échoué et de l'heure de l'échec. Pour plus d'informations, reportez-vous aux informations de type de test précédentes.

Configuration de la surveillance d'Horizon 8 Edge avec Splunk Enterprise

Si vous disposez d'une licence Horizon Plus, vous pouvez intégrer une configuration de Splunk Enterprise avec un ou plusieurs de vos dispositifs Horizon 8 Edge. Vous pouvez ensuite utiliser Splunk Enterprise pour surveiller vos dispositifs Horizon 8 Edge.

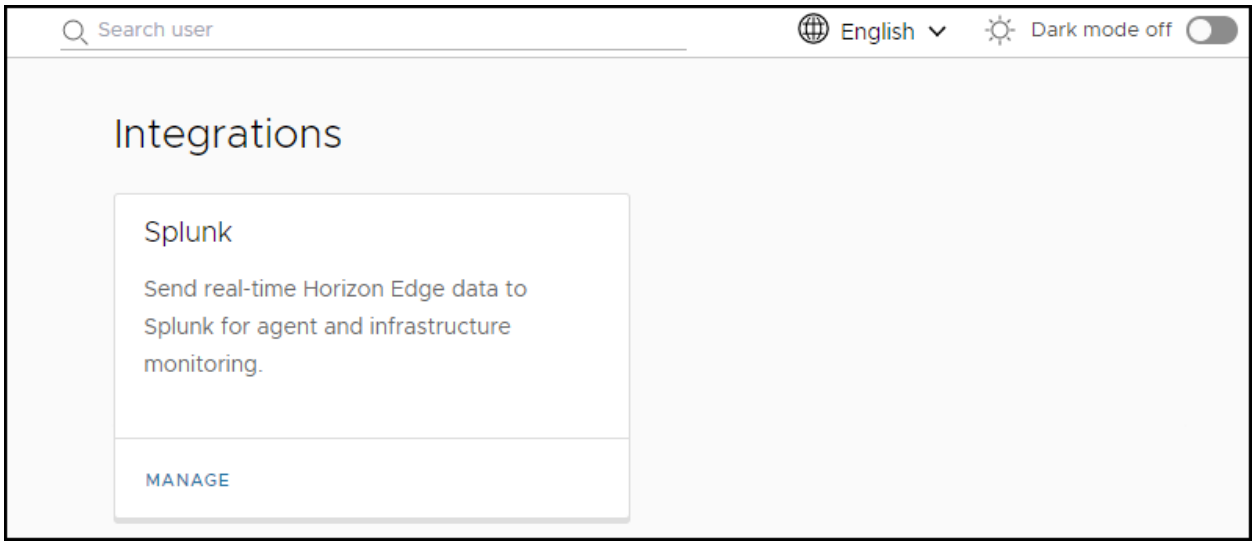
Attention Cette fonctionnalité Horizon Cloud Service - next-gen s'applique uniquement à la passerelle Horizon 8 Edge pour la licence Horizon Plus.

La licence Horizon Plus prend en charge l'option de surveillance de Splunk Enterprise des dispositifs Horizon 8 Edge au lieu de l'option de surveillance de Workspace ONE Intelligence.

Vous pouvez intégrer plusieurs instances de Splunk Enterprise à vos dispositifs Horizon 8 Edge, mais les instances de Splunk Enterprise n'ont pas besoin de communiquer entre elles. Chaque instance de Splunk Enterprise fonctionne comme un Hub, tandis que les dispositifs Horizon 8 Edge de cette analogie fonctionnent en tant que spokes.

Par conséquent, plusieurs dispositifs Horizon 8 Edge peuvent être attribués à une seule instance de Splunk Enterprise, ce qui permet d'envoyer des données à cette instance de Splunk. La communication entre Dispositifs Horizon Edge et l'instance de Splunk Enterprise est unidirectionnelle entre les dispositifs Horizon 8 Edge et l'instance de Splunk Enterprise.

Pour utiliser Horizon Universal Console afin d'ajouter, d'attribuer ou de supprimer une configuration de Splunk Enterprise, accédez à la page Splunk en cliquant sur **Intégrations** dans la barre de navigation, puis sur **Gérer** dans la vignette d'intégrations **Splunk**.



Ajouter la configuration d'une instance de Splunk Enterprise

Vous pouvez utiliser Horizon Universal Console pour ajouter une configuration de Splunk.

Conditions préalables

Préparez les informations suivantes de l'instance de Splunk Enterprise avec laquelle vous souhaitez intégrer vos Dispositifs Horizon Edge.

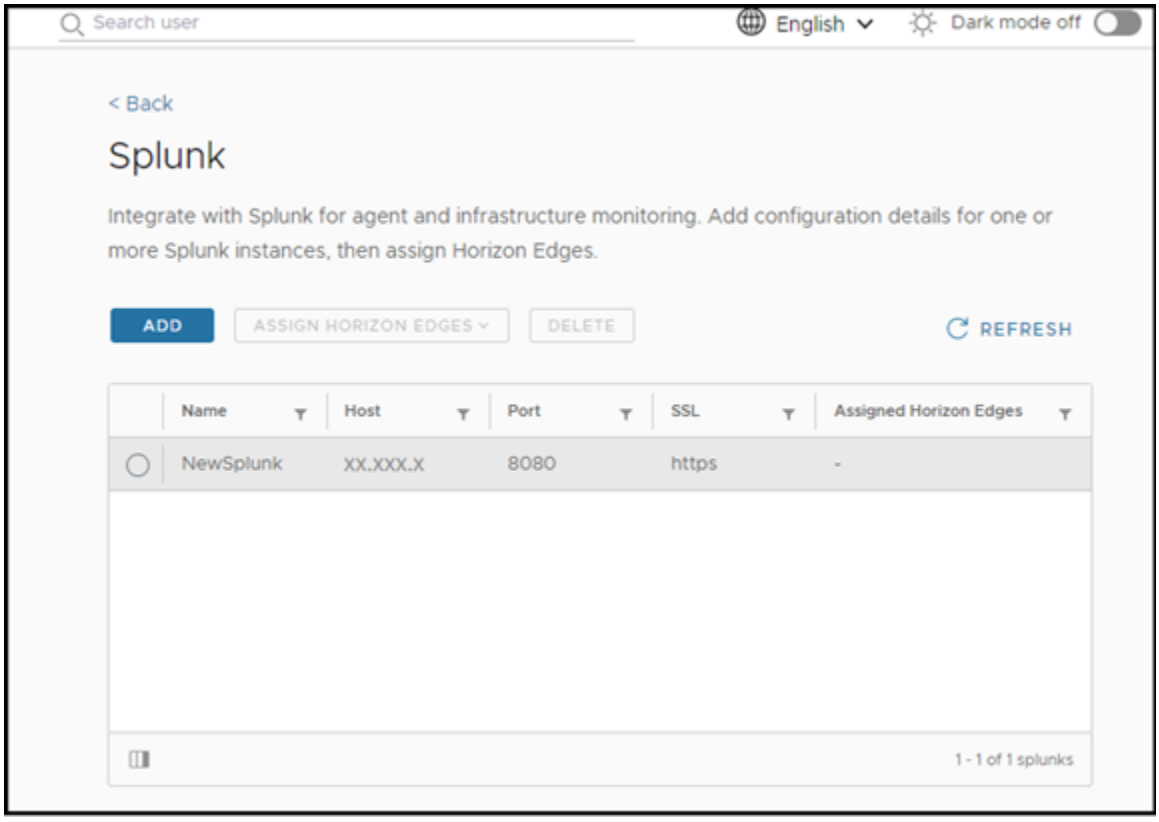
- Adresse IP de votre hôte Splunk Enterprise.
- Numéro de port de votre instance de Splunk Enterprise.
- Jeton secret de votre instance de Splunk Enterprise.

  Vous pouvez copier ce jeton à partir de votre instance de Splunk Enterprise lorsque vous êtes prêt pour l'intégration.
- Bien qu'il ne soit pas recommandé d'utiliser un certificat auto-signé, faites en sorte qu'il soit disponible pour le chargement si vous décidez finalement de l'utiliser comme certificat auto-signé

Procédure

1 Cliquez sur **Gérer** dans la vignette d'intégrations Splunk.

  La page Splunk s'ouvre.



2 Pour ajouter des informations de configuration pour une instance existante de Splunk Enterprise, cliquez sur **Ajouter**.

3 Entrez les informations que vous avez collectées comme condition préalable à cette tâche, puis cliquez sur **Enregistrer**.

Attribuer une instance d'Horizon Edge à une configuration de Splunk Enterprise

Après avoir utilisé Horizon Universal Console pour ajouter une ou plusieurs configurations de Splunk Enterprise, procédez comme suit pour attribuer un dispositif Horizon Edge à une configuration de Splunk Enterprise.

Procédure

1. Sur la page Splunk, sélectionnez une configuration de Splunk Enterprise.
2. Sélectionnez **Attribuer des dispositifs Horizon Edge > Ajouter**.
3. Sélectionnez un ou plusieurs dispositifs Dispositifs Horizon Edge à attribuer à la configuration de Splunk, puis cliquez sur **Ajouter**.

Résultats

Les dispositifs Dispositifs Horizon Edge attribués sont désormais intégrés à Splunk. Vous pouvez utiliser Splunk pour surveiller les dispositifs Dispositifs Horizon Edge attribués.

Vous trouverez plusieurs détails identiques sur la page de résumé du dispositif Horizon Edge attribué.

Annuler l'attribution d'un dispositif Horizon Edge d'une configuration de Splunk Enterprise

Une fois que vous avez attribué un dispositif Horizon Edge à une configuration de Splunk Enterprise, vous pouvez à tout moment annuler l'attribution de ce dispositif Horizon Edge.

Procédure

1. Sur la page Splunk, sélectionnez une configuration de Splunk Enterprise.
2. Sélectionnez **Attribuer des dispositifs Horizon Edge > Supprimer**.
3. Sélectionnez un ou plusieurs dispositifs Dispositifs Horizon Edge pour lesquels vous souhaitez annuler l'attribution de la configuration de Splunk, puis cliquez sur **Supprimer**.

Modifier une configuration de Splunk Enterprise

Vous pouvez modifier les informations de configuration de votre instance de Splunk Enterprise, telles que le jeton secret de votre instance de Splunk Enterprise, le certificat SSL et l'adresse IP de l'hôte.

Après avoir modifié une configuration de Splunk Enterprise attribuée à un ou plusieurs dispositifs Dispositifs Horizon Edge, la configuration est mise à jour vers ces dispositifs Dispositifs Horizon Edge attribués, ainsi que vers la base de données.

Lorsque vous modifiez une configuration de Splunk Enterprise qui n'est attribuée à aucun dispositif Horizon Edge, la configuration de Splunk Enterprise est mise à jour uniquement vers la base de données.

Conditions préalables

Préparez les informations que vous souhaitez modifier, à savoir :

- Nouvelle adresse IP de votre hôte Splunk Enterprise.
- Nouveau numéro de port de votre instance de Splunk Enterprise.
- Nouveau jeton secret de votre instance de Splunk Enterprise.
- Emplacement sur votre hôte d'un nouveau certificat auto-signé.

Procédure

1. Sur la page **Intégrations > Splunk**, sélectionnez une configuration de Splunk Enterprise à modifier.
2. Cliquez sur **Modifier**.
3. Modifiez les informations de configuration à mettre à jour et cliquez sur **Enregistrer**.

Supprimer une configuration de Splunk Enterprise

Après avoir annulé l'attribution de tous les dispositifs Dispositifs Horizon Edge d'une configuration de Splunk Enterprise, vous pouvez supprimer cette dernière.

Procédure

1. Sur la page Splunk, sélectionnez la configuration de Splunk Enterprise à supprimer.
2. Cliquez sur **Supprimer**.

   La boîte de dialogue Confirmer la suppression s'affiche.
3. Cliquez sur **Supprimer**.