Notes de mise à jour de VMware Horizon 7 version 7.12

Publié le 17 mars 2020

Ces notes de mise à jour comprennent les rubriques suivantes :

Nouveautés de cette version

La version 7.12 de VMware Horizon 7 apporte les nouvelles fonctionnalités et améliorations suivantes. Ces informations sont regroupées par composant installable.

Pour plus d'informations sur les problèmes résolus dans cette version, reportez-vous à la section Problèmes résolus.

Améliorations du produit

La version 7.12 de VMware Horizon 7 inclut de nombreuses nouvelles fonctionnalités et améliorations apportées à l'Horizon Connection Server et à Horizon Agent, notamment le développement de la parité des fonctionnalités d'Horizon Console, la console Web basée sur HTML5 qui remplacera à terme Horizon Administrator, qui sera obsolète début 2020.

Horizon Connection Server sur site

- **Horizon Console (interface Web basée sur HTML5)**
  Horizon Console comporte plusieurs améliorations. Celles-ci incluent :
  - Vous pouvez configurer l'authentification à deux facteurs pour un utilisateur final après l'expiration d'une session. Reportez-vous à la rubrique Paramètres généraux pour les sessions client dans Horizon Console dans le document *Administration de VMware Horizon Console*.
  - Vous pouvez cliquer sur n'importe quel lien dans Horizon Console pour ouvrir Horizon

Console dans un autre onglet du navigateur Web. Reportez-vous à la rubrique Connexion à Horizon Console dans le document *Administration de VMware Horizon Console*.
    - Pour chaque Serveur de connexion, vous pouvez afficher le nombre de sessions de protocole de passerelle et de non-passerelle dans le tableau de bord d'Horizon Console. Reportez-vous à la rubrique Surveiller l'état de charge d'Horizon Connection Server dans le document *Administration de VMware Horizon Console*.
    - Le tableau de bord d'Horizon Console inclut des détails de résumé pour les statistiques de tableau de bord. Reportez-vous à la rubrique Surveiller les composants d'Horizon 7 dans le document *Administration de VMware Horizon Console*.
    - Vous pouvez afficher le nombre total d'utilisateurs autorisés qui utilisent une application publiée. Reportez-vous à la rubrique Création d'un pool d'applications dans Horizon Console dans le document *Administration de VMware Horizon Console*.
    - Vous pouvez attribuer plusieurs utilisateurs à chaque machine dans un pool de postes de travail avec une attribution d'utilisateur dédiée. Cela s'applique aux pools automatisés qui contiennent des machines virtuelles complètes, des pools de postes de travail manuels et des pools de postes de travail Instant Clone. Reportez-vous au document *Configuration de postes de travail virtuels dans Horizon Console*.
    - Vous pouvez afficher le nom d'hôte de la machine attribuée à la place du nom d'affichage du pool de postes de travail lorsque vous vous connectez à Horizon Client. Cela s'applique à tous les types de pools de postes de travail et aux droits globaux. Reportez-vous au document *Configuration de postes de travail virtuels dans Horizon Console*.
- Architecture Cloud Pod
    - Vous pouvez afficher des informations sur toutes les sessions Architecture Cloud dans le volet Sessions Architecture Cloud Pod du tableau de bord d'Horizon Console. Reportez-vous à la rubrique Affichage des sessions de poste de travail et d'application dans Horizon Console.
    - Lorsque vous créez une autorisation globale de poste de travail, vous pouvez sélectionner **Afficher le nom de la machine attribuée** pour afficher le nom d'hôte de la machine attribuée plutôt que le nom du droit global dans Horizon Client. Reportez-vous à la rubrique Feuille de calcul pour la configuration d'un droit d'accès global.
    - Lorsque vous utilisez les commandes lmvutil --createGlobalEntitlement et --updateGlobalEntitlement, vous pouvez spécifier l'option --displayAssignedHostName pour afficher le nom d'hôte de la machine attribuée plutôt que le nom du droit global dans Horizon Client. Lorsque vous utilisez la commande lmvutil --updateGlobalEntitlement, vous pouvez utiliser l'option --disableDisplayAssignedHostName pour spécifier que le nom d'hôte de la machine attribuée ne s'affiche pas dans Horizon Client. Reportez-vous aux sections Création d'un droit global et Modification d'un droit global.
    - La ligne de commande pour sauvegarder LDAP global à l'aide de vdmexport.exe est modifiée pour prendre en charge plus d'options. Les scripts existants continueront à fonctionner sans modification. Reportez-vous à la rubrique Exporter des données de configuration LDAP.
- Applications et postes de travail publiés
    - En activant l'option Prélancement, vous pouvez lancer une session d'application dans un pool de postes de travail avant qu'un utilisateur ouvre l'application dans Horizon Client. Reportez-vous à la rubrique Feuille de calcul pour la création manuelle d'un pool d'applications.
- Postes de travail virtuels
    - L'adresse MAC est conservée lors d'une resynchronisation ou d'une actualisation d'un pool de postes de travail Instant Clone flottant pendant le provisionnement initial. Reportez-vous à la rubrique Feuille de calcul pour créer un pool de postes de travail Instant Clone dans Horizon Console. L'adresse MAC est également conservée lors d'une resynchronisation ou d'une actualisation des batteries de serveurs RDSH.
    - Prise en charge de SDDC à hôte unique sur VMware Cloud on AWS. Reportez-vous à Création de pools de postes de travail sur un SDDC à hôte unique.
    - Prise en charge de vmCrypt et d'Instant Clone avec vSphere 7.0
- Horizon Help Desk Tool
    - Dans Horizon Help Desk Tool, vous pouvez rechercher un processus de session ou une application par son nom en entrant le nom du processus de session ou de l'application dans la zone de texte du filtre de recherche. Reportez-vous à la rubrique Processus de session pour Horizon Help Desk Tool ou Statut de l'application pour Horizon Help Desk Tool.

- **Système d'exploitation pris en charge**
  - Prise en charge des PC physiques pour Windows 1903 et version ultérieure.

Horizon Agent for Linux

- **Nouvelles distributions prises en charge**
  Horizon Agent for Linux prend désormais en charge les systèmes d'exploitation suivants pour les postes de travail à distance Linux. Pour plus d'informations, reportez-vous à la rubrique Configuration système requise pour Horizon 7 for Linux.
  - RHEL 8.1
  - CentOS 8.1
- **Collaboration de session sur KDE**
  La collaboration de session est désormais prise en charge sur les postes de travail RHEL 7.5 utilisant l'environnement de poste de travail KDE. Pour plus d'informations, reportez-vous à la rubrique Fonctionnalités des postes de travail Horizon Linux.

Horizon Agent

- **Expérience à distance**
  - La fonctionnalité VMware Integrated Printing fonctionne désormais avec Horizon Client pour Chrome et HTML Access. Reportez-vous à la rubrique Configuration de VMware Integrated Printing.
  - Avec la fonctionnalité VMware Integrated Printing, vous ne pouvez plus définir le type de support sur une imprimante UPD. Pour modifier le type de support sur une imprimante UPD, activez le paramètre de la stratégie de groupe **Désactiver la persistance de propriété de l'imprimante** et remplacez le paramètre de type de support de l'imprimante cliente par le paramètre souhaité. Reportez-vous à la rubrique Configuration de VMware Integrated Printing.
  - Vous pouvez utiliser la stratégie de groupe **Nom de l'imprimante pour les agents RDSH** pour configurer les noms des imprimantes clientes qui sont redirigées vers des postes de travail publiés et des applications publiées avec la fonctionnalité VMware Integrated Printing. Reportez-vous à la section Paramètres de stratégie de VMware Integrated Printing.
  - La fonctionnalité de redirection de contenu URL fonctionne désormais avec Horizon Client 5.4 for Linux ou version ultérieure. Pour utiliser la fonctionnalité de redirection de contenu URL sur un client Linux, vous devez utiliser un navigateur Firefox avec l'extension de redirection d'URL VMware Horizon installée et activée. Reportez-vous à la rubrique Configuration requise pour la redirection de contenu URL.
  - Vous pouvez configurer les applications prises en charge par la fonctionnalité de redirection de contenu URL sous Windows pour le protocole dans l'URL. Reportez-vous au paramètre de la stratégie de groupe **Configuration de la liste blanche pour la redirection d'URL** dans Paramètres de la stratégie de groupe de redirection de contenu URL.
  - L'utilisation du GPU est réduite pour les pools avec NVidia GPU.

Horizon GPO Bundle

- Le fichier modèle ADMX pour la configuration de VMware View Agent, vdm_agent.admx, contient les nouveaux paramètres suivants :
  - Délai d'expiration de la session de préchauffage
- Le fichier modèle ADMX pour la configuration de VMware Horizon Client, vdm_client.admx, contient les nouveaux paramètres suivants :
  - Utiliser l'instance de client existante lors de la connexion au même serveur
- Le fichier modèle ADMX de VMware Blast, vdm_blast.admx, contient les nouveaux paramètres suivants :
  - Haute précision couleur HEVC
  - Le paramètre UDP Protocol prend effet lors de l'ouverture/fermeture de session, alors qu'un redémarrage était nécessaire auparavant.
- Le fichier modèle ADMX de VMware Integrated Printing, printerRedirection.admx, contient les

nouveaux paramètres suivants :
    - Désactiver la redirection de l'imprimante pour le client externe au bureau
    - Nom de l'imprimante pour les agents RDSH
- Le fichier modèle ADMX de redirection du contenu URL, urlRedirection.admx, contient les nouveaux paramètres suivants :
    - Configuration de la liste blanche pour la redirection d'URL

Horizon Client

Pour plus d'informations sur les nouvelles fonctionnalités d'Horizon Client 5.4, notamment HTML Access 5.4, consultez les notes de mise à jour sur la page Documentation d'Horizon Client.

Horizon 7 Cloud Connector

Applicable aux clients disposant d'une licence universelle VMware Horizon. Le dispositif virtuel Horizon Cloud Connector est un composant requis pour Horizon 7 version 7.6 et versions ultérieures, afin de prendre en charge la gestion d'espaces Horizon 7 à l'aide d'Horizon Cloud Service.

Horizon 7 déployé sur VMware Cloud on AWS

Pour obtenir une liste des fonctionnalités d'Horizon 7 prises en charge sur VMware Cloud on AWS, reportez-vous à l'article 58539 de la base de connaissances de VMware.

Avant de commencer

- Note importante sur l'installation de VMware View Composer
  Si vous prévoyez d'installer View Composer 7.2 ou version ultérieure ou d'effectuer une mise à niveau vers celui-ci, vous devez mettre à niveau Microsoft .NET Framework vers la version 4.6.1. Dans le cas contraire, l'installation échouera.
- Note importante sur l'installation de VMware Tools
  Si vous prévoyez d'installer une version de VMware Tools téléchargée depuis le site de téléchargement de VMware, plutôt que la version par défaut fournie avec vSphere, vérifiez que la version de VMware Tools est prise en charge. Pour déterminer les versions de VMware Tools prises en charge, accédez à la Matrice d'interopérabilité des produits VMware, sélectionnez la solution **VMware Horizon View** et la version, puis sélectionnez **VMware Tools (downloadable only)**.
- Si vous souhaitez installer View Composer de façon silencieuse, consultez l'article 2148204 de la base de connaissances de VMware Microsoft Windows Installer Command-Line Options for Horizon Composer (Options de la ligne de commande du programme d'installation Microsoft Windows pour Horizon Composer).
- La version d'Horizon 7 inclut de nouvelles exigences de configuration qui diffèrent de celles de certaines versions antérieures. Consultez le document *Mises à niveau d'Horizon 7* pour obtenir des instructions de mise à niveau.
- Si vous envisagez de mettre à niveau une version d'Horizon 7 antérieure à la version 6.2, et si le Serveur de connexion, le serveur de sécurité ou le serveur View Composer utilise le certificat auto-signé qui a été installé par défaut, vous devez supprimer le certificat auto-signé existant avant d'effectuer la mise à niveau. Il est possible que les connexions ne fonctionnent pas si vous conservez les certificats auto-signés existants. Lors d'une mise à niveau, le programme d'installation ne remplace pas les certificats existants. La suppression de l'ancien certificat auto-signé garantit l'installation d'un nouveau certificat. Le certificat auto-signé dans cette version a une clé RSA plus longue (2 048 bits au lieu de 1 024) et une signature plus forte (SHA-256 avec RSA au lieu de SHA-1 avec RSA) que dans les versions antérieures à la version 6.2. Notez que les certificats auto-signés ne sont pas sûrs et qu'ils doivent être remplacés par des certificats signés par une autorité de certification dès que possible, et que les certificats SHA-1 ne sont plus considérés comme sûrs et qu'ils doivent être remplacés par des certificats SHA-2.
  Ne supprimez pas les certificats signés par une autorité de certification qui ont été installés pour une utilisation en production, comme le recommande VMware. Les certificats signés par une autorité de

certification continuent à fonctionner après la mise à niveau vers cette version.

- Une fois que vous avez effectué une nouvelle installation ou une mise à niveau de toutes les instances du Serveur de connexion vers Horizon 7 version 7.2 ou ultérieure, vous ne pouvez pas rétrograder les instances du Serveur de connexion vers une version antérieure à Horizon 7 version 7.2, car les clés utilisées pour protéger les données LDAP ont été modifiées. Pour conserver la possibilité de rétrograder des instances du Serveur de connexion lors de la planification d'une mise à niveau vers Horizon 7 version 7.2 ou ultérieure, vous devez effectuer une sauvegarde LDAP avant de commencer la mise à niveau. Si vous avez besoin de rétrograder les instances du Serveur de connexion, vous devez rétrograder toutes les instances du Serveur de connexion, puis appliquer la sauvegarde LDAP au dernier Serveur de connexion rétrogradé.
- La sélection de l'option de configuration de la redirection de scanner avec l'installation d'Horizon Agent peut affecter de façon significative le taux de consolidation de l'hôte. Pour garantir la consolidation d'hôte optimale, assurez-vous que l'option de configuration Redirection de scanner est uniquement sélectionnée pour les utilisateurs qui en ont besoin. (par défaut, l'option Redirection de scanner n'est pas sélectionnée lorsque vous installez Horizon Agent). Pour les utilisateurs ayant besoin de la fonctionnalité Redirection de scanner, configurez un pool de postes de travail distinct et sélectionnez l'option de configuration uniquement dans ce pool.
- Horizon 7 utilise uniquement TLSv1.1 et TLSv1.2. En mode FIPS, il utilise uniquement TLSv1.2. Vous risquez de ne pas pouvoir vous connecter à vSphere si vous n'appliquez pas les correctifs vSphere. Pour plus d'informations sur la réactivation de TLSv1.0, consultez les sections Activer TLSv1 sur des connexions vCenter depuis le Serveur de connexion et Activer TLSv1 sur des connexions vCenter et ESXi depuis View Composer dans le document *Mises à niveau d'Horizon 7*.
- Le mode FIPS n'est pas pris en charge sur les versions antérieures à la version 6.2. Si vous activez le mode FIPS dans Windows et que vous mettez à niveau Horizon Composer ou Horizon Agent à partir d'une version antérieure à Horizon View 6.2 vers Horizon 7 version 7.2 ou ultérieure, l'option du mode FIPS n'est pas affichée. Vous devez effectuer une nouvelle installation au lieu d'installer Horizon 7 version 7.2 ou ultérieure en mode FIPS.
- Les postes de travail Linux utilisent le port 22443 pour le protocole d'affichage VMware Blast.
- À partir d'Horizon 7 version 7.2, il est possible que l'ordre des suites de chiffrement soit appliqué par le Serveur de connexion. Pour plus d'informations, consultez le document *Sécurité d'Horizon 7*.
- À partir d'Horizon 7 version 7.2, le Serveur de connexion doit être capable de communiquer sur le port 32111 avec d'autres Serveurs de connexion dans le même espace. Si ce trafic est bloqué lors de l'installation ou de la mise à niveau, l'installation échouera.
- À partir d'Horizon 7 version 7.3.2, les négociations TLS sur le port 443 doivent s'effectuer dans les 10 secondes, ou dans les 100 secondes si l'authentification par carte à puce est activée. Dans les versions précédentes d'Horizon 7, les connexions TLS sur le port 443 avaient 100 secondes pour se terminer dans toutes les situations. Vous pouvez ajuster la durée des négociations TLS sur le port 443 en définissant la propriété de configuration `handshakeLifetime`. Éventuellement, le client responsable d'une négociation TLS qui dépasse la durée peut être automatiquement ajouté à une liste noire. Les nouvelles connexions des clients sur liste noire sont retardées d'une période configurable avant d'être traitées, de sorte que les connexions des autres clients soient prioritaires. Vous pouvez activer cette fonctionnalité en définissant la propriété de configuration `secureHandshakeDelay`. Pour plus d'informations sur la configuration des propriétés de configuration, consultez le document *Sécurité d'Horizon 7*.
- Lorsque le rôle Services Bureau à distance n'est pas présent, le programme d'installation d'Horizon Agent vous invite à installer Horizon Agent en mode RDS ou bureau.

Internationalisation

L'interface utilisateur d'Horizon Administrator et d'Horizon Console, l'aide en ligne d'Horizon Administrator et d'Horizon Console et la documentation du produit Horizon 7 sont disponibles en français, allemand, espagnol, japonais, chinois simplifié, chinois traditionnel et coréen. Pour la documentation, reportez-vous au Centre de documentation de VMware Horizon 7.

Notes de compatibilité

- Pour connaître les systèmes d'exploitation invités pris en charge par Horizon Agent sur des machines mono-utilisateur et des hôtes RDS, consultez l'article 2150295 de la base de connaissances de VMware Supported Windows Versions for Remote Desktop Systems for Horizon Agent (Versions prises en charge de Windows pour les systèmes de postes de travail distants pour Horizon Agent).
- Si vous utilisez des serveurs Horizon 7 avec une version de View Agent antérieure à 6.2, vous devrez activer TLSv1.0 pour les connexions PCoIP. Les versions de View Agent antérieures à 6.2 ne prennent en charge le protocole de sécurité TLSv1.0 que pour PCoIP. TLSv1.0 est désactivé par défaut sur les serveurs Horizon 7, y compris les serveurs de connexion et les serveurs de sécurité. Vous pouvez activer TLSv1.0 pour les connexions PCoIP sur ces serveurs en suivant les instructions de l'article 2130798 de la base de connaissances de VMware Configure security protocols for PCoIP for Horizon 6 version 6.2 and later, and Horizon Client 3.5 and later (Configurer des protocoles de sécurité pour PCoIP pour Horizon 6 version 6.2 et ultérieures, et Horizon Client 3.5 et versions ultérieures).
- Pour les systèmes d'exploitation invités Linux pris en charge pour Horizon Agent, consultez la section Configuration système requise pour Horizon 7 for Linux dans le document *Configuration de postes de travail Horizon 7 for Linux*.
- Pour connaître les systèmes d'exploitation pris en charge par le Serveur de connexion, le serveur de sécurité et View Composer, consultez Configuration système requise pour les composants de serveur dans le document *Installation d'Horizon 7*.
- La fonctionnalité d'Horizon 7 est améliorée par un ensemble mis à jour de systèmes Horizon Client fournis avec cette version. Par exemple, Horizon Client 4.0 ou version ultérieure est requis pour les connexions VMware Blast Extreme. Reportez-vous à la page Documentation des clients VMware Horizon Client pour obtenir des informations sur les clients Horizon Client pris en charge.
- La fonctionnalité d'Instant Clones requiert vSphere 6.0 Update 1 ou version ultérieure.
- Windows 7 et Windows 10 sont pris en charge pour les Instant Clones, mais pas Windows 8 ou Windows 8.1.
- Pour en savoir plus sur la compatibilité d'Horizon 7 avec les versions actuelles et précédentes de vSphere, consultez la Matrice d'interopérabilité des produits VMware.
- Pour les niveaux fonctionnels du domaine AD DS (Active Directory Domain Services) pris en charge, reportez-vous à Préparation d'Active Directory dans le document *Installation d'Horizon 7*.
- Pour connaître les autres exigences système, par exemple les navigateurs pris en charge par Horizon Administrator, consultez le document *Installation d'Horizon 7*.
- RC4, SSLv3 et TLSv1.0 sont désactivés par défaut dans les composants Horizon 7, conformément au RFC 7465 « Prohibiting RC4 Cipher Suites », au RFC 7568 « Deprecating Secure Sockets Layer Version 3.0 », à PCI-DSS 3.1 « Payment Card Industry (PCI) Data Security Standard » et à SP800-52r1 « Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations ». Pour réactiver RC4, SSLv3 ou TLSv1.0 sur un Serveur de connexion, un serveur de sécurité, View Composer ou une machine Horizon Agent, consultez Protocoles et chiffrements antérieurs désactivés dans View dans le document *Sécurité d'Horizon 7*.
- Si une passerelle sécurisée PCoIP (PSG, PCoIP Secure Gateway) a été déployée pour des connexions PCoIP, le microprogramme du client zéro doit être de version 4.0 ou ultérieure.
- Lorsque vous utilisez la redirection de lecteur client (CDR), déployez Horizon Client 3.5 ou version ultérieure et View Agent 6.2 ou version ultérieure pour vous assurer que les données de CDR sont envoyées sur un canal virtuel crypté depuis un périphérique client externe vers le serveur de sécurité PCoIP et depuis le serveur de sécurité vers le poste de travail distant. Si vous déployez des versions antérieures d'Horizon Client ou d'Horizon Agent, les connexions externes vers le serveur de sécurité PCoIP sont chiffrées mais, dans le réseau d'entreprise, les données sont envoyées depuis le serveur de sécurité vers le poste de travail distant sans chiffrement. Vous pouvez désactiver la CDR en configurant un paramètre de stratégie de groupe Services Bureau à distance Microsoft dans Active Directory. Pour plus de détails, consultez la section Gestion de l'accès à la redirection du lecteur client dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.
- L'option de configuration de la redirection USB dans le programme d'installation d'Horizon Agent est désactivée par défaut. Vous devez sélectionner cette option pour installer la fonctionnalité de redirection USB. Pour obtenir des instructions sur l'utilisation de la redirection USB en toute sécurité, consultez Déploiement de périphériques USB dans un environnement View sécurisé dans

le document *Sécurité d'Horizon 7*.

- La stratégie globale, Redirection multimédia (MMR), est définie par défaut sur **Refuser**. Pour utiliser MMR, vous devez ouvrir Horizon Administrator, modifier les stratégies globales, puis définir explicitement cette valeur sur **Autoriser**. Pour contrôler l'accès à MMR, vous pouvez activer ou désactiver la stratégie Redirection multimédia (MMR) globalement ou pour un pool ou un utilisateur individuel. Les données de redirection multimédia (MMR) sont envoyées sur le réseau sans cryptage basé sur une application et peuvent contenir des données sensibles, selon le contenu redirigé. Pour garantir que les données ne puissent pas être surveillées sur le réseau, utilisez MMR uniquement sur un réseau sécurisé.
- Avant de définir le niveau de partage de page transparente (TPS, Transparent Page Sharing) dans Horizon Administrator, VMware recommande de bien comprendre les implications sur la sécurité. Pour obtenir des instructions, consultez l'article 2080735 de la base de connaissances de VMware Security considerations and disallowing inter-Virtual Machine Transparent Page Sharing (Aspects de sécurité et désactivation du partage de page transparente entre machines virtuelles).
- Pour permettre l'utilisation de View Storage Accelerator dans un environnement vSphere 5.5 ou version ultérieure, la taille d'une machine virtuelle de poste de travail doit être de 512 Go au maximum. View Storage Accelerator est désactivé sur les machines virtuelles d'une taille supérieure à 512 Go. La taille d'une machine virtuelle est définie par la capacité VMDK totale. Par exemple, un fichier VMDK peut avoir une taille de 512 Go ou un ensemble de fichiers VMDK peut avoir une taille totale de 512 Go. Cette exigence s'applique également aux machines virtuelles qui ont été créées dans une version antérieure de vSphere et mises à niveau vers vSphere 5.5.
- Horizon 7 ne prend pas en charge vSphere Flash Read Cache (anciennement vFlash).
- Dans Horizon (avec View) version 6.0 et versions ultérieures, les applets de commande View PowerCLI Get-TerminalServer, Add-TerminalServerPool et Update-TerminalServerPool sont obsolètes.
- Le DMA d'écran est désactivé par défaut dans les machines virtuelles qui sont créées dans vSphere 6.0 et versions ultérieures. View requiert que le DMA d'écran soit activé. Si le DMA d'écran est désactivé, les utilisateurs voient un écran noir lorsqu'ils se connectent au poste de travail distant. Lorsqu'Horizon 7 provisionne un pool de postes de travail, il active automatiquement le DMA d'écran pour toutes les machines virtuelles gérées par vCenter Server dans le pool. Toutefois, si Horizon Agent est installé dans une machine virtuelle en mode non géré (VDM_VC_MANAGED_AGENT=0), le DMA d'écran n'est pas activé. Pour plus d'informations sur l'activation manuelle du DMA d'écran, consultez l'article 2144475 de la base de connaissances de VMware Manually enabling screen DMA in a virtual machine (Activation manuelle du DMA d'écran dans une machine virtuelle).
- Les pools de postes de travail d'Instant Clone avec vGPU activé sont pris en charge pour vSphere 2016 et versions ultérieures.
- Microsoft Windows Server requiert qu'une plage de ports dynamique soit ouverte entre tous les Serveurs de connexion dans l'environnement Horizon 7. Ces ports sont requis par Microsoft Windows pour le fonctionnement normal de l'appel de procédure distante (RPC) et la réplication Active Directory. Pour plus d'informations sur la plage de ports dynamique, consultez la documentation de Microsoft Windows Server.
- Dans Horizon 7 version 7.2 ou ultérieure, l'outil viewDBChk n'a pas d'accès aux informations d'identification de vCenter ou de View Composer et il demande ces informations au besoin.
- Les règles de transfert pour les demandes HTTP reçues par les instances du Serveur de connexion et les serveurs de sécurité ont été modifiés dans cette version. Si vous avez défini des entrées `frontMapping` personnalisées dans `locked.properties`, vous devez les supprimer avant la mise à niveau. Si vous souhaitez interdire les connexions administrateur à certaines instances du Serveur de connexion, au lieu de définir des entrées `frontMapping` personnalisées, ajoutez cette entrée à `locked.properties` :

  ```
  frontServiceWhitelist =
  tunnel|ajp:broker|ajp:portal|ajp:misc|moved:*|file:docroot
  ```

  Sur les serveurs de sécurité, cette entrée est appliquée automatiquement et ne doit pas être définie dans `locked.properties`.
- Horizon Persona Management n'est pas compatible avec les volumes accessibles en écriture utilisateur créés avec le modèle UIA + Profil.

- Dans Horizon 7 version 7.0.3 ou ultérieure, les vérifications de validation internes déterminent si l'Instant Clone et le modèle interne disposent d'adresses IP valides et d'une connexion réseau. Si une machine virtuelle dispose d'une carte réseau à laquelle il n'est pas possible d'attribuer une adresse IP lors du provisionnement, le provisionnement d'Instant Clone échoue.
- Pour plus d'informations sur les modèles de cartes GPU NVIDIA prises en charge par Horizon 7, consultez la page suivante : https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html.
- Les cartes graphiques AMD v340 sont prises en charge.
- L'Audio/Vidéo en temps réel (RTAV) est pris en charge dans un environnement IPv6.
- Reportez-vous à la Matrice d'interopérabilité des produits VMware pour plus d'informations sur la compatibilité d'Horizon 7 avec les dernières versions de VMware Unified Access Gateway, VMware Identity Manager, VMware App Volumes, VMware Dynamic Environment Manager et VMware Tools.
- JMP Server prend en charge VMware App Volumes 2.14 ou version ultérieure, mais pas App Volumes 4.0. Pour utiliser JMP Server, vous devez installer App Volumes 2.xx, version 2.14 ou ultérieure.
- PCoIP n'est pas pris en charge avec les pools Instant Clone RDSH dans un environnement IPv6. PCoIP est pris en charge avec des postes de travail distants dans un environnement IPv6.
- À partir de la version 18.2.7, Avi Networks (VMware NSX Advanced Load Balancer) prend en charge l'équilibrage de charge pour le Serveur de connexion, les dispositifs Unified Access Gateway et App Volumes Manager.
- Les connexions par authentification unique réelle et SSO basées sur des cartes à puce ne sont pas prises en charge avec Horizon sous Windows 10 2004.

Systèmes d'exploitation Windows 10 pris en charge

Pour obtenir une liste à jour des systèmes d'exploitation Windows 10 pris en charge, consultez l'article 2149393 de la base de connaissances de VMware, Supported Versions of Windows 10 on Horizon 7 (Versions prises en charge de Windows 10 sous Horizon 7).
Pour plus d'informations sur les exigences relatives aux mises à niveau pour les systèmes d'exploitation Windows 10, consultez l'article 2148176 de la base de connaissances de VMware Upgrade Requirements for Windows 10 Operating Systems (Exigences relatives aux mises à niveau pour les systèmes d'exploitation Windows 10) ici.

Prise en charge de Red Hat Enterprise Linux Workstation

Horizon Agent for Linux prend en charge l'installation sur les systèmes exécutant Red Hat Enterprise Linux Workstation. Red Hat Enterprise Linux Server n'est pas pris en charge.

Dans le document Configuration des postes de travail Horizon 7 for Linux, toutes les occurrences de « Red Hat Enterprise Linux » et de « RHEL » font référence à Red Hat Enterprise Linux Workstation uniquement.

Pour obtenir la liste des versions de Red Hat Enterprise Linux Workstation prise en charge, reportez-vous à la section Configuration système requise pour Horizon 7 for Linux.

Versions antérieures d'Horizon 7

Les fonctionnalités introduites dans les versions antérieures sont décrites dans les notes de mise à jour de chaque version, avec les problèmes connus.

Problèmes résolus

Le nombre fourni avant chaque problème résolu fait référence au système de suivi des problèmes internes VMware.

- Dans Horizon Administrator, les boutons Fermer la session et Déconnecter la session ne sont pas désactivés pour les sessions distantes démarrées depuis vCenter Server.
- Dans Horizon Console, lorsque vous créez un pool de postes de travail manuel, le champ Délai d'expiration de session vide (applications seulement) n'est pas mis à jour lorsque l'option Type de session est « Application » ou « Poste de travail et Application ».
- Horizon Console ne reflète pas le nouveau nom du groupe de ports ou du segment lorsque vous sélectionnez des réseaux pour un pool de postes de travail Instant Clone ou une batterie de serveurs lorsque le nom du segment est modifié dans la console VMware Cloud on AWS.
- 2467168 : la synchronisation de Persona ne s'est pas terminée à la fermeture de session.
- 2485807 : la synchronisation de Persona est bloquée lors de la tentative de création du snapshot.
- 2487211 : fuite de mémoire du pilote de Persona VMWVvpfsd.sys.
- 2490882 : échec du pilote de Persona avec le contrôle de bogue C1F5 lorsque les fichiers Common Log File System (CLFS) sont endommagés.
- 2487199 : échec de Persona si vous modifiez les informations de fichier dans un état de mémoire faible.

Problèmes connus

Les problèmes connus à ce jour sont regroupés comme suit.

- Horizon Persona Management
- View Composer
- Horizon Connection Server
- Horizon Agent for Linux
- Horizon Agent
- Horizon GPO Bundle
- Horizon Client
- Horizon JMP Server et JMP Integrated Workflow
- Horizon Cloud Connector

Horizon Persona Management

- Après chaque connexion, la gestion de persona met du temps pour répliquer le premier persona d'utilisateur sur un système d'exploitation invité qui utilise la version v6 du profil d'utilisateur.
- Lorsque vous ouvrez une session sur une machine Windows 10 LTSB à l'aide d'un profil de persona et que vous essayez d'accéder à des dossiers redirigés à partir d'Accès rapide, tels que Téléchargements ou Mes Documents, vous recevez cette erreur :

  C:\Users\vdiuser7\Downloads n'est pas disponible. Microsoft ne fournit pas l'API pour ajouter un dossier ou un fichier à Accès rapide.
  Solution : Aucun

- Lorsque vous vous connectez pour la deuxième fois à une machine virtuelle configurée avec Persona Management, le navigateur Microsoft Edge se bloque et un message d'erreur indiquant que l'application OneDrive n'a jamais été utilisée s'affiche. En outre, les fichiers et dossiers ne peuvent pas être répliqués correctement. Ce problème se produit avec Windows 10 build 1703 et versions ultérieures.
  Solution : désactivez le paramètre **Déplacer des dossiers de paramètres locaux** de Persona Management. Lorsque vous désactivez ce paramètre, le navigateur Microsoft Edge fonctionne correctement, mais l'application OneDrive est disponible uniquement lorsque vous vous connectez pour la première fois.

- Les icônes hors ligne ne sont pas affichées pour les fichiers sur une machine virtuelle Windows Server 2012 avec le paramètre Horizon Persona Management activé.
  Solution : aucune connue.

- Après une connexion initiale réussie à une machine virtuelle sur laquelle Horizon Agent est installé sur un système Windows 10 version 1703 CBB et où Gestion de persona est activée, le message d'erreur « OneDrive -Image incorrecte » s'affiche lors des tentatives de connexion suivantes.

  Solution : n'utilisez pas OneDrive sur votre système Windows 10 version 1703 CBB. Dans l'éditeur de gestion de stratégie de groupe, désactivez le paramètre « Déplacer des dossiers de paramètres locaux » dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Configuration de VMware View Agent > Gestion de persona > Itinérance et synchronisation**.

- Le menu Démarrer ne fonctionne pas sur les machines Windows 10 2004 64 bits et 32 bits lorsque Persona est installé.

  Solution : pour plus d'informations, reportez-vous à l'article 78047 de la base de connaissances.

View Composer

- Lorsque vous exécutez le programme d'installation de View Composer sur Windows Server 2016 avec la dernière mise à jour de Windows à partir de la ligne de commande, vous obtenez une erreur Microsoft
  .NET 4.6 framework. Ce problème se produit, car le programme d'installation de l'interface de ligne de commande ne parvient pas à reconnaître la dernière version de Microsoft .NET 4.7.
  Solution : utilisez l'interface utilisateur du programme d'installation de View Composer pour exécuter le programme d'installation.

- La création ou la recomposition de pools de postes de travail échoue après la mise à niveau de la machine virtuelle parente du build 1511 vers le build 1607 du système d'exploitation Windows 10. Le build 1607 est le système d'exploitation Windows 10 Anniversary Update.
  Solution :
  - Option 1. Effectuez une nouvelle installation de Windows 10 Build 1607 sur la machine virtuelle parente.
  - Option 2. Ne sélectionnez pas « Rediriger les fichiers supprimables » dans l'assistant de création de pool de postes de travail.
- La connexion à View Composer échoue lorsque vous exécutez la commande suivante : viewdbchk.cmd – findMachine
  Solution : importez le certificat auto-signé pour View Composer dans le magasin de clés du Serveur de connexion ou utilisez un certificat d'autorité de certification personnalisé.

- En raison de modifications récentes apportées à l'utilitaire de personnalisation d'invité sur vSphere 6.7, pendant une mise à niveau d'Horizon 7 vers la version 7.5, vous ne pouvez pas utiliser View Composer 7.5 avec une version antérieure d'Horizon Agent pour le provisionnement et la recomposition de pools de clone lié à l'aide de la méthode de personnalisation Sysprep. Les batteries de serveurs et les postes de travail de clone lié restent bloqués indéfiniment dans l'état de personnalisation lors des opérations de provisionnement ou de recomposition.
  Solution : mettez à niveau vers la dernière version de VMware Tools, mettez à niveau Horizon Agent vers la version 7.5 sur la machine virtuelle parente et prenez un snapshot de la machine virtuelle parente mise à niveau. Ensuite, provisionnez ou recomposez des pools de postes de travail de clone lié à l'aide de la méthode de personnalisation Sysprep sur vSphere 6.7.

- Les clones liés se bloquent à l'état de personnalisation dans les versions Standard et Datacenter de Win2k12.
  Solution : pour plus d'informations sur la résolution de ce problème, consultez l'article 57348 de la base de connaissances de VMware : https://kb.vmware.com/s/article/57348.

Horizon Connection Server

- Lors du provisionnement d'un pool de postes de travail d'Instant Clone, si l'espace sur les banques de données n'est pas suffisant, le message d'erreur qui s'affiche dans Horizon Administrator est « Le clonage de la VM <nom de VM> a échoué - VC_FAULT_FATAL : échec d'étendue du fichier d'échange de 0 Ko à 2097152 Ko ». Ce message n'indique pas clairement la cause principale du problème.
  Solution : augmentez suffisamment l'espace disponible dans la banque de données.
- Dans Horizon Administrator, si vous accédez à **Catalogue** > **Pools de postes de travail**, que vous double-cliquez dans un pool de postes de travail d'Instant Clone, que Vous accédez à l'onglet **Inventaire** et que vous cliquez sur **Machines (détails d'Instant Clone)**, la fenêtre affiche des détails sur les Instant Clones. Toutefois, la colonne Banque de données de disque de système d'exploitation n'affiche aucune information.
  Solution : Aucun
- Dans un environnement à grande échelle, certains postes de travail dans un pool de postes de travail d'Instant Clone peuvent passer dans l'état IP non valide.
  Solution : dans Horizon Administrator, accédez à **Inventaire de pool**, sélectionnez les postes de travail dans l'état **IP non valide** et cliquez sur **Récupérer**.
- Lorsque vous redémarrez ou réinitialisez une machine virtuelle pour laquelle une session d'utilisateur final existe dans un pool de postes de travail à partir de vCenter Server ou à partir du menu Système d'exploitation Windows, la machine virtuelle redémarre, mais l'état de la machine virtuelle peut être « Déjà utilisé » dans Horizon Administrator.
  Ce problème peut se produire pour les types de pool suivants :
  - Pools de postes de travail d'Instant Clone.
  - Pools de postes de travail flottants de clone lié avec « Supprimer à la fermeture de session » activé.
  - Pools de postes de travail flottants de clone lié avec « Actualiser à la fermeture de session » activé.
  - Pools de postes de travail flottants de clone complet avec « Supprimer à la fermeture de session » activé.

  Solution : utilisez Horizon Administrator ou Horizon Client pour redémarrer ou réinitialiser la machine virtuelle dans le pool de postes de travail d'Instant Clone. Si la machine virtuelle est déjà dans l'état « Déjà utilisé », supprimez-la. Cette action crée automatiquement une machine virtuelle en fonction des paramètres de provisionnement du pool.
- Si vous provisionnez des Instant Clones sur des banques de données locales, les hôtes correspondants ne peuvent pas passer en mode de maintenance. Cela se produit, car les VM internes et les Instant Clones sont stockés sur des banques de données locales ce qui empêche leur migration.
  Solution : supprimez le pool de postes de travail d'Instant Clone. Cela supprime les VM associées et permet aux hôtes correspondants de passer en mode maintenance.

- La correction des hôtes ESXi qui utilisent VUM échoue si la VM parente d'Instant Clone est présente sur l'hôte dans un état sous tension.
  Solution : pour plus d'informations, consultez l'article 2144808 de la base de connaissances de VMware Entering and exiting maintenance mode for an ESXi host that has Horizon instant clones (Entrée et sortie du mode de maintenance pour un hôte ESXi disposant de Horizon Instant Clones).

- Les applications de plate-forme Windows universelle (UWP) ne sont pas prises en charge en tant qu'applications publiées sur les hôtes Windows Server 2016 et Windows Server 2019 RDS.

- Pour l'authentification unique réelle, l'état de la connectivité entre l'instance du Serveur de connexion et le serveur d'inscription ne s'affiche que sur le tableau de bord État de santé du système pour le serveur de connexion que vous utilisez pour accéder à Horizon Administrator. Par exemple, si vous utilisez `https://server1.example.com/admin` pour Horizon Administrator, l'état de la connectivité avec le serveur d'inscription est collecté uniquement pour le serveur de connexion `server1.example.com`. Vous pouvez voir un ou les deux messages suivants :
  - `Le serveur d'inscription principal ne peut pas être contacté pour gérer des sessions sur ce serveur de connexion.`
  - `Le serveur d'inscription secondaire ne peut pas être contacté pour gérer des sessions sur ce serveur de connexion.`

Il est obligatoire de configurer un serveur d'inscription principal. La configuration d'un serveur d'inscription secondaire est facultative. Si vous ne disposez que d'un seul serveur d'inscription, vous ne verrez que le premier message (sur l'erreur). Si vous disposez d'un serveur d'inscription principal et d'un secondaire et que les deux présentent des problèmes de connectivité, vous verrez les deux messages.

- Lorsque vous configurez l'authentification unique réelle dans un environnement avec des autorités de certification (CA) et des sous-autorités de certification (SubCA) avec des modèles différents configurés sur chacune d'elles, vous êtes autorisé à configurer l'authentification unique réelle avec une combinaison de modèles d'une CA ou d'une SubCA avec une autre CA ou SubCA. Ainsi, le tableau de bord peut afficher l'état de l'authentification unique réelle avec la couleur verte. Toutefois, il échoue lorsque vous essayez d'utiliser l'authentification unique réelle.

- Dans Horizon Help Desk Tool, le nom d'espace n'apparaît pas si la session est une session locale ou une session exécutée dans l'espace local.
  Solution : configurez l'environnement Architecture Cloud Pod pour afficher les noms d'espace dans Horizon Help Desk Tool.

- Le réglage du mode Workspace ONE n'est pas répercuté dans le serveur réplica à partir de Workspace ONE.
  Solution : configurez le mode Workspace ONE dans le Serveur de connexion.

- Lorsque vous créez des pools de postes de travail de clone complet, il arrive parfois que des modèles incorrects s'affichent et que des modèles valides soient masqués à cause d'un problème de cache.
  Solution : redémarrez le Serveur de connexion.
- Lorsque vous essayez d'ajouter un authentificateur SAML dans Horizon Administrator, le bouton **Ajouter** est désactivé sur la page Gérer les authentificateurs SAML.
  Solution : connectez-vous à Horizon Administrator en tant qu'utilisateur avec le rôle Administrateurs ou Administrateurs locaux.
- Dans un environnement Architecture Cloud Pod, les sessions d'application prélancées à partir de droits d'application globaux ne sont pas affichées dans **Inventaire > Sessions de recherche** dans Horizon Administrator.
  Solution : connectez-vous à l'interface utilisateur d'Horizon Administrator pour une instance du Serveur de connexion dans l'espace d'hébergement et sélectionnez **Contrôle > Événements** pour afficher les informations des sessions prélancées.

- Pour Intel vDGA, seules les séries Haswell et Broadwell des GPU intégrés Intel sont prises en charge. Les GPU intégrés Broadwell sont pris en charge uniquement sur vSphere 6 Update 1b et versions ultérieures. Les GPU intégrés Haswell sont pris en charge sur vSphere 5.5 et versions ultérieures. Le GPU doit être activé dans le BIOS avant de pouvoir être reconnu par ESXi. Pour plus d'informations, consultez la documentation de votre hôte ESXi. Intel recommande de laisser les paramètres de mémoire graphique dans le BIOS sur leurs valeurs par défaut. Si vous choisissez de modifier les paramètres, gardez le paramètre d'ouverture sur sa valeur par défaut (256 M).
- Le provisionnement de machines virtuelles basées sur des pools de postes de travail View Composer configurés pour utiliser NVIDIA GRID vGPU échoue avec l'erreur suivante : La quantité de ressources graphiques disponibles dans le pool de ressources parent est insuffisante pour l'opération.
  Solution : utilisez un seul profil vGPU pour tous les postes de travail virtuels configurés pour le rendu 3D dans un cluster.

- Pour vCenter Server 6.0 U3 ou version ultérieure, notamment vCenter Server 6.5, les machines virtuelles parentes internes migrent vers un autre hôte pendant une panne. Cette migration entraîne un problème, car des machines virtuelles parentes inutiles résident sur l'hôte de destination.
  Solution : supprimez manuellement ces machines virtuelles parentes. Pour plus d'informations, consultez le document *Configuration de postes de travail virtuels dans Horizon 7*.

- Pour réduire le risque d'insuffisance de mémoire, les profils vGPU avec 512 Mo ou moins de tampon de trame ne prennent en charge qu'un seul affichage virtuel sur un système d'exploitation invité Windows 10.

  Les profils de vGPU suivants disposent de 512 Mo ou moins de tampon de trame :

  - Tesla M6-0B, M6-0Q
  - Tesla M10-0B, M10-0Q
  - Tesla M60-0B, M60-0Q
  - GRID K100, K120Q
  - GRID K200, K220Q

  Solution : utilisez un profil qui prend en charge plusieurs affichages virtuels et qui dispose d'au moins 1 Go de tampon de trame.

- Le lancement des postes de travail publiés et des pools d'applications échoue si la fonctionnalité de restriction client est activée et si vous êtes autorisé à accéder à un domaine configuré avec une approbation AD unidirectionnelle.
  Solution : Aucun

- Après une mise à niveau, l'option pour ajouter une batterie de serveurs est grisée si vous disposez d'un rôle avec « Gérer des batteries de serveurs et des pools de postes de travail et d'applications » (privilège spécifique de l'objet).
  Solution : modifiez le rôle ou recréez-le avec le privilège « Gérer des batteries de serveurs et des pools de postes de travail et d'applications », ce qui ajoute également le privilège « Gérer la configuration et les stratégies générales ».

- Après une mise à niveau, les signets n'apparaissent pas dans Workspace ONE.
  Solution : ajoutez de nouveau les signets depuis le catalogue dans Workspace ONE.

- Lorsque vous déconnectez et reconnectez le câble réseau, puis cliquez sur « Se déconnecter et fermer la session » sur la machine cliente, le poste de travail distant ne se déconnecte pas et ne ferme pas la session.

  Solution : fermez manuellement la fenêtre du poste de travail distant et déconnectez-vous de la session distante.

- Dans Horizon Administrator, l'étape « Prêt à terminer » n'affiche pas les valeurs de nombreux champs pendant le processus de clonage d'un pool automatisé contenant des machines virtuelles complètes. Cependant, l'opération de clonage réussit.
  Solution : aucune.

- Lorsque vous créez des clones liés et des clones complets avec la méthode de personnalisation SysPrep, la personnalisation et la jonction de domaine échouent parfois sur des systèmes d'exploitation invités Windows 10.
  Solution : cela se produit en raison d'un problème de Microsoft Windows. Pour résoudre ce problème, suivez les étapes décrites dans l'article de la base de connaissances de Microsoft : https://support.microsoft.com/en-us/help/2769827.

- Vous ne pouvez pas créer un pool de postes de travail de clone lié ou une batterie de serveurs dans Horizon Console si aucune licence Horizon 7 n'est configurée.
  Solution : utilisez Horizon Administrator pour créer un pool de postes de travail de clone lié ou une batterie de serveurs sans licence Horizon 7.

- La connexion à Horizon Console à partir du navigateur Internet Explorer n'affiche que les mots-clés à la place des icônes. Ce problème se produit lorsque vous vous connectez à un Serveur de connexion ou un serveur de sécurité à l'aide d'une adresse IP plutôt qu'avec un nom DNS.
  Solution : utilisez un nom DNS plutôt qu'une adresse IP lors de la connexion. Pour plus d'informations, consultez l'article https://kb.vmware.com/s/article/2150307 de la base de connaissances de VMware.

- Lorsque vous utilisez Safari version 10.1.1 comme navigateur Web pour vous connecter à Horizon Console avec un nom de domaine complet, des problèmes d'interface utilisateur peuvent se produire (par exemple, les panneaux bas apparaissent vides).
  Solution : Safari version 10.1.1 n'est pas une version de navigateur Web prise en charge pour Horizon Console. Utilisez une version de Safari antérieure à la version 10.1.1 ou la version 11.0.2 et versions ultérieures pour vous connecter à Horizon Console.

- Les problèmes d'interface utilisateur suivants se produisent dans Horizon Help Desk Tool pour des sessions Linux globales dans un déploiement d'Architecture Cloud Pod :

  - Le message Une erreur interne s'est produite s'affiche, l'état de Skype Entreprise ne s'affiche pas et la version du système d'exploitation indique « - » lorsque vous cliquez sur les détails de la session dans l'onglet Détails.
  - Le message « Échec de l'obtention du ticket d'assistance à distance » s'affiche lorsque vous cliquez sur Assistance à distance.
  - Le message Une erreur interne s'est produite s'affiche lorsque vous cliquez sur l'onglet Applications.

  Solution : aucune. Le Service d'assistance d'Horizon ne prend pas en charge les fonctionnalités d'interface utilisateur suivantes pour les postes de travail Linux : état de Skype Entreprise, Assistance à distance, onglet Applications et état d'inactivité de session.

- Horizon Administrator ne met pas à jour les informations de récupération d'espace pour un serveur vCenter Server sur vSphere 6.7 qui utilise le système VMFS6 avec la fonctionnalité UNMAP automatique.
  Solution : aucune.

- Après une mise à niveau vers Horizon 7 version 7.5, seul le premier Serveur de connexion qui a été installé peut se connecter au serveur d'inscription.
  Solution : arrêtez le service d'Horizon Connection Server, supprimez les certificats avec le nom convivial « vdm.ec » du magasin de certificats de VMware Horizon View et redémarrez le service d'Horizon Connection Server.

- La connexion à Horizon Console échoue si vous utilisez l'adresse IP pour vous connecter à Horizon Console sur un navigateur Web Firefox, Google Chrome, Microsoft Edge ou Safari.
  Solution : utilisez le nom de domaine complet pour vous connecter à Horizon Console. Pour plus d'informations sur l'utilisation du nom de domaine complet pour vous connecter à des applications Web, consultez le document *Sécurité d'Horizon 7*.

- Horizon Administrator affiche nul/nul dans la colonne Nom d'utilisateur de la page Utilisateurs et groupes pour les utilisateurs suivants : Opérateurs de compte, Générateurs d'approbations de forêt entrante, Serveurs de licences des services Terminal Server, Groupe d'accès d'autorisation Windows, Opérateurs de serveur et Accès compatible pré-Windows 2000.
  Solution : aucune.

- Après une mise à niveau vers vSphere 6.7, vous ne pouvez pas utiliser la spécification personnalisée créée avec une version de vSphere antérieure à 6.7.
  Solution : après une mise à niveau vers vSphere 6.7, créez une spécification personnalisée et utilisez-la pour le provisionnement de pool.

- Horizon Help Desk Tool affiche l'heure d'ouverture de session de l'espace d'échange et de l'espace d'hébergement, mais n'affiche pas l'heure d'ouverture de session d'un espace qui n'est ni l'espace d'échange ni l'espace d'hébergement. Horizon Help Desk Tool affiche l'heure d'ouverture de session au bout de quelques minutes pour l'espace d'hébergement si l'espace d'échange est un espace distant.
  Solution : si Horizon Help Desk Tool n'affiche pas l'heure d'ouverture de session pour l'espace d'hébergement, fermez la page qui affiche les détails de la session, attendez 7 à 8 minutes et accédez à l'onglet Détails pour afficher de nouveau les détails de session.

- VMware Identity Manager échoue parfois à lancer des postes de travail. Lorsque vous enregistrez des détails de configuration SAML pour la première fois dans VMware Identity Manager avec SAML activé sur le Serveur de connexion, des postes de travail ne démarrent pas.
  Solution : enregistrez à nouveau le profil et effectuez une opération de synchronisation sur le nouveau profil. L'opération de synchronisation peut se produire toutes les heures ou tous les jours, selon le réglage défini par l'administrateur.

- Horizon Administrator sur Chrome en mode incognito affiche une erreur lorsque vous tentez d'exporter le contenu d'un tableau au format CSV : **Le fichier ne peut pas être exporté, car un fichier avec le même nom est actuellement ouvert. Fermez le fichier et réessayez ou bien utilisez un nom de fichier différent.**
  Solution : utilisez Horizon Administrator sur Chrome en mode normal pour exporter le tableau.

- Lorsque vous utilisez Sysprep pour personnaliser des clones liés Windows 10 sur vCenter Server 6.7, les postes de travail de clone lié se bloquent indéfiniment dans l'état de personnalisation lors d'opérations de provisionnement ou de recomposition.
  Solution : utilisez vCenter Server 6.5 U2 ou une version antérieure. Si vous devez utiliser vCenter Server 6.7, utilisez la méthode de personnalisation Quickprep.

- Dans Horizon Administrator, vous pouvez ajouter un utilisateur d'accès à distance en tant qu'utilisateur d'accès non authentifié. Toutefois, les utilisateurs d'accès non authentifié ne peuvent pas obtenir un accès distant depuis des passerelles externes. L'utilisateur ne pourra pas accéder à des postes de travail virtuels et ne peut lancer que des applications en tant qu'utilisateur d'accès non authentifié. Si l'utilisateur tente de se connecter avec un accès normal, le message d'erreur « Type d'authentification incorrect demandé » s'affiche.
  Solution : aucune.

- L'authentification unique d'Horizon échoue lorsque la portée du paramètre d'authentification de confiance est définie sur « Authentification sélective ».
  Solution : utilisez l'une des solutions suivantes pour résoudre ce problème.

    - Utilisez l'authentification à l'échelle du domaine.
    - Continuez à utiliser le paramètre de sécurité « Authentification sélective », mais octroyez explicitement l'autorisation « Autorisation d'authentifier » à tous les comptes d'hôte d'Horizon Connection Server (système local) sur tous les contrôleurs de domaine des objets ordinateur (ordinateurs ressource) qui résident dans le domaine ou la forêt de confiance. Pour plus d'informations sur la façon d'octroyer l'autorisation « Autorisation d'authentifier », consultez l'article de Microsoft Grant the Allowed to Authenticate permission on computers in the trusting domain or forest (Octroyer l'autorisation Autorisation d'authentifier sur des ordinateurs dans le domaine ou la forêt de confiance).
- Avec la fonctionnalité Architecture Cloud Pod, dans certains cas, les serveurs du Gestionnaire de licences des services Bureau à distance (RDS) délivrent plusieurs licences permanentes au même client dans un environnement de gestion des licences en mode mixte.

  Solution : aucune. Il s'agit d'un problème de tiers sur la façon dont les serveurs du Gestionnaire de licences des services Bureau à distance de Microsoft délivrent les licences, sans rapport avec Horizon 7.

- Dans Horizon Administrator, l'option « Utiliser VMware Virtual vSAN » n'apparaît pas comme étant sélectionnée à l'étape Optimisation du stockage pendant le processus de clonage d'un pool de clones liés ou d'un pool automatisé contenant des machines virtuelles complètes créées sur une banque de données vSAN. Cependant, l'opération de clonage réussit.
  Solution : aucune.

- Les problèmes suivants se produisent lorsque vous parcourez la banque de données lors de la modification d'un pool de postes de travail automatisé contenant des machines virtuelles complètes :

    - Sous l'onglet Paramètres de vCenter, lorsque vous cliquez sur « Parcourir le magasin de

données », la valeur de stockage minimale recommandée en Go s'affiche.
    - Sous l'onglet Paramètres d'approvisionnement, augmentez le nombre maximal de machines, puis sélectionnez l'onglet Paramètres vCenter et cliquez sur « Parcourir le magasin de données ». La valeur de stockage minimale recommandée en Go augmente, mais elle est ajoutée à la valeur existante.
    - Pour un pool de postes de travail contenant trois machines dont l'une est disponible et l'autre toujours en phase de provisionnement ou de personnalisation, modifiez le pool de postes de travail, puis sélectionnez l'onglet Paramètres vCenter et cliquez sur « Parcourir le magasin de données ». La valeur de stockage minimale recommandée en Go s'affiche pour le total des trois machines.

  Solution : utilisez Horizon Administrator pour rechercher une banque de données lors de la modification d'un pool de postes de travail automatisé contenant des machines virtuelles complètes pour voir la valeur de stockage minimale recommandée en Go appropriée.

- Les problèmes suivants se produisent lorsque vous parcourez la banque de données pendant la modification de pools de postes de travail d'Instant Clone :

    - Une fois qu'un pool de postes de travail d'Instant Clone dispose de toutes ses machines à l'état disponible, modifiez-le, puis dans l'onglet Paramètres de vCenter, cliquez sur « Parcourir le magasin de données ». Les paramètres Minimum recommandé (Go), Maximum recommandé (Go) et Utilisation 50 % ont des valeurs positives.
    - Une fois qu'un pool de postes de travail d'Instant Clone dispose de toutes ses machines à l'état disponible, modifiez-le, puis augmentez le nombre maximal de machines virtuelles sous l'onglet Paramètres d'approvisionnement et cliquez sur « Parcourir le magasin de données » dans l'onglet Paramètres de vCenter. Les valeurs Minimum recommandé (Go), Maximum recommandé (Go) et Utilisation 50 % augmentent, mais elles sont ajoutées à la valeur existante.
    - Pour un pool de postes de travail contenant trois machines dont l'une est disponible et l'autre toujours en phase de provisionnement ou de personnalisation, modifiez le pool de postes de travail, puis sélectionnez l'onglet Paramètres vCenter et cliquez sur « Parcourir le magasin de données ». Les valeurs Minimum recommandé (Go), Maximum recommandé (Go) et Utilisation 50 % sont affichées pour le total des trois machines.

  Solution : utilisez Horizon Administrator pour rechercher une banque de données pendant la modification de pools de postes de travail d'Instant Clone pour afficher les valeurs Minimum recommandé (Go), Maximum recommandé (Go) et Utilisation 50 % appropriées.

- Après que vous avez créé, puis modifié un pool de postes de travail automatisé contenant des machines virtuelles complètes avec au moins deux noms en utilisant une valeur pour « # machines non attribuées maintenues sous tension » inférieure aux noms réels spécifiés, le champ « # machines non attribuées maintenues sous tension » n'accepte pas une valeur égale au nombre total de noms spécifié pendant le processus de création du pool. Vous obtenez donc un message d'erreur incorrect.
  Solution : utilisez Horizon Administrator pour modifier le pool de postes de travail automatisé qui contient des machines virtuelles complètes avec au moins deux noms afin de mettre à jour la valeur du champ « # machines non attribuées maintenues sous tension ».

- Les tentatives de connexion au portail HTML Access ou à l'une des consoles d'administration à l'aide d'une adresse IP ou du CNAME échouent pour la plupart des navigateurs sans configuration supplémentaire. Le plus souvent, une erreur est signalée, mais parfois un message d'erreur vide s'affiche.
  Solution : pour résoudre ce problème, consultez la section « Vérification de l'origine » du document *Sécurité d'Horizon 7*.

- Lors de la configuration de Skype Entreprise, il existe une fonctionnalité facultative pour activer le Contournement de média qui contourne le serveur de médiation.
  Dans le cas d'appels optimisés Skype Entreprise à destination et en provenance des utilisateurs PSTN, le média est toujours acheminé via le serveur de médiation, que la fonction Contournement de média soit activée ou non.

Solution : aucune. La fonction Contournement de média n'est pas prise en charge avec le Pack de virtualisation pour Skype Entreprise. Consultez l'article 56977 dans la base de connaissances de VMware : https://kb.vmware.com/s/article/56977.

- Si le même utilisateur existe dans les deux espaces du Serveur de connexion qui doivent être couplés dans un environnement Architecture Cloud Pod, Horizon Administrator indique que la valeur de « Espaces source » est 2 et il source l'utilisateur depuis les deux espaces. Un administrateur peut modifier l'utilisateur dans les deux espaces, ce qui peut entraîner des incohérences dans la configuration de l'utilisateur lors de l'ouverture de session hybride. En outre, l'ouverture de session hybride pour l'utilisateur ne peut pas être désactivée.
  Solution : vous devez supprimer l'utilisateur dans les deux espaces, puis le recréer et le configurer pour l'ouverture de session hybride.

- Des messages d'erreur de vidage de mémoire sont générés lors de l'ajout de banques de données Virtual Volumes sur ESXi imbriqué ou ESXi virtuel imbriqué.
  Solution : aucune.

- Horizon Administrator et Horizon Console affichent les noms de dossier internes au lieu des noms de dossier réels lorsque vous parcourez une banque de données vSAN pour importer un disque persistant.
  Solution : aucune.

- Dans Horizon Administrator et Horizon Console, des rôles personnalisés avec le privilège Gérer le service d'assistance (lecture seule) sont affichés comme étant applicables aux groupes d'accès.
  Solution : aucune.

- Les utilisateurs qui disposent du rôle Administrateurs (lecture seule) ne peuvent pas voir **Configuration de View > Architecture Cloud Pod** dans Horizon Administrator.
  Solution : utilisez Horizon Console.

- Dans Horizon Administrator, lorsque vous ajoutez ou modifiez une batterie de serveurs de clone lié qui utilise des banques de données vSAN, l'option Durée d'interruption est désactivée.
  Solution : utilisez Horizon Console pour définir des durées d'interruption pour une batterie de serveurs de clone lié qui utilise des banques de données vSAN.

- Dans Horizon Administrator, le bouton Recréer ne fonctionne pas dans le résumé de machine d'un pool de postes de travail automatisé qui contient des machines virtuelles complètes.
  Solution : dans Horizon Administrator, utilisez la fonctionnalité Recréer dans Machines > vCenter Server.

- Lorsque vous ajoutez un serveur vCenter Server au Serveur de connexion à l'aide d'un script PowerShell existant, le message d'erreur suivant s'affiche : Échec de l'ajout de l'instance de vc : Aucune constante enum com.vmware.vdi.commonutils.Thumbprint.Algorithm.SHA-1. Ce problème se produit, car la propriété certificateEncoding qui indique un remplacement de certificat pour des certificats auto-signés est ajoutée dans Horizon 7 version 7.8. Par conséquent, les versions antérieures des scripts VMware PowerCLI qui ont la valeur SHA-1 incorrecte échouent.
  Solution : mettez à jour les scripts PowerShell pour utiliser la valeur de propriété DER_BASE64_PEM au lieu de SHA-1. Par exemple, définissez $certificate_override.sslCertThumbprintAlgorithm = 'DER_BASE64_PEM'.

- Lorsqu'une application UWP (Universal Windows Platform) est mise à niveau, le chemin d'accès contenant la version change et l'application est inaccessible par le chemin d'origine. L'état de l'application est **Non disponible** dans Horizon Administrator et un utilisateur ne peut pas lancer l'application.

  Solution : mettez à jour le chemin de l'application dans Horizon Administrator après une mise à niveau et vérifiez que l'état de l'application est **Disponible**. Vous pouvez également ne pas mettre à niveau l'application.

- Lorsque le filtrage des périphériques est configuré pour la fonctionnalité de redirection du lecteur client et qu'un utilisateur utilise le protocole d'affichage RDP pour se connecter, le filtrage des périphériques ne fonctionne pas.

  Solution : lorsque le filtrage des périphériques est configuré pour la redirection du lecteur client, configurez le Serveur de connexion afin que les connexions RDP ne soient pas autorisées.

- La fonctionnalité de déverrouillage de poste de travail d'authentification unique réelle est prise en charge dans les protocoles PCoIP et Blast, mais pas dans le protocole RDP (Remote Desktop Protocol).

- Dans Horizon Console, le résumé de l'utilisateur ou du groupe ne parvient pas à se charger en raison de problèmes d'approbation de domaine dans les cas suivants :

  - Lorsque des utilisateurs et des groupes appartiennent à un domaine d'approbation unidirectionnelle et que l'administrateur connecté dispose des autorisations nécessaires à partir d'un domaine d'approbation unidirectionnelle.
  - Lorsque des utilisateurs et des groupes appartiennent à un domaine d'approbation bidirectionnelle et que l'administrateur connecté dispose des autorisations nécessaires à partir d'un domaine d'approbation bidirectionnelle.
  - Lorsque des utilisateurs et des groupes appartiennent à un domaine d'approbation unidirectionnelle ou bidirectionnelle et que l'administrateur connecté provient du domaine enfant et dispose des autorisations nécessaires.

  Solution : utilisez Horizon Administrator pour accéder au résumé de l'utilisateur ou du groupe.

- Dans Horizon Console, certains événements peuvent ne pas être répertoriés, car l'heure du Serveur de connexion est définie de manière incorrecte par rapport au fuseau horaire du Serveur de connexion.
  Solution : utilisez Horizon Administrator pour consulter tous les événements.

- Vous pouvez récupérer une machine virtuelle Instant Clone avec une session active. Cela se produit dans Horizon Administrator et dans Horizon Console.
  Solution : aucune.

- Dans Horizon Administrator et Horizon Console, lorsque vous supprimez des instances de vCenter Server avec des disques persistants détachés, Horizon Administrator affiche toujours les disques de ces instances, mais ils ne peuvent pas être utilisés. Horizon Console n'affiche aucun disque détaché, mais affiche des bannières d'erreur internes.
  Solution : aucune solution connue. Vérifiez qu'il n'y a aucun disque détaché de vCenter Server avant la suppression.

- Les machines virtuelles installées avec Windows 2019 et créées en sélectionnant le système d'exploitation Windows 2019 dans vSphere Client pour vSphere 7 ne sont ni répertoriées ni prises en charge dans Horizon 7.
  Solution : installez Windows 2019 sur la machine virtuelle en sélectionnant la version du système d'exploitation Windows 2016 dans vSphere Client.

- Lorsque vous lancez Horizon Administrator à partir de l'icône de la console Horizon 7 Administrator ou en entrant `https://localhost/admin` ou `https://localhost/newadmin` dans la barre d'adresses d'un navigateur, vous êtes redirigé vers `https://127.0.0.1/admin`. Cette redirection vers une adresse IP peut entraîner un échec de l'authentification, comme décrit dans l'article 2150307 de la base de connaissances de VMware : Impossible de se connecter à une application Web VMware, telle que Horizon Administrator ou Horizon Help Desk Tool.

  Solution : pour empêcher la redirection vers une adresse IP, entrez `https://localhost/admin/` dans la barre d'adresses du navigateur (assurez-vous d'ajouter « `/` » à la fin de l'URL).

- Dans Horizon Console, lorsque vous dupliquez un pool de postes de travail de clone lié qui utilise la technologie de snapshot NFS natif, l'assistant « Dupliquer le pool » n'affiche pas l'option « Utiliser des snapshots NFS natifs (VAAI) » sélectionnée dans l'étape d'optimisation avancée lorsque la récupération d'espace disque est activée sur l'instance de vCenter Server sélectionnée.
  Solution : sélectionnez manuellement l'option « Utiliser des snapshots NFS natifs (VAAI) » dans l'assistant Dupliquer le pool.

- Les options **Prélancement** et **Utiliser le site d'accueil** ne fonctionnent pas correctement ensemble pour les droits applicatifs globaux. Lorsque vous créez un droit applicatif global, si vous activez les options **Prélancement** et **Utiliser le site d'accueil**, la session prélancée peut ne pas être créée à partir du site de base. Ce problème se produit, car la même session est utilisée pour démarrer les applications suivantes, et ces sessions ne sont pas démarrées à partir du site de base.

  Solution : aucune.

- Le message d'erreur suivant peut s'afficher lors de l'installation ou de la désinstallation du serveur de connexion : « Erreur durant l'ouverture du fichier journal d'installation. Vérifiez que l'emplacement spécifié pour le journal existe et qu'il est accessible en écriture. » Cette erreur se produit en raison d'une erreur de Microsoft. Pour plus d'informations, reportez-vous à la page : https://support.microsoft.com/en-in/help/2564571/error-opening-installation-log-file-verify-that-the-specified-location.
  Solution : redémarrez la machine virtuelle sur laquelle le serveur de connexion est installé.

Horizon Agent for Linux

Cette section décrit les problèmes qui peuvent se produire avec Horizon Agent for Linux ou lorsque vous configurez un poste de travail Linux.

- Parfois, la fenêtre Collaboration n'apparaît pas une fois que vous êtes connecté à un poste de travail distant et que vous cliquez sur l'icône d'interface utilisateur de Collaboration.

  Solution : redimensionnez la fenêtre du poste de travail ou reconnectez-vous au poste de travail distant.

- La configuration de quatre écrans avec une résolution de 2 560 x 1 600 sur des machines virtuelles RHEL 6.6 ou CentOS 6.6 dans vSphere 6.0 n'est pas prise en charge.
  Solution : utilisez la résolution de 2 048 x 1 536 ou déployez cette configuration dans vSphere 5.5.

- La disposition et les paramètres régionaux du clavier de l'agent Linux ne se synchronisent pas avec le client si le système de méthode de saisie du clavier est défini sur `fcitx`.
  Solution : définissez le système de méthode de saisie du clavier sur `iBus`.
- L'authentification unique (SSO) ne fonctionne pas correctement sur un poste de travail RHEL/CentOS 7.2 lorsque vous ajoutez un domaine à l'aide de SSSD (System Security Services Daemon).
  Solution : une fois que vous ajoutez un domaine à l'aide de SSSD, modifiez le fichier `/etc/pam.d/password-auth` en utilisant les informations dans l'article 2150330 de la base de connaissances de VMware SSO configuration changes required when using SSSD to join AD on RHEL/CentOS 7.2 Desktops (Modifications de configuration SSO requises lorsque vous utilisez SSSD pour joindre AD sur des postes de travail RHEL/CentOS 7.2).

- **Lorsqu'un utilisateur client s'authentifiant avec la redirection de carte à puce se connecte à un poste de travail Ubuntu 18.04/16.04 ou SLED/SLES 12 SP3 et retire ou réinsère la carte à puce avant d'entrer le code PIN, le poste de travail ne semble pas reconnaître la modification.**
  Le poste de travail détecte uniquement une modification de l'état de la carte à puce une fois que l'utilisateur ferme l'invite demandant le code PIN.

  Solution : à l'invite, entrez le code PIN de la carte à puce et cliquez sur OK. Ou cliquez sur Annuler pour ignorer l'invite sans entrer de code PIN.

- Sur Ubuntu 16.04, si l'administrateur tente de désactiver la redirection de carte à puce en définissant VVC.ScRedir.Enable sur « FALSE » dans le fichier de configuration /etc/vmware/config, le poste de travail se bloque sur l'écran de connexion.

- **Lorsqu'un utilisateur client se connecte à un poste de travail Ubuntu 18.04/16.04 ou SLED/SLES 12 SP3, « Erreur 2306 : Aucun jeton adapté disponible » s'affiche sur l'écran de connexion.**
  Ce message d'erreur indique qu'une carte à puce a été retirée du système client. L'utilisateur peut se connecter au poste de travail en entrant le mot de passe de l'utilisateur ou en réinsérant la carte à puce.

- **Après s'être connecté à un poste de travail Ubuntu 16.04 et avoir entré un code PIN incorrect pour l'authentification par carte à puce, l'utilisateur client rencontre une invite de connexion pour entrer le mot de passe de l'utilisateur au lieu du code PIN de la carte à puce.**
  L'utilisateur client peut cliquer sur OK pour fermer l'invite de mot de passe de l'utilisateur. Une nouvelle invite s'affiche et demande à l'utilisateur d'entrer le code PIN de la carte à puce.

- **Sur Ubuntu 18.04/16.04 et SLED/SLES 12 SP3, l'économiseur d'écran du poste de travail n'est pas verrouillé comme prévu lorsque l'utilisateur retire une carte à puce du système client.**
  Par défaut, l'économiseur d'écran du poste de travail n'est pas verrouillé, même après que l'utilisateur client a supprimé la carte à puce utilisée pour s'authentifier sur le poste de travail. Pour verrouiller l'économiseur d'écran dans ces conditions, vous devez configurer pkcs11_eventmgr sur le poste de travail.

  Solution : configurez pkcs11_eventmgr pour spécifier le comportement correct de l'économiseur d'écran en réponse aux événements de carte à puce.

- Après l'installation d'Horizon Agent avec la redirection de carte à puce activée (paramètre -m défini sur « Oui ») sur un poste de travail RHEL 7.0, Horizon Administrator, Horizon Console ou vSphere peut afficher un écran noir. La redirection de carte à puce est prise en charge sur des postes de travail exécutant RHEL 7.1 ou version ultérieure. La fonctionnalité n'est pas prise en charge sur les postes de travail RHEL 7.0.

  Solution : installez Horizon Agent avec la redirection de carte à puce activée sur un poste de travail exécutant RHEL 7.1 ou version ultérieure.

- Si vous configurez deux écrans avec des résolutions différentes, et que la résolution de l'écran principal est inférieure à celle de l'écran secondaire, vous pouvez ne pas parvenir à bouger la souris ou à faire glisser des fenêtres d'application vers certaines zones de l'écran.
  Solution : assurez-vous que la résolution de l'écran principal est au moins égale à celle de l'écran secondaire.

- Lorsque vous utilisez une carte à puce sur un poste de travail RHEL 7 et activez l'option pour verrouiller l'écran lors du retrait de la carte, l'écran peut se verrouiller immédiatement après votre connexion avec la carte à puce. Il s'agit d'un problème connu de RHEL 7.

  Solution : pour accéder au poste de travail, déverrouillez l'écran après la connexion avec la carte à puce.

- Sur un poste de travail Ubuntu, Single Sign-On (SSO) ne fonctionne pas lorsque le système d'exploitation met automatiquement à jour le fichier binaire gnome-shell. La stratégie par défaut dans Ubuntu consiste à télécharger et à installer automatiquement les mises à jour du système d'exploitation.

  Solution : modifiez la stratégie dans Ubuntu pour télécharger et installer manuellement les mises à jour du système d'exploitation, au lieu d'une installation automatique.

- Lorsqu'un utilisateur final utilise une carte à puce pour ouvrir une session sur un poste de travail RHEL 8.0/8.1, l'écran d'accueil peut demander le mot de passe de l'utilisateur au lieu du code PIN de la carte à puce. Ce problème peut se produire plus fréquemment lorsque la latence du réseau est élevée.

  Solution : pour réduire les occurrences de ce problème, modifiez le fichier `/etc/sssd/sssd.conf` en augmentant la valeur de `p11_child_timeout` sous la section `[pam]`. Redémarrez ensuite le poste de travail.

Horizon Agent

- En mode FIPS, Horizon Agent ne parvient pas à se coupler avec le Serveur de connexion et l'état du pool n'est pas disponible lorsqu'Horizon Agent est installé sur un lecteur qui n'est pas le lecteur C.
  Solution : en mode FIPS, installez Horizon Agent sur le lecteur C.
- Un message d'avertissement sur les applications utilisées s'affiche lorsque vous désinstallez Horizon Agent sous Windows Server 2016.
  Solution : cliquez sur Ignorer dans la boîte de dialogue qui s'affiche lorsque vous utilisez Ajouter ou supprimer des programmes de Windows pour désinstaller Horizon Agent. Si vous désinstallez Horizon Agent à partir de la ligne de commande, utilisez la commande `msiexec /x /qn {GUID of Agent}` plutôt que la commande `msiexec /x {GUID of Agent}`.
- Lorsque vous désinstallez Horizon Agent, la vitesse de la souris est lente et saccadée. La désinstallation d'Horizon Agent désinstalle également le pilote vmkbd.sys.
  Solution : réparez VMware Tools sur la machine virtuelle Horizon Agent.

- Lors d'une mise à niveau d'Horizon Agent 7.1 vers Horizon Agent 7.2 sur un système d'exploitation invité Windows 7, une boîte de dialogue « Fichiers en cours d'utilisation » s'affiche. La boîte de dialogue indique que l'application VMware Horizon Agent utilise des fichiers qui doivent être mis à jour par le programme d'installation.
  Solution : cliquez sur Ignorer pour poursuivre la mise à niveau.

- Avant que la gestion des profils ne termine la synchronisation des données utilisateur, le poste de travail est actualisé ou supprimé si la stratégie d'actualisation ou de suppression à la fermeture de session est activée.

  Solution : Aucun

- L'installation d'Horizon Agent sur Windows 10 32 bits déclenche l'exception « les arguments ne sont pas valides » et l'installation continue lorsque vous cliquez sur OK. Cette erreur se produit, car le service de spouleur d'impression est désactivé.
  Solution : activez le service de spouleur d'impression pour que l'installation fonctionne comme prévu.
- Si le propriétaire d'une session regarde une vidéo qui a été accélérée à l'aide de MMR pendant une session de collaboration, les collaborateurs voient un écran noir au lieu de la vidéo.

  Solution : en tant que propriétaire de session, si vous avez besoin de lire une vidéo pendant une session de collaboration, n'utilisez pas Windows Media Player ou Internet Explorer pour lire la vidéo, ou désactivez MMR sur les pools dans lesquels la collaboration est activée.

- Si un collaborateur rejoint une session à plusieurs écrans et active le mode de souris relative sur son client, il est possible que la souris se déplace vers un moniteur secondaire qui n'est pas visible par le collaborateur.

  Solution : déplacez la souris en arrière sur l'écran. Vous pouvez également ne pas utiliser le mode de souris relative dans une session à plusieurs écrans.

- Si vous utilisez Chrome avec la redirection de contenu URL, que vous définissez « .*.google.* » comme protocole HTTPS dans les règles de filtrage et Google comme page d'accueil dans Chrome, la redirection vers google.com se produit chaque fois que vous ouvrez un nouvel onglet.

  Solution : modifiez la page d'accueil ou les règles de filtrage.

- Lorsque vous configurez une session de collaboration, l'ajout d'un collaborateur par son adresse e-mail à partir d'un domaine approuvé bidirectionnel échoue.

  Solution : ajoutez le collaborateur à l'aide de domaine\utilisateur.

- La redirection multimédia HTML5 fonctionne pour Edge dans un poste de travail virtuel antérieur à Windows 10 1803, mais, après la mise à jour vers la dernière version de Windows 10 1803, telle que 17133, la redirection ne fonctionne pas, en particulier pour les sites Web qui utilisent la lecture automatique, comme youtube.com.

  Solution : forcez le redémarrage du poste de travail virtuel Windows 10.

- Les applications publiées ne sont pas déconnectées lorsque la session du client est inactive, même lorsque le délai d'expiration de session inactive est défini avec MaxIdleTime à l'aide de la méthode GPO ou non-GPO. Un message d'avertissement de déconnexion s'affiche, mais l'application n'est pas déconnectée.

- Après avoir effectué une opération de recherche de support de diffusion en continu à l'aide de la redirection multimédia, l'audio et la vidéo ne sont pas nets.

  Solution : attendez quelques minutes ou rouvrez le support de diffusion en continu.

- Parfois, lorsqu'un utilisateur utilise la fonctionnalité de redirection multimédia HTML5 pour lire une vidéo YouTube dans le navigateur Edge, la vidéo conserve la mise en mémoire tampon et il n'y a pas d'image ou de son.

  Solution : actualisez la page.

- Lorsque vous êtes connecté à un poste de travail distant sur lequel la fonctionnalité Audio/Vidéo en temps réel est activée, le message suivant peut s'afficher : « Votre PC doit être redémarré pour terminer la configuration de ce périphérique : *devicename* (VDI). »

  Solution : vous pouvez ignorer ce message, car le périphérique est utilisable sur le poste de travail distant. Vous pouvez également désactiver la notification de paramètres Windows pour empêcher l'affichage du message.

- Si vous êtes connecté à un poste de travail avec plusieurs moniteurs haute résolution (4K) et que vous lisez une vidéo en plein écran avec le nouveau codec Blast, les performances de lecture peuvent être médiocres (fréquence d'image faible).

  Solution : utilisez H.264 pour lire les vidéos en plein écran.

- Les utilisateurs ne peuvent pas utiliser une imprimante série avec la fonctionnalité de redirection de port série lorsqu'Horizon Agent est installé sur un hôte RDS si le paramètre de stratégie de groupe d'agent **Mode d'isolation du port COM** est défini sur **Isolation complète** (paramètre par défaut). Ce problème affecte les clients Windows et Linux. Ce problème ne se produit pas sur les postes de travail virtuels.

  Solution : modifiez le paramètre de stratégie de groupe **Mode d'isolation du port COM**, modifiez le mode sur **Isolation désactivée** et redémarrez Horizon Agent. Pour plus d'informations, consultez la section « Paramètres de la stratégie de groupe de redirection de port série » du document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

- Lorsque vous utilisez la fonctionnalité VMware Integrated Printing, si vous vous connectez à une machine agent Windows 10 à partir d'une machine cliente Windows 7 et que vous imprimez des documents contenant des polices Delta à partir d'une imprimante redirigée, les polices ne s'affichent pas correctement.

  Solution : aucune. Il s'agit d'un problème de tiers.

- Échec de Sysprep pour les clones liés et les clones complets avec les systèmes d'exploitation Windows 10 1903, Windows 10 1909 (32 bits et 64 bits) avec l'erreur : **SYSPRP Sysprep_Clean_Validate_Opk: le mode audit ne peut pas être activé s'il existe un scénario actif. hr = 0x800F0975**

  Solution : appliquez ces instructions sur l'image maître, puis provisionnez le poste de travail : https://social.technet.microsoft.com/Forums/fr-FR/0dcbdf32-05a1-4edc-8f22-287998d30de5/sysprep-problem-audit-mode-canamp39t-be-turned-on-if-there-is-an-active-scenario?forum=win10itprosetup.

- Le lancement d'une application RDSH à l'aide d'associations de type de fichier nécessite que la fonctionnalité Redirection du lecteur client soit installée et activée sur la machine agent.

- Lorsque vous mettez à jour le système d'exploitation de Windows 1809 vers 1903, un écran noir peut s'afficher sur Horizon Agent.

  Solution : appliquez la procédure décrite dans cet article de la base de connaissances sur l'image du système d'exploitation.

- Si Horizon Agent est installé sur un hôte RDS et que le paramètre de stratégie de groupe **Nom de l'imprimante pour les agents RDSH** de la fonctionnalité VMware Integrated Printing est configuré pour utiliser le nom de la machine cliente comme suffixe, le nom de la machine cliente prend uniquement en charge les caractères de langue anglaise. Si le nom de la machine cliente contient des caractères dans une langue autre que l'anglais, la fonctionnalité VMware Integrated Printing ne fonctionne pas dans les postes de travail publiés et les applications publiées.

  Solution : aucune.

- Si vous disposez d'Horizon Agent 7.12 ou version antérieure s'exécutant sur un hôte avec un écran de 5K et si vous vous connectez à un poste de travail distant à l'aide du protocole PCoIP ou Blast en mode plein écran et si vous augmentez la taille de la fenêtre à une valeur supérieure à 4K, l'affichage de la session distante ne s'ajuste pas automatiquement à la taille de l'écran ou de la fenêtre.

  Solution : réduisez la taille de la fenêtre du poste de travail à une valeur inférieure à 4K. Sur les périphériques qui prennent en charge l'écran Retina, quittez le mode plein écran et passez à l'affichage Normal.

Horizon GPO Bundle

- Les objets de stratégie globale (GPO) basés sur ordinateur et nécessitant un redémarrage ne sont pas appliqués aux Instant Clones.
  Solution : consultez l'article 2150495 de la base de connaissances de VMware.

- Dans une configuration en mode imbriqué où le poste de travail de premier niveau (la machine sur laquelle Horizon Client et Horizon Agent sont installés) est un poste de travail virtuel et où le poste de travail de second niveau est un poste de travail publié, le paramètre de stratégie de groupe « Spécifier un filtre de redirection des imprimantes clientes » n'affecte pas le poste de travail de second niveau si vous le configurez dans le poste de travail virtuel de premier niveau.

  Solution : si vous voulez filtrer les imprimantes pour le poste de travail de second niveau, configurez la stratégie de groupe « Spécifier un filtre de redirection des imprimantes clientes » dans le poste de travail de second niveau.

Horizon Client

Cette section décrit les problèmes que les utilisateurs finaux peuvent rencontrer lors de l'utilisation d'Horizon Client ou d'HTML Access pour se connecter à des applications et postes de travail distants. Si des problèmes se produisent uniquement dans une plate-forme Horizon Client spécifique, reportez-vous aux notes de mise à jour d'Horizon Client sur la page de Documentation des clients Horizon Client.

- Il manque des données de profil pour plusieurs sessions utilisateur sur des hôtes RDS. Ce problème se produit lorsque les sessions sont dans l'état déconnecté, mais le gestionnaire des tâches sur l'hôte RDS affiche toujours ces sessions.
  Solution : supprimez les sessions de l'hôte RDS ou fermez la session de l'utilisateur à partir de l'application ou du poste de travail publié.

- Lorsque vous vous connectez à Workspace ONE, la session de prélancement d'applications ne se déclenche pas. Les sessions de prélancement sont déclenchées uniquement lors d'une connexion au Serveur de connexion à partir d'Horizon Client.
  Solution : démarrez manuellement une application ou un poste de travail à partir de Workspace ONE pour déclencher le démarrage des applications activées pour le prélancement.

- Lorsque le protocole d'affichage VMware Blast est utilisé avec Blast Secure Gateway (BSG) désactivé, Horizon Client n'est pas toujours en mesure de récupérer après une brève panne de réseau (1 minute environ) et la connexion au poste de travail est alors perdue. Ce problème ne se produit pas lorsque BSG est activé.
  Solution : reconnectez la session.
- L'hôte RDS ne stocke qu'un seul ensemble de données d'application pour le premier lancement d'application d'une session. Aucune donnée de lancement d'application suivante n'est perdue.
  Solution : fermez la session et lancez une autre application pour stocker ces données.

- Les postes de travail ne démarrent pas lorsque vous utilisez HTML Access à partir des navigateurs Web Internet Explorer ou Microsoft Edge pour vous connecter au Serveur de connexion, au serveur de sécurité ou au Serveur réplica sur un système d'exploitation client Windows 10. Ce problème affecte les postes de travail dotés des systèmes d'exploitation Windows 10 N, Windows 10 KN, Windows 7 N et Windows 7 KN.
  Solution : utilisez les navigateurs Web Firefox ou Google Chrome pour HTML Access.

- Pour Intel vDGA, la prise en charge de plusieurs moniteurs est limitée à 3 moniteurs maximum. Le pilote Intel prend en charge 3 moniteurs maximum avec une résolution de 3 840 x 2 160 maximum. Si vous essayez de connecter 4 moniteurs, la connexion indique 3 écrans noirs avec un seul qui fonctionne.
- Si un poste de travail VDI se trouve dans un emplacement distant et rencontre une latence réseau élevée, un déverrouillage récursif utilisant l'authentification par carte à puce peut ne pas fonctionner.
  Solution : déverrouillez le poste de travail manuellement.

- Si l'utilisateur d'un poste de travail distant Windows 8 se connecte avec l'authentification Kerberos et que le poste de travail est verrouillé, le compte d'utilisateur permettant de déverrouiller le poste de travail que Windows 8 indique par défaut à l'utilisateur est le compte Windows Active Directory lié, et non le compte d'origine du domaine Kerberos. L'utilisateur ne peut pas voir le compte avec lequel il est connecté. Il s'agit d'un problème de Windows 8 qui n'est pas directement lié à Horizon 7. Ce problème peut se produire dans certains cas sous Windows 7.

  Solution : l'utilisateur doit déverrouiller le poste de travail en sélectionnant « Autre utilisateur ». Windows affiche le domaine Kerberos correct et l'utilisateur peut se connecter en utilisant son identité Kerberos.

- Lorsque vous utilisez Ambir Image Scan Pro 490i pour effectuer une numérisation sur une application ou un poste de travail distant, la boîte de dialogue affiche toujours « Numérisation… » et ne se termine pas.
  Solution : réalisez une numérisation sur le client. La numérisation du client étalonne le scanner. Une fois l'opération d'étalonnage terminée, enregistrez le fichier d'étalonnage et déployez-le dans `ProgramData\AmbirTechnology\ImageScanPro490i`

- L'entrée de clavier Unicode ne fonctionne pas correctement avec HTML Access sur les postes de travail Horizon 7 for Linux.

  Solution : aucune.

- Lorsque vous vous connectez à un poste de travail Linux, certaines entrées de clavier ne fonctionnent pas. Par exemple, si vous utilisez un éditeur de méthode d'entrée (IME) qui n'est pas en anglais à la fois sur le périphérique client et sur le poste de travail distant, certaines touches ne s'affichent pas correctement.
  Solution : définissez l'IME en anglais sur le périphérique client et dans une autre langue sur le poste de travail distant.
- Parfois, un appel audio ne démarre pas correctement à partir de Skype vers Skype Entreprise. L'état de l'appel est « Connexion de l'appel en cours… » sur le client Skype Entreprise.

  Solution : aucune.

- Si vous utilisez Skype Entreprise à l'intérieur d'un poste de travail non persistant, vous risquez d'atteindre la limite de 16 certificats de périphérique de Skype Entreprise. Lorsque cette limite est atteinte et que Skype for Business tente une nouvelle ouverture de session, un nouveau certificat est émis et le certificat le plus ancien attribué est révoqué.

  Solution : aucune.

- Si vous lancez Horizon Client 4.8 pour Linux ou version antérieure avec le mode FIPS activé et que vous essayez de vous connecter à une instance d'Horizon Agent 7.6 ou à l'Horizon Connection Server 7.6 ou version ultérieure avec le mode FIPS activé, le message d'erreur « Invalid license info for rds-license (Informations de licence non valides pour rds-license) : ID de client manquant » s'affiche.

  Solution : pour utiliser Horizon Client pour Linux avec le mode FIPS activé pour vous connecter à une instance d'Horizon Agent 7.6 ou version ultérieure ou à l'Horizon Connection Server 7.6 ou version ultérieure avec le mode FIPS activé, utilisez Horizon Client 4.9 pour Linux ou version ultérieure.

- Le certificat de serveur TLS auto-signé par défaut généré sur Unified Access Gateway, l'Horizon Connection Server et le serveur de sécurité peuvent ne pas être utilisables par les navigateurs Chrome, les navigateurs Safari ou les clients VMware Horizon s'exécutant sous macOS 10.15, iOS 13 et Chrome OS 76. Ce problème peut se produire, car Apple a modifié les conditions requises pour les certificats de serveur TLS approuvés dans ces versions de système d'exploitation. Les certificats auto-signés par défaut ne répondent actuellement pas à ces nouvelles exigences. Si la connexion à Horizon à partir d'un client se fait via un équilibrage de charge intermédiaire ou un proxy qui termine TLS, les nouvelles conditions de certificat doivent également être remplies sur ces périphériques. Sur Horizon Client pour Mac sur macOS 10.15, le mode « Avertir avant de se connecter à des serveurs non approuvés » peut ne pas continuer sans vérifier le certificat auto-signé. La boîte de dialogue « Connexion au serveur non approuvée » s'affiche avec le message d'erreur « VMware Horizon Client ne peut pas vérifier votre connexion. Contactez votre administrateur. » et seuls les boutons « Afficher le certificat » et « Ne pas se connecter » sont disponibles.

  Solution : VMware recommande généralement que le certificat de serveur TLS auto-signé par défaut sur ces produits soit remplacé par un certificat signé par une autorité de certification de confiance pour l'environnement. Cette recommandation est toujours une bonne pratique de sécurité. Dans cette situation, à condition que le certificat signé par une autorité de certification de confiance réponde aux nouvelles exigences d'Apple, le problème ne se produit pas. Une autre solution pour les clients d'Horizon macOS et iOS consiste à définir la configuration SSL pour ne pas vérifier les certificats de serveur. Pour plus d'informations sur les conditions requises du certificat Apple, consultez https://support.apple.com/fr-fr/HT210176

Horizon JMP Server et JMP Integrated Workflow

- Dans un environnement où plusieurs serveurs JMP Server sont installés, des conflits peuvent se produire lors de la création ou de la suppression d'attributions JMP si plusieurs serveurs JMP Server font référence au même partage de configuration User Environment Manager.

  Solution : aucune.

- Si vous avez configuré vos paramètres JMP afin de n'utiliser qu'une seule instance de VMware App Volumes Manager et si, pendant la création d'une attribution JMP, vous avez sélectionné un pool de postes de travail pour lequel Horizon Agent ne pointe pas vers cette instance configurée d'App Volumes Manager, vous pouvez toujours sélectionner des AppStacks dans l'instance d'App Volumes Manager qui est indiquée par Horizon Agent du pool postes de travail. De plus, si vous avez configuré vos paramètres JMP pour utiliser plusieurs instances d'App Volumes Manager, même si vous sélectionnez un pool de postes de travail pour lequel Horizon Agent pointe vers l'une de ces instances d'App Volumes Manager, vous pouvez toujours sélectionner des AppStacks dans les autres instances d'App Volumes Manager configurées dans vos paramètres JMP. Toutefois, lorsque le pool de postes de travail est lancé, les AppStacks sélectionnées dans cette autre instance d'App Volumes Manager ne sont pas disponibles.

  Solution : aucune.

- Si une AppStack actuellement utilisée par une attribution JMP existante est renommée par l'utilisation d'App Volumes Manager ou par la modification de l'attribution JMP, la page de résumé des attributions JMP existantes ne se met pas à jour avec le nouveau nom de l'AppStack.

  Solution : aucune.

- Si vous disposez de deux instances d'Horizon 7 qui sont enregistrées avec la même instance de JMP Server et qui utilisent la même instance d'App Volumes Manager, la suppression d'une attribution JMP d'une instance d'Horizon 7 peut supprimer les attributions d'AppStacks utilisées par une autre attribution JMP dans l'autre instance d'Horizon 7.

  Solution : aucune.

- Lors de l'ajout ou de la modification d'informations d'Active Directory sur la page Paramètres JMP, l'opération échoue si la valeur entrée pour **Nom d'utilisateur de liaison** contient un ou plusieurs caractères d'une plage de 30 caractères chinois codés sur 3 octets, tels que le caractère « 试 », ce qui entraîne l'échec de l'authentification Active Directory.

  Solution : utilisez un autre nom d'utilisateur de liaison de votre Active Directory qui dispose de privilèges d'administration et qui ne contient aucun des 30 caractères chinois codés sur 3 octets, tels que le caractère « 试 ».

- Lors de l'ajout ou de la modification d'informations de l'instance App Volumes Manager sur la page Paramètres JMP, l'opération échoue si la valeur entrée pour **Nom d'utilisateur du compte de service** contient un ou plusieurs caractères d'une plage de 30 caractères chinois codés sur 3 octets, tels que le caractère « 试 », ce qui entraîne l'échec de l'authentification de l'instance d'App Volumes Manager.

  Solution : utilisez un autre nom d'utilisateur de liaison de votre instance d'App Volumes Manager qui dispose de privilèges d'administration et qui ne contient aucun des 30 caractères chinois codés sur 3 octets, tels que le caractère « 试 ».

- Les paramètres de mappage de lecteurs qui ont été mappés à l'aide de VMware Dynamic Environment Manager version 9.2.1 ne sont pas visibles lorsque le pool de postes de travail Windows 10 1703 est lancé.

  Solution : une fois que le pool de postes de travail Windows 10 1703 est lancé, exécutez la commande suivante.

  ```
  C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe -UemRefreshDrives
  ```

Consultez l'article https://kb.vmware.com/s/article/2113657 de la base de connaissances de VMware pour plus d'informations.

- Si vous accédez à Horizon Console à l'aide de localhost, le message d'erreur « Le JMP Server n'est pas accessible pour le moment. » s'affiche dans le volet Paramètres JMP d'Horizon Console.

  Solution : ouvrez Horizon Console à l'aide d'un nom de domaine complet uniquement, au lieu d'utiliser localhost.

- Lors de la création d'une attribution JMP, le message d'avertissement suivant peut s'afficher dans l'onglet **Applications** : « L'instance d'App Volumes associée au pool de postes de travail sélectionné ne correspond à aucune des instances d'App Volumes enregistrées. » Ce problème se produit lorsque l'une des conditions suivantes est vraie :

  - L'instance d'App Volumes Agent utilisée dans le pool de postes de travail a été installée avec une adresse IP plutôt qu'un nom de domaine complet.
  - L'instance d'App Volumes Agent utilisée dans le pool de postes de travail a été installée avec un nom de domaine complet, mais l'adresse IP de l'instance d'App Volumes Manager a été enregistrée dans les paramètres JMP à la place.

  Solution : réinstallez l'instance d'App Volumes Agent avec un nom de domaine complet et utilisez ce nom lors de l'inscription de l'instance d'App Volumes Manager dans l'onglet **Paramètres (JMP) > App Volumes**.

- Lors de l'installation de VMware Horizon JMP Server, le programme d'installation de JMP Server ne parvenait pas à continuer, car l'antivirus McAfee détectait NSSM.EXE comme une menace.

  Solution : ajoutez les fichiers suivants à la liste d'exclusion de l'antivirus McAfee avant de réinstaller JMP Server.

  C:\Program Files (x86)\VMware\JMP\nssm-2.24\nssm-2.24\win32\nssm.exe
  C:\Program Files (x86)\VMware\JMP\com\xmp\node_modules\winser\bin\nssm.exe

- Si vous avez sélectionné l'option **Autoriser le groupe d'administrateurs local** lors de l'installation d'Horizon Connection Server 7, ce qui crée un groupe BUILTIN\Administrators plutôt que <*domainName*>\Administrator, l'ajout des informations de JMP Server à l'aide d'Horizon Console échoue avec le message d'erreur « Privilèges Horizon insuffisants ».

  Solution : à l'aide d'Horizon Administrator, enregistrez <*domainName*>/Administrator avec un accès d'administrateur complet. Reconnectez-vous à Horizon Console et ajoutez les informations de JMP Server.

- Lorsque vous créez une attribution JMP et que vous survolez un pool de postes de travail d'Instant Clone, la valeur indiquée pour l'option Convertisseur 3D est **Désactivé** au lieu de **Gérer à l'aide de vSphere Client**.

  Solution : aucune.

- L'enregistrement de JMP Server échoue lorsque la portée du paramètre d'authentification de confiance est définie sur « Authentification sélective ».

  Solution : utilisez l'une des solutions suivantes pour résoudre ce problème.

  - Utilisez l'authentification à l'échelle du domaine.
  - Continuez à utiliser le paramètre de sécurité « Authentification sélective », mais octroyez explicitement l'autorisation « Autorisation d'authentifier » à tous les comptes d'hôte d'Horizon Connection Server (système local) sur tous les contrôleurs de domaine des objets ordinateur (ordinateurs ressource) qui résident dans le domaine ou la forêt de confiance. Pour plus d'informations sur la façon d'octroyer l'autorisation « Autorisation d'authentifier », consultez l'article de Microsoft Grant the Allowed to Authenticate permission on computers in the trusting domain or forest (Octroyer l'autorisation Autorisation d'authentifier sur des ordinateurs dans le domaine ou la forêt de confiance).

- Les attributions JMP ne fonctionnent pas comme prévu, car les informations à propos de l'instance d'App Volumes Manager utilisée par le pool de postes de travail et la version d'User Environment Manager utilisée par JMP Server n'ont pas pu être déterminées.

  Solution : lorsque vous configurez un pool de postes de travail, définissez la valeur **Nombre de machines en réserve (sous tension)** sur 1 ou plus dans la section Dimensionnement du pool de postes de travail du volet Paramètres de provisionnement. De plus, si vous avez sélectionné l'option **Provisionner des machines à la demande** dans la section Durée de provisionnement, définissez la valeur **Nombre min. de machines** sur 1 ou plus.

- Lorsque le fichier du programme d'installation de JMP Server 1.0.2.x est exécuté sur un hôte où JMP Server 1.0.0.516 est installé, le processus d'installation ne s'exécute pas.

  Solution : utilisez le panneau de configuration pour désinstaller JMP Server version 1.0.0.516. Exécutez le fichier d'installation pour JMP Server version 1.0.2.x et suivez l'assistant pour terminer l'installation. Fournissez les mêmes informations de base de données SQL Server pendant le processus d'installation afin de conserver toutes les données dont vous disposiez avec l'installation de JMP Server version 1.0.0.516.

- Dans les scénarios suivants, votre instance JMP Server devient inutilisable après une tentative de mise à niveau de votre installation actuelle à l'aide de la version 1.1.0.xxx du programme d'installation de JMP Server. La mise à niveau échoue et l'installation est annulée.

  - Le certificat de la base de données SQL Server est absent de votre installation JMP Server et la case **Activer SSL** est cochée lors de la mise à niveau.
  - La mise à niveau de JMP Server est effectuée à l'aide du mode de connexion Authentification Windows, mais aucun compte de connexion SQL Server n'a été créé pour le système hôte de JMP Server.
  - Vous avez annulé l'opération de mise à niveau en cliquant sur **Annuler**.

  Solution : recommencez la mise à niveau en exécutant à nouveau la version 1.1.0.xxx du programme d'installation de JMP Server. Vous devez ressaisir les mêmes informations de base de données SQL Server que vous aviez utilisées pour installer la version précédente de JMP Server. Après la mise à niveau, vérifiez que tous les certificats que vous avez configurés pour JMP Server sont toujours intacts. En fonction du moment où la défaillance de l'installation ou l'annulation est survenue, les certificats peuvent avoir été altérés.

- Lorsque vous tentez d'ajouter un partage de configuration Dynamic Environment Manager (DEM), le message d'erreur suivant peut s'afficher : **runOne] Error running file_share.createFileShare { code: 400,\n took: 221,\n data: {},\n error: 'Unable to create file share <fileshare-unc-path>.'**

  L'ajout d'un partage de configuration DEM échoue lorsque le mot de passe pour le partage de configuration DEM contient l'un des caractères suivants : “ #+,;<>=\~

  Solution : utilisez un autre mot de passe contenant l'un des caractères autorisés suivants : !$%&'()*-./:?@[]^_`{|}

Horizon Cloud Connector

- Lorsque vous utilisez vSphere Web Client basé sur HTML5 pour déployer le fichier OVA du dispositif virtuel Horizon Cloud Connector, l'erreur suivante se produit : « Valeur non valide 'false' spécifiée pour la propriété proxySsl. Échec du déploiement du module OVF. »
  Solution : utilisez vSphere Web Client basé sur Flex ou sur Flash pour déployer le fichier OVA du dispositif virtuel Horizon Cloud Connector.

- **Lorsque vous démarrez Horizon Cloud Connector, le message suivant s'affiche « [FAILED] Échec du démarrage d'attente de la configuration du réseau. Pour plus d'informations, consultez 'systemctl status systemd-networkd-wait-online.service' ».**
  Ce message s'affiche de manière incorrecte et n'indique pas un problème réel sur le réseau. Vous pouvez ignorer ce message et continuer à utiliser Horizon Cloud Connector comme d'habitude.