

Intégration d'Horizon 7

Modifié le 29 mai 2018
VMware Horizon 7 7.5



vmware®

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

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

N'hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l'adresse suivante :

docfeedback@vmware.com

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

VMware, Inc.
100-101 Quartier Boieldieu
92042 Paris La Défense
France
www.vmware.com/fr

Copyright © 2016–2018 VMware, Inc. Tous droits réservés. [Copyright et informations sur les marques.](#)

Table des matières

Intégration d' Horizon 7 5

1 Introduction à l'intégration de Horizon 7 6

Composants Horizon 7 6

Interfaces d'intégration à Horizon 7 7

2 Intégration de Horizon 7 à la base de données des événements 8

Tables et schémas de base de données des événements 8

Événements Horizon Connection Server 11

Événements Horizon Agent 18

Événements Horizon Administrator 18

Attributs de message d'événement 28

Exemples de requêtes et de vues de base de données 30

3 Déploiement d' Horizon 7 sur VMware Cloud on AWS 33

Scénarios de déploiement d' Horizon 7 sur VMware Cloud on AWS 34

Configuration du réseau pour Horizon 7 sur VMware Cloud on AWS 35

Configuration de VMware Cloud on AWS pour le déploiement d' Horizon 7 36

Configuration de la connexion et du pare-feu pour le déploiement d' Horizon 7 sur

VMware Cloud on AWS 36

Préparation d'Active Directory pour le déploiement d' Horizon 7 sur VMware Cloud on AWS 38

Environnements Horizon 7 sur VMware Cloud on AWS 38

Lier Horizon 7 sur VMware Cloud on AWS avec Horizon 7 sur site 39

Lier des espaces Horizon 7 sur VMware Cloud on AWS 40

Prise en main d'un déploiement de Cloud hybride pour Horizon 7 41

4 Personnalisation des données LDAP 42

Présentation des données de configuration LDAP 42

Modification des données de configuration LDAP 43

5 Examen des statistiques de session PCoIP avec WMI 50

Utilisation des statistiques de session PCoIP 50

Statistiques générales de session PCoIP 51

Statistiques audio PCoIP 52

Statistiques de création d'images PCoIP 53

Statistiques de réseau PCoIP 54

Statistiques PCoIP USB 56

Exemples d'utilisation de cmdlets PowerShell pour examiner les statistiques PCoIP 56

6	Définition de stratégies de poste de travail avec des scripts de démarrage de session	58
	Obtention de données d'entrée pour un script de démarrage de session	58
	Meilleures pratiques pour l'utilisation de scripts de démarrage de session	59
	Préparation d'un poste de travail Horizon 7 pour utiliser un script de démarrage de session	60
	Exemples de scripts de démarrage de session	62

Intégration d' Horizon 7

Le document *Intégration d'Horizon 7* décrit comment intégrer le logiciel Horizon 7™ à un logiciel tiers, tel que Windows PowerShell et des moteurs de création de rapport d'informatique décisionnelle.

Public cible

Ce document est destiné à toute personne souhaitant personnaliser ou intégrer un logiciel pour l'utiliser avec Horizon 7. Les informations de ce document sont destinées aux administrateurs Windows ou Linux expérimentés qui connaissent bien la technologie des machines virtuelles et les opérations de centres de données.

Introduction à l'intégration de Horizon 7

1

Horizon 7 permet aux administrateurs système de provisionner des postes de travail et de contrôler l'accès des utilisateurs à ces postes de travail. Le logiciel client connecte les utilisateurs à des machines virtuelles en cours d'exécution dans VMware vSphere™, ou à des systèmes physiques exécutés au sein de votre environnement réseau. En outre, les administrateurs de Horizon 7 peuvent configurer des hôtes des services Bureau à distance (RDS) pour fournir des sessions de poste de travail et d'application Horizon 7 aux périphériques clients.

Ce chapitre aborde les rubriques suivantes :

- [Composants Horizon 7](#)
- [Interfaces d'intégration à Horizon 7](#)

Composants Horizon 7

Vous pouvez utiliser Horizon 7 avec VMware vCenter Server pour créer des postes de travail à partir de machines virtuelles qui s'exécutent sur des hôtes VMware ESX® ou VMware ESXi™, puis déployer ces postes de travail vers les utilisateurs finaux. Vous pouvez également installer Horizon 7 sur les hôtes RDS pour déployer des postes de travail et des applications vers les utilisateurs finaux. Horizon 7 utilise votre infrastructure Active Directory existante pour l'authentification et la gestion des utilisateurs.

Après la création d'une application ou d'un poste de travail, les utilisateurs finaux autorisés peuvent utiliser un logiciel client installé localement ou sur le Web pour se connecter en toute sécurité à des machines virtuelles, des systèmes physiques principaux ou des hôtes RDS centralisés.

Horizon 7 comprend les composants principaux suivants.

Horizon Connection Server

Service logiciel qui agit comme un broker pour les connexions clientes en authentifiant et en dirigeant les demandes entrantes d'un utilisateur vers la machine virtuelle, le système physique ou l'hôte RDS adéquat.

Horizon Agent

Service logiciel qui est installé sur toutes les machines virtuelles, systèmes physiques ou hôtes RDS invités pour leur permettre d'être gérés par Horizon 7. Horizon Agent fournit des fonctionnalités telles que le contrôle des connexions, l'impression virtuelle, la prise en charge USB et l'authentification unique.

Horizon Client	Application logicielle qui communique avec le Serveur de connexion pour permettre aux utilisateurs de se connecter à leurs postes de travail.
Horizon Administrator	Application Web qui permet aux administrateurs d'Horizon 7 de configurer le Serveur de connexion, de déployer des pools de postes de travail et d'applications, de gérer des machines, de contrôler l'authentification des utilisateurs, d'initier et d'examiner des événements système et d'effectuer des activités analytiques.
vCenter Server	Serveur qui agit en tant qu'administrateur central pour les hôtes ESX/ESXi qui sont connectés sur un réseau. Une instance de vCenter Server centralise la configuration, le provisionnement et la gestion des machines virtuelles dans le centre de données.
View Composer	Service logiciel qui est installé sur une instance de vCenter Server pour permettre à Horizon 7 de déployer rapidement plusieurs postes de travail de clone lié à partir d'une image de base centrale unique.

Interfaces d'intégration à Horizon 7

Vous pouvez utiliser plusieurs interfaces pour intégrer Horizon 7 à des applications externes.

Base de données des événements	Vous pouvez configurer Horizon 7 pour enregistrer des événements dans une base de données Microsoft SQL Server ou Oracle. Vous pouvez ensuite utiliser des moteurs de création de rapport d'informatique décisionnelle pour accéder à cette base de données et l'analyser.
Lightweight Directory Access Protocol (LDAP)	Vous pouvez exporter et importer des données de configuration LDAP depuis et vers Horizon 7. Vous pouvez créer des scripts qui mettent à jour ces données de configuration sans accéder directement à Horizon Administrator.
Windows Management Instrumentation (WMI)	Vous pouvez examiner les statistiques de performances d'une session PCoIP.

Intégration de Horizon 7 à la base de données des événements

2

Vous pouvez configurer Horizon 7 pour enregistrer des événements dans une base de données Microsoft SQL Server ou Oracle. Horizon 7 enregistre les événements tels que les actions de l'utilisateur final, les actions de l'administrateur, les alertes qui indiquent des échecs et des erreurs du système, ainsi qu'un échantillonnage statistique.

L'utilisateur final peut journaliser et démarrer des sessions de postes de travail et d'applications. Les administrateurs peuvent ajouter des droits d'accès et créer des pools de postes de travail et d'applications. L'échantillonnage statistique consiste, par exemple, à enregistrer le nombre maximal d'utilisateurs sur une période de 24 heures.

Vous pouvez utiliser des moteurs de rapport de Business Intelligence tels que Crystal Reports, IBM Cognos, MicroStrategy 9 et Oracle Enterprise Performance Management System pour accéder à la base de données des événements et l'analyser.

Ce chapitre aborde les rubriques suivantes :

- [Tables et schémas de base de données des événements](#)
- [Événements Horizon Connection Server](#)
- [Événements Horizon Agent](#)
- [Événements Horizon Administrator](#)
- [Attributs de message d'événement](#)
- [Exemples de requêtes et de vues de base de données](#)

Tables et schémas de base de données des événements

Horizon 7 utilise des tables de base de données pour implémenter la base de données des événements. La base de données des événements ajoute aux noms de ces tables un préfixe que vous définissez lorsque vous configurez la base de données.

Tables de base de données des événements

Le tableau suivant répertorie les tables de base de données qui implémentent la base de données des événements dans Horizon 7.

Tableau 2-1. Tables de base de données des événements

Nom de la table	Description
event	Métadonnées et données d'optimisation de recherche des événements récents.
event_data	Valeurs des données des événements récents.
event_data_historical	Valeurs des données de tous les événements.
event_historical	Métadonnées et données d'optimisation de recherche de tous les événements.

Horizon 7 enregistre les informations détaillées des événements pour toutes les tables de base de données. Après un certain temps à la suite de l'écriture d'un enregistrement d'événement, Horizon 7 supprime l'enregistrement des tables event et event_data. Vous pouvez utiliser Horizon Administrator pour configurer la période durant laquelle la base de données conserve un enregistrement dans les tables event et event_data.

Important Horizon 7 ne limite pas la croissance des tables event_historical et event_data_historical. Vous devez implémenter une stratégie de gestion de l'espace pour ces tables.

Une clé primaire unique, EventID, identifie chaque événement que Horizon 7 enregistre dans les tables event et event_historical. Horizon 7 enregistre les valeurs des données de chaque événement dans les tables event_data et event_data_historical. Vous pouvez obtenir l'ensemble des informations pour un événement en joignant les tables event et event_data ou les tables event_historical et event_data_historical dans la colonne EventID.

Les colonnes EventType, Severity et Time des tables event et event_historical identifient le type et la gravité d'un événement, ainsi que l'heure à laquelle il s'est produit.

Pour plus d'informations sur la configuration de la base de données des événements, consultez le document *Installation d'Horizon 7*.

Remarque Pour vider les données des tableaux historiques, reportez-vous à l'article <http://kb.vmware.com/kb/2150309>.

Schémas de la base de données des événements

Le tableau suivant indique le schéma des tables de base de données event et event_historical.

Tableau 2-2. Schéma des tables event et event_historical

Nom de la colonne	Type de données Oracle	Type de données SQL Server	Description
Acknowledged	SMALLINT	tinyint	Indique si Horizon 7 a reconnu l'événement. <ul style="list-style-type: none"> 0 = false 1 = true
DesktopId	NVARCHAR2(512)	nvarchar(512)	ID de poste de travail du pool associé.
EventID	NOMBRE ENTIER	int	Clé primaire unique de l'événement.

Tableau 2-2. Schéma des tables event et event_historical (suite)

Nom de la colonne	Type de données Oracle	Type de données SQL Server	Description
EventType	NVARCHAR2(512)	nvarchar(512)	Nom de l'événement qui correspond à un élément dans le catalogue de messages. Par exemple, BROKER_USERLOGGEDIN.
FolderPath	NVARCHAR2(512)	nvarchar(512)	Chemin d'accès complet du dossier qui contient l'objet associé.
GroupId	NVARCHAR2(512)	nvarchar(512)	SID du groupe associé dans Active Directory.
LUNId	NVARCHAR2(512)	nvarchar(512)	ID du LUN qui stocke les objets associés.
MachineId	NVARCHAR2(512)	nvarchar(512)	ID de la machine virtuelle ou physique associée.
Module	NVARCHAR2(512)	nvarchar(512)	Composant Horizon 7 qui a déclenché l'événement. Par exemple, Admin, Broker, Tunnel, Framework, Client ou Agent.
ModuleAndEventText	NVARCHAR2(512)	nvarchar(512)	Message d'événement dont les valeurs sont remplacées par les paramètres d'attribut.
Node	NVARCHAR2(512)	nvarchar(512)	Nom du nœud du périphérique virtuel.
Gravité	NVARCHAR2(512)	nvarchar(512)	Niveau de gravité. Par exemple, INFO, WARNING, ERROR, AUDIT_SUCCESS, AUDIT_FAIL.
Source	NVARCHAR2(512)	nvarchar(512)	Identifiant de la source de l'événement.
ThinAppId	NVARCHAR2(512)	nvarchar(512)	ID de l'objet ThinApp™ associé.
Heure	TIMESTAMP	datetime	Heure à laquelle l'événement s'est produit, mesurée depuis l'époque (1er janvier 1970).
UserDiskPathId	NVARCHAR2(512)	nvarchar(512)	ID de disque de l'utilisateur.
UserSID	NVARCHAR2(512)	nvarchar(512)	SID de l'utilisateur associé dans Active Directory.

Le tableau suivant indique le schéma des tables de base de données event_data et event_data_historical.

Tableau 2-3. Schéma des tables event_data et event_data_historical

Nom de la colonne	Type de données Oracle	Type de données SQL Server	Description
BooleanValue	SMALLINT	tinyint	Valeur d'un attribut booléen. ■ 0 = false ■ 1 = true
EventID	NOMBRE ENTIER	int	Clé primaire unique de l'événement.
IntValue	NOMBRE ENTIER	int	Valeur d'un attribut de nombre entier.

Tableau 2-3. Schéma des tables event_data et event_data_historical (suite)

Nom de la colonne	Type de données Oracle	Type de données SQL Server	Description
Nom	NVARCHAR2(512)	nvarchar(512)	Nom d'attribut (par exemple, UserDisplayName).
StrValue	NVARCHAR2(512)	nvarchar(512)	Valeur d'un attribut de chaîne. Pour d'autres types d'attributs, cette colonne contient une interprétation du type de données sous forme de chaîne.
TimeValue	TIMESTAMP	datetime	Valeur d'un attribut de date et heure.
Type	SMALLINT	tinyint	Type de données de l'attribut. <ul style="list-style-type: none"> 0 = StrValue 1 = IntValue 2 = TimeValue 3 = BooleanValue

Événements Horizon Connection Server

Les événements du Horizon Connection Server signalent des informations relatives au Serveur de connexion, telles que les sessions de poste de travail et d'application, les échecs d'authentification d'utilisateur et les erreurs de provisionnement.

L'événement `BROKER_DAILY_MAX_DESKTOP_SESSIONS` signale le nombre maximal de sessions de poste de travail simultanées sur une période de 24 heures. Si un utilisateur exécute plusieurs sessions de poste de travail simultanément, chaque session de poste de travail est comptée séparément.

L'événement `BROKER_DAILY_MAX_APP_USERS` signale le nombre maximal d'utilisateurs d'application simultanés pendant une période de 24 heures. Un utilisateur qui exécute plusieurs applications simultanément n'est compté qu'une seule fois. Il est possible que les sessions de courte durée ne soient pas comptées, car l'échantillonnage s'effectue toutes les cinq minutes.

Les événements `BROKER_VC_DISABLED` et `BROKER_VC_ENABLED` signalent l'état du pilote vCenter que Horizon 7 utilise pour effectuer le suivi d'une instance de vCenter Server.

Les événements `BROKER_VC_STATUS_*` signalent l'état d'une instance de vCenter Server.

Le tableau suivant répertorie tous les types d'événements du Serveur de connexion.

Tableau 2-4. Événements du Serveur de connexion

Type d'événement	Gravité	ModuleAndEventText
<code>BROKER_AGENT_OFFLINE</code>	AVERTISSEMENT	L'agent exécuté sur la machine \${MachineName} n'a pas répondu aux requêtes, il est donc marqué comme hors ligne
<code>BROKER_AGENT_ONLINE</code>	AVERTISSEMENT	L'agent exécuté sur la machine \${MachineName} répond de nouveau, mais il n'a pas envoyé un message de démarrage

Tableau 2-4. Événements du Serveur de connexion (suite)

Type d'événement	Gravité	ModuleAndEventText
BROKER_APPLICATION_LAUNCH_FAILURE	ERREUR	Impossible de démarrer depuis le pool \${PoolId} pour l'utilisateur \${UserDisplayName} : le broker a rencontré une erreur lors du traitement de la demande. Contactez le support pour obtenir de l'aide
BROKER_APPLICATION_MISSING	AVERTISSEMENT	Au moins \${ApplicationMissingCount} applications, notamment \${ApplicationExecutable}, ne sont pas installées sur \${MachineName} dans le pool \${PoolId}
BROKER_APPLICATION_NOT_ENTITLED	AUDIT_FAIL	Impossible de démarrer depuis le pool \${PoolId} pour l'utilisateur \${UserDisplayName} : l'utilisateur n'est pas autorisé sur ce pool
BROKER_APPLICATION_PROTOCOL_NOT_SUPPORTED	AUDIT_FAIL	Impossible de démarrer depuis le pool \${PoolId} pour l'utilisateur \${UserDisplayName} : le protocole demandé \${ProtocolId} n'est pas pris en charge
BROKER_APPLICATION_REQUEST	INFO	L'utilisateur \${UserDisplayName} a demandé l'application \${ApplicationId}
BROKER_APPLICATION_SESSION_REQUEST	INFO	L'utilisateur \${UserDisplayName} a demandé une session d'application depuis le pool \${PoolId}
BROKER_DAILY_MAX_DESKTOP_SESSIONS	INFO	\${Time} : au cours des dernières 24 heures, le nombre maximal de sessions de poste de travail simultanées était de \${UserCount}
BROKER_DAILY_MAX_APP_USERS	INFO	\${Time} : au cours des dernières 24 heures, le nombre maximal d'utilisateurs impliqués dans des sessions d'application simultanées était de \${UserCount}
BROKER_DESKTOP_LAUNCH_FAILURE	ERREUR	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : le broker a rencontré une erreur lors du traitement de la demande, contactez le support pour obtenir de l'aide
BROKER_DESKTOP_NOT_ENTITLED	AUDIT_FAIL	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : l'utilisateur n'est pas autorisé sur ce pool
BROKER_DESKTOP_PROTOCOL_NOT_SUPPORTED	AUDIT_FAIL	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : le protocole demandé \${ProtocolId} n'est pas pris en charge
BROKER_DESKTOP_REQUEST	INFO	L'utilisateur \${UserDisplayName} a demandé le pool \${DesktopId}
BROKER_EVENT_HANDLING_STARTED	INFO	Le broker \${BrokerName} a démarré la gestion d'événements
BROKER_EVENT_HANDLING_STOPPED	INFO	\${BrokerName} a arrêté de gérer les événements
BROKER_MACHINE_ALLOCATED	INFO	L'utilisateur \${UserDisplayName} a demandé le pool \${DesktopId}, la machine allouée \${MachineName}
BROKER_MACHINE_ASSIGNED_UNAVAILABLE	AUDIT_FAIL	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : la machine attribuée \${MachineName} n'est pas disponible

Tableau 2-4. Événements du Serveur de connexion (suite)

Type d'événement	Gravité	ModuleAndEventText
BROKER_MACHINE_CANNOT_CONNECT	AUDIT_FAIL	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : échec de la connexion à la machine \${MachineName} à l'aide de \${ProtocolId}
BROKER_MACHINE_CONFIGURED_VIDEO_SETTINGS	INFO	Paramètres vidéo correctement configurés pour la machine virtuelle \${MachineName} dans le pool \${DesktopId}
BROKER_MACHINE_NOT_READY	AVERTISSEMENT	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : la machine \${MachineName} n'est pas prête à accepter les connexions
BROKER_MACHINE_OPERATION_DELETED	INFO	La machine \${MachineName} a été supprimée
BROKER_MACHINE_PROTOCOL_NOT_SUPPORTED	AUDIT_FAIL	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : la machine \${MachineName} ne prend pas en charge le protocole \${ProtocolId}
BROKER_MACHINE_PROTOCOL_UNAVAILABLE	AUDIT_FAIL	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : la machine \${MachineName} n'a pas signalé que le protocole \${ProtocolId} était prêt
BROKER_MACHINE_REJECTED_SESSION	AVERTISSEMENT	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : la machine \${MachineName} a rejeté la demande de session de démarrage
BROKER_MACHINE_SESSION_TIMEOUT	AVERTISSEMENT	La session de l'utilisateur \${UserDisplayName} a expiré
BROKER_MULTIPLE_DESKTOPS_FOR_KIOSK_USER	AVERTISSEMENT	L'utilisateur \${UserDisplayName} est autorisé sur plusieurs pools de postes de travail
BROKER_POOL_CANNOT_ASSIGN	AUDIT_FAIL	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : aucune machine à affecter à l'utilisateur n'est disponible
BROKER_POOL_COMANAGER_REQUIRED	AUDIT_FAIL	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : aucune cogestion n'est disponible pour le protocole \${ProtocolId}
BROKER_POOL_EMPTY	AUDIT_FAIL	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : le pool de postes de travail est vide
BROKER_POOL_NO_MACHINE_ASSIGNED	AUDIT_FAIL	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : aucune machine n'est attribuée à cet utilisateur
BROKER_POOL_NO_RESPONSES	AUDIT_FAIL	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : aucune machine du pool de postes de travail ne répond

Tableau 2-4. Événements du Serveur de connexion (suite)

Type d'événement	Gravité	ModuleAndEventText
BROKER_POOL_OVERLOADED	AUDIT_FAIL	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : toutes les machines réactives sont occupées
BROKER_POOL_POLICY_VIOLATION	AUDIT_FAIL	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : le pool de postes de travail n'autorise pas les sessions en ligne
BROKER_POOL_PROTOCOL_NOT_SUPPORTED	AUDIT_FAIL	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : les machines disponibles ne prennent pas en charge le protocole \${ProtocolId}
BROKER_POOL_PROTOCOL_UNAVAILABLE	AUDIT_FAIL	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : aucune machine disponible n'a signalé que le protocole \${ProtocolId} était prêt
BROKER_POOL_TUNNEL_NOT_SUPPORTED	AUDIT_FAIL	Impossible de démarrer depuis le pool \${DesktopId} pour l'utilisateur \${UserDisplayName} : la tunnellation n'est pas prise en charge pour le protocole \${ProtocolId}
BROKER_PROVISIONING_ERROR_CONFIG_CLEARED	INFO	Le problème de configuration signalé précédemment n'est plus présent sur le pool \${DesktopId}
BROKER_PROVISIONING_ERROR_CONFIG_SET	ERREUR	Une erreur de provisionnement s'est produite sur le pool \${DesktopId} en raison d'un problème de configuration
BROKER_PROVISIONING_ERROR_DISK_CLEARED	INFO	Le problème de disque signalé précédemment n'est plus présent sur le pool \${DesktopId}
BROKER_PROVISIONING_ERROR_DISK_LC_RESERVATION_CLEARED	INFO	L'erreur signalée précédemment, en raison d'un espace disque disponible réservé pour les clones liés, n'est plus présente sur le pool \${DesktopId}
BROKER_PROVISIONING_ERROR_DISK_LC_RESERVATION_SET	ERREUR	Une erreur de provisionnement s'est produite sur le pool \${DesktopId}, car l'espace disque disponible est réservé pour les clones liés
BROKER_PROVISIONING_ERROR_DISK_SET	AVERTISSEMENT	Une erreur de provisionnement s'est produite sur le pool \${DesktopId} en raison d'un problème de disque
BROKER_PROVISIONING_ERROR_LICENSE_CLEARED	INFO	Le problème de licence signalé précédemment n'est plus présent sur le pool \${DesktopId}
BROKER_PROVISIONING_ERROR_LICENSE_SET	ERREUR	Une erreur de provisionnement s'est produite sur le pool \${DesktopId} en raison d'un problème de licence
BROKER_PROVISIONING_ERROR_NETWORKING_CLEARED	INFO	Les problèmes de réseau d'Horizon Agent signalés précédemment ne sont plus présents sur le pool \${DesktopId}
BROKER_PROVISIONING_ERROR_NETWORKING_SET	ERREUR	Une erreur de provisionnement s'est produite sur le pool \${DesktopId} en raison d'un problème de mise en réseau d'Horizon Agent

Tableau 2-4. Événements du Serveur de connexion (suite)

Type d'événement	Gravité	ModuleAndEventText
BROKER_PROVISIONING_ERROR_RESOURCED_CLEARED	INFO	Le problème de ressource signalé précédemment n'est plus présent sur le pool \${DesktopId}
BROKER_PROVISIONING_ERROR_RESOURCE_SET	ERREUR	Une erreur de provisionnement s'est produite sur le pool \${DesktopId} en raison d'un problème de ressource
BROKER_PROVISIONING_ERROR_TIMEOUT_CUSTOMIZATION_CLEARED	INFO	Le délai d'expiration signalé pendant la personnalisation n'est plus présent sur le pool \${DesktopId}
BROKER_PROVISIONING_ERROR_TIMEOUT_CUSTOMIZATION_SET	ERREUR	Une erreur de provisionnement s'est produite sur le pool \${DesktopId} en raison d'un délai d'expiration lors d'une personnalisation
BROKER_PROVISIONING_ERROR_VM_CLONING	ERREUR	Une erreur d'approvisionnement s'est produite pour la machine \${MachineName} : échec du clonage pour la machine
BROKER_PROVISIONING_ERROR_VM_CUSTOMIZATION_ERROR	ERREUR	Une erreur d'approvisionnement s'est produite pour la machine \${MachineName} : l'opération de personnalisation a expiré
BROKER_PROVISIONING_ERROR_VM_CUSTOMIZATION_NETWORKING	ERREUR	Une erreur de provisionnement s'est produite pour la machine \${MachineName} : il s'agit d'une erreur de personnalisation provoquée par une absence de communication réseau entre Horizon Agent et le Serveur de connexion
BROKER_PROVISIONING_ERROR_VM_CUSTOMIZATION_TIMEOUT	ERREUR	Une erreur d'approvisionnement s'est produite pour la machine \${MachineName} : l'opération de personnalisation a expiré
BROKER_PROVISIONING_SVI_ERROR_COMPOSER_AGENT_INIT_FAILED	ERREUR	Une erreur d'approvisionnement s'est produite pour la machine \${MachineName} : échec de l'initialisation de View Composer Agent
BROKER_PROVISIONING_SVI_ERROR_RECONFIG_FAILED	ERREUR	Une erreur d'approvisionnement s'est produite pour la machine \${MachineName} : échec de l'opération de reconfiguration
BROKER_PROVISIONING_SVI_ERROR_REFIT_FAILED	ERREUR	Une erreur d'approvisionnement s'est produite pour la machine \${MachineName} : échec de l'opération d'adaptation \${SVIOperation}
BROKER_PROVISIONING_SVI_ERROR_REMOVING_VM	ERREUR	Une erreur d'approvisionnement s'est produite pour la machine \${MachineName} : impossible de supprimer la machine de l'inventaire
BROKER_PROVISIONING_VERIFICATION_FAILED_USER_ASSIGNED	AVERTISSEMENT	Échec de la vérification du provisionnement pour la machine \${MachineName} : l'utilisateur est déjà attribué à une machine dans le pool \${DesktopId}
BROKER_PROVISIONING_VERIFICATION_FAILED_USER_CANNOT_BE_ASSIGNED	AVERTISSEMENT	Échec de la vérification du provisionnement pour la machine \${MachineName} : impossible d'attribuer un utilisateur, car le pool \${DesktopId} n'est pas persistant

Tableau 2-4. Événements du Serveur de connexion (suite)

Type d'événement	Gravité	ModuleAndEventText
BROKER_PROVISIONING_VERIFICATION_FAILED_VMNAME_IN_USE	AVERTISSEMENT	Échec de la vérification du provisionnement pour la machine \${MachineName} : une machine du pool \${DesktopId} porte déjà le nom \${MachineName}
BROKER_SECURITY_SERVER_ADD_FAILED	AUDIT_FAIL	Échec de l'ajout du serveur de sécurité \${SecurityServerId}
BROKER_SECURITY_SERVER_ADD_FAILED_PASSWORD_EXPIRED	AUDIT_FAIL	Échec de l'ajout du serveur de sécurité \${SecurityServerId}, mot de passe de couplage expiré
BROKER_SECURITY_SERVER_ADD_FAILED_PASSWORD_INCORRECT	AUDIT_FAIL	Échec de l'ajout du serveur de sécurité \${SecurityServerId}, mot de passe de couplage incorrect
BROKER_SECURITY_SERVER_ADD_FAILED_PASSWORD_NOT_SET	AUDIT_FAIL	Échec de l'ajout du serveur de sécurité \${SecurityServerId}, mot de passe de couplage non défini
BROKER_SECURITY_SERVER_ADDED	AUDIT_SUCCESS	Serveur de sécurité \${SecurityServerId} ajouté
BROKER_SVI_ARCHIVE_UDD_FAILED	AUDIT_FAIL	Échec de l'archivage du disque de données utilisateur \${UserDiskName} à l'emplacement \${SVIPath}
BROKER_SVI_ARCHIVE_UDD_SUCCEEDED	AUDIT_SUCCESS	Disque de données utilisateur \${UserDiskName} archivé à l'emplacement \${SVIPath}
BROKER_SVI_ATTACH_UDD_FAILED	AUDIT_FAIL	Échec de l'association du disque de données utilisateur \${UserDiskName} à la machine virtuelle \${SVIVMID}
BROKER_SVI_ATTACH_UDD_SUCCEEDED	AUDIT_SUCCESS	Disque de données utilisateur \${UserDiskName} associé à la machine virtuelle \${SVIVMID}
BROKER_SVI_DETACH_UDD_FAILED	AUDIT_FAIL	Échec du détachement du disque de données utilisateur \${UserDiskName} de la machine virtuelle \${SVIVMID}
BROKER_SVI_DETACH_UDD_SUCCEEDED	AUDIT_SUCCESS	Disque de données utilisateur \${UserDiskName} détaché de la machine virtuelle \${SVIVMID}
BROKER_USER_AUTHFAILED_ACCOUNT_DISABLED	AUDIT_FAIL	L'utilisateur \${UserDisplayName} n'a pas pu s'authentifier car le compte est désactivé
BROKER_USER_AUTHFAILED_ACCOUNT_EXPIRED	AUDIT_FAIL	L'utilisateur \${UserDisplayName} n'a pas pu s'authentifier car le compte a expiré
BROKER_USER_AUTHFAILED_ACCOUNT_LOCKED_OUT	AUDIT_FAIL	L'utilisateur \${UserDisplayName} n'a pas pu s'authentifier car le compte est verrouillé
BROKER_USER_AUTHFAILED_ACCOUNT_RESTRICTION	AUDIT_FAIL	L'utilisateur \${UserDisplayName} n'a pas pu s'authentifier en raison d'une restriction de compte
BROKER_USER_AUTHFAILED_BAD_USER_PASSWORD	AUDIT_FAIL	L'utilisateur \${UserDisplayName} n'a pas pu s'authentifier en raison d'un nom d'utilisateur ou d'un mot de passe incorrect
BROKER_USER_AUTHFAILED_GENERAL	AUDIT_FAIL	L'utilisateur \${UserDisplayName} n'a pas pu s'authentifier

Tableau 2-4. Événements du Serveur de connexion (suite)

Type d'événement	Gravité	ModuleAndEventText
BROKER_USER_AUTHFAILED_NO_LOGON_SERVERS	AUDIT_FAIL	L'utilisateur \${UserDisplayName} n'a pas pu s'authentifier car il n'y a pas de serveurs d'ouverture de session
BROKER_USER_AUTHFAILED_PASSWORD_EXPIRED	AUDIT_FAIL	L'utilisateur \${UserDisplayName} n'a pas pu s'authentifier car le mot de passe a expiré
BROKER_USER_AUTHFAILED_PASSWORD_MUST_CHANGE	AUDIT_FAIL	L'utilisateur \${UserDisplayName} n'a pas pu s'authentifier car le mot de passe doit être modifié
BROKER_USER_AUTHFAILED_SECUREID_ACCESS_DENIED	AUDIT_FAIL	Accès SecurID refusé pour l'utilisateur \${UserDisplayName}
BROKER_USER_AUTHFAILED_SECUREID_NEWPIN_REJECTED	AUDIT_FAIL	Accès SecurID refusé pour l'utilisateur \${UserDisplayName} car le nouveau code PIN a été rejeté
BROKER_USER_AUTHFAILED_SECUREID_WRONG_NEXTTOKEN	AUDIT_FAIL	Accès SecurID refusé pour l'utilisateur \${UserDisplayName} en raison de la saisie du mauvais jeton suivant
BROKER_USER_AUTHFAILED_SECUREID_WRONG_STATE	AUDIT_FAIL	Accès SecurID refusé pour l'utilisateur \${UserDisplayName} en raison d'un état incorrect
BROKER_USER_AUTHFAILED_TIME_RESTRICTION	AUDIT_FAIL	L'utilisateur \${UserDisplayName} n'a pas pu s'authentifier en raison d'une restriction de temps
BROKER_USER_NOT_AUTHORIZED	AUDIT_FAIL	L'utilisateur \${UserDisplayName} s'est authentifié, mais il n'est pas autorisé à effectuer l'opération
BROKER_USER_NOT_ENTITLED	AUDIT_FAIL	L'utilisateur \${UserDisplayName} s'est authentifié, mais il n'est autorisé sur aucun pool
BROKER_USERCHANGEDPASSWORD	AUDIT_SUCCESS	Le mot de passe de \${UserDisplayName} a été modifié par l'utilisateur
BROKER_USERLOGGEDIN	AUDIT_SUCCESS	L'utilisateur \${UserDisplayName} a ouvert une session
BROKER_USERLOGGEDOUT	AUDIT_SUCCESS	L'utilisateur \${UserDisplayName} a fermé une session
BROKER_VC_DISABLED	INFO	vCenter à l'adresse \${VCAddress} a été temporairement désactivé
BROKER_VC_ENABLED	INFO	vCenter à l'adresse \${VCAddress} a été activé
BROKER_VC_STATUS_CHANGED_CANNOT_LOGIN	AVERTISSEMENT	Impossible de se connecter à vCenter à l'adresse \${VCAddress}
BROKER_VC_STATUS_CHANGED_DOWN	INFO	vCenter à l'adresse \${VCAddress} est inactif
BROKER_VC_STATUS_CHANGED_INVALID_CREDENTIALS	AVERTISSEMENT	vCenter à l'adresse \${VCAddress} a des informations d'authentification non valides
BROKER_VC_STATUS_CHANGED_NOT_YET_CONNECTED	INFO	Pas encore connecté à vCenter à l'adresse \${VCAddress}
BROKER_VC_STATUS_CHANGED_RECONNECTING	INFO	Reconnexion à vCenter à l'adresse \${VCAddress}

Tableau 2-4. Événements du Serveur de connexion (suite)

Type d'événement	Gravité	ModuleAndEventText
BROKER_VC_STATUS_CHANGED_UNKNO WN	AVERTISSEMENT	L'état de vCenter à l'adresse \${VCAddress} est inconnu
BROKER_VC_STATUS_CHANGED_UP	INFO	vCenter à l'adresse \${VCAddress} est actif

Événements Horizon Agent

Les événements Horizon Agent signalent des informations relatives à Horizon Agent, comme les utilisateurs qui se sont connectés à une machine spécifique ou s'en sont déconnectés, si Horizon Agent s'est arrêté sur une machine spécifique et si Horizon Agent a envoyé un message de démarrage à partir d'une machine spécifique au Horizon Connection Server.

Tableau 2-5. Événements Horizon Agent

Type d'événement	Gravité	ModuleAndEventText
AGENT_CONNECTED	INFO	L'utilisateur \${UserDisplayName} a ouvert une nouvelle session sur la machine \${MachineName}
AGENT_DISCONNECTED	INFO	L'utilisateur \${UserDisplayName} s'est déconnecté de la machine \${MachineName}
AGENT_ENDED	INFO	L'utilisateur \${UserDisplayName} a fermé une session sur la machine \${MachineName}
AGENT_PENDING	INFO	L'agent exécuté sur la machine \${MachineName} a accepté une session allouée pour l'utilisateur \${UserDisplayName}
AGENT_PENDING_EXPIRED	AVERTISSEMENT	La session en attente sur la machine \${MachineName} pour l'utilisateur \${UserDisplayName} a expiré
AGENT_RECONFIGURED	INFO	La machine \${MachineName} a bien été reconfigurée
AGENT_RECONNECTED	INFO	L'utilisateur \${UserDisplayName} s'est reconnecté à la machine \${MachineName}
AGENT_RESUME	INFO	L'agent sur la machine \${MachineName} a envoyé un message de reprise
AGENT_SHUTDOWN	INFO	L'agent exécuté sur la machine \${MachineName} s'est arrêté, cette machine sera indisponible
AGENT_STARTUP	INFO	L'agent exécuté sur la machine \${MachineName} a contacté le serveur de connexion et a envoyé un message de démarrage
AGENT_SUSPEND	INFO	L'agent sur la machine \${MachineName} a envoyé un message d'interruption

Événements Horizon Administrator

Les événements Horizon Administrator signalent des informations sur les actions que les utilisateurs lancent dans Horizon Administrator.

Tableau 2-6. Événements Horizon Administrator

EventType	Gravité	ModuleAndEventText
ADMIN_ADD_DESKTOP_ENTITLEMENT	AUDIT_SUCCESS	\${EntitlementDisplay} était autorisé sur le pool \${DesktopId} par \${UserDisplayName}
ADMIN_ADD_LICENSE	AUDIT_SUCCESS	\${UserDisplayName} a ajouté une licence
ADMIN_ADD_LICENSE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu ajouter une licence
ADMIN_ADD_PM	AUDIT_SUCCESS	\${UserDisplayName} a ajouté la machine physique \${MachineName} au pool \${DesktopId}
ADMIN_ADD_PM_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu ajouter la machine physique \${MachineName} au pool \${DesktopId}
ADMIN_ADD_THINAPP_ENTITLEMENT	AUDIT_SUCCESS	L'application \${ThinAppDisplayName} a été attribuée au poste de travail \${MachineName} par \${UserDisplayName}
ADMIN_ADD_THINAPP_ENTITLEMENT_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu ajouter une autorisation d'application
ADMIN_ADD_THINAPP_POOL_ENTITLEMENT	AUDIT_SUCCESS	L'application \${ThinAppDisplayName} a été attribuée au pool \${DesktopId} par \${UserDisplayName}
ADMIN_ADMINISTRATOR_REMOVE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu supprimer toutes les autorisations pour l'administrateur \${AdminPermissionEntity}
ADMIN_ADMINISTRATOR_REMOVED	AUDIT_SUCCESS	\${UserDisplayName} a supprimé toutes les autorisations pour l'administrateur \${AdminPermissionEntity}
ADMIN_CONNECTION_BROKER_UPDATE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu mettre à jour le broker de connexion \${BrokerId}
ADMIN_CONNECTION_BROKER_UPDATED	AUDIT_SUCCESS	\${UserDisplayName} a mis à jour du broker de connexion \${BrokerId} : (\${AttrChangeType} : \${AttrName} = \${AttrValue})
ADMIN_CONNECTION_SERVER_BACKUP_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu lancer une sauvegarde du broker de connexion \${BrokerId}
ADMIN_CONNECTION_SERVER_BACKUP_INITIATED	AUDIT_SUCCESS	\${UserDisplayName} a lancé une sauvegarde du broker de connexion \${BrokerId}
ADMIN_CONNECTION_SERVER_DISABLE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu désactiver le broker de connexion \${BrokerId}

Tableau 2-6. Événements Horizon Administrator (suite)

EventType	Gravité	ModuleAndEventText
ADMIN_CONNECTION_SERVER_DISABLED	AUDIT_SUCCESS	\${UserDisplayName} désactive le broker de connexion \${BrokerId}
ADMIN_CONNECTION_SERVER_ENABLE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu activer le broker de connexion \${BrokerId}
ADMIN_CONNECTION_SERVER_ENABLED	AUDIT_SUCCESS	\${UserDisplayName} active le broker de connexion \${BrokerId}
ADMIN_DATABASE_CONFIGURATION_ADD_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu ajouter la configuration de base de données
ADMIN_DATABASE_CONFIGURATION_ADDED	AUDIT_SUCCESS	\${UserDisplayName} a ajouté la configuration de base de données
ADMIN_DATABASE_CONFIGURATION_DELETE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu supprimer la configuration de base de données
ADMIN_DATABASE_CONFIGURATION_DELETE_FAILED	AUDIT_SUCCESS	\${UserDisplayName} a supprimé la configuration de base de données
ADMIN_DATABASE_CONFIGURATION_UPDATE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu mettre à jour la configuration de base de données
ADMIN_DATABASE_CONFIGURATION_UPDATED	AUDIT_SUCCESS	\${UserDisplayName} a mis à jour la configuration de base de données
ADMIN_DEFAULT_DESKTOPPOOL_ASSIGN	AUDIT_SUCCESS	\${UserDisplayName} a attribué le pool \${DesktopId} pour le poste de travail par défaut à \${UserName}
ADMIN_DEFAULT_DESKTOPPOOL_ASSIGN_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu attribuer le pool \${DesktopId} pour le poste de travail par défaut à \${UserName}
ADMIN_DEFAULT_DESKTOPPOOL_UNASSIGN	AUDIT_SUCCESS	\${UserDisplayName} a supprimé l'attribution de pool pour le poste de travail par défaut à \${UserName}
ADMIN_DEFAULT_DESKTOPPOOL_UNASSIGN_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu supprimer l'attribution de pool pour le poste de travail par défaut à \${UserName}
ADMIN_DESKTOP_ADDED	AUDIT_SUCCESS	\${UserDisplayName} a ajouté le pool \${DesktopId}
ADMIN_DESKTOP_ASSIGN	AUDIT_SUCCESS	\${UserDisplayName} a attribué le poste de travail \${MachineName} à \${UserName}
ADMIN_DESKTOP_ASSIGN_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu attribuer le poste de travail \${MachineName} à \${UserName}
ADMIN_DESKTOP_EDITED	AUDIT_SUCCESS	\${UserDisplayName} a modifié le pool \${DesktopId} (\${AttrChangeType}) : \${AttrName} = \${AttrValue}

Tableau 2-6. Événements Horizon Administrator (suite)

EventType	Gravité	ModuleAndEventText
ADMIN_DESKTOP_MAINTENANCE_MODE_UPDATE_FAILED	AUDIT_FAIL	\$(UserDisplayName) n'a pas pu mettre à jour le poste de travail \${MachineName} sur le mode de maintenance \${MaintenanceMode}
ADMIN_DESKTOP_MAINTENANCE_MODE_UPDATED	AUDIT_SUCCESS	\$(UserDisplayName) a mis à jour le poste de travail \${MachineName} sur le mode de maintenance \${MaintenanceMode}
ADMIN_DESKTOP_UNASSIGN	AUDIT_SUCCESS	\$(UserDisplayName) a supprimé l'attribution pour le poste de travail \${MachineName}
ADMIN_DESKTOP_UNASSIGN_FAILED	AUDIT_FAIL	\$(UserDisplayName) n'a pas pu supprimer l'attribution pour le poste de travail \${MachineName}
ADMIN_ENABLE_DESKTOP_FAILED	AUDIT_FAIL	\$(UserDisplayName) n'a pas pu définir le pool \${DesktopId} sur \${EnableStatus}
ADMIN_ENABLE_DESKTOP_SUCCEEDED	AUDIT_SUCCESS	\$(UserDisplayName) a défini le pool \${DesktopId} sur \${EnableStatus}
ADMIN_ENABLED_DESKTOP_PROVISION_FAILED	AUDIT_FAIL	\$(UserDisplayName) n'a pas pu définir le provisionnement du pool \${DesktopId} sur \${EnableStatus}
ADMIN_ENABLED_DESKTOP_PROVISION_SUCCEEDED	AUDIT_SUCCESS	\$(UserDisplayName) a défini le provisionnement du pool \${DesktopId} sur \${EnableStatus}
ADMIN_EVENT_CONFIGURATION_UPDATE_FAILED	AUDIT_FAIL	\$(UserDisplayName) n'a pas pu mettre à jour la configuration d'événements
ADMIN_EVENT_CONFIGURATION_UPDATED	AUDIT_SUCCESS	\$(UserDisplayName) a mis à jour la configuration générale
ADMIN_FOLDER_ADD_FAILED	AUDIT_FAIL	\$(UserDisplayName) n'a pas pu ajouter le dossier \${AdminFolderName}
ADMIN_FOLDER_ADDED	AUDIT_SUCCESS	\$(UserDisplayName) a ajouté le dossier \${AdminFolderName}
ADMIN_FOLDER_CHANGE_FAILED	AUDIT_FAIL	\$(UserDisplayName) n'a pas pu modifier l'objet \${ObjectID}(type=\${ObjectType}) sur le dossier \${AdminFolderName}
ADMIN_FOLDER_CHANGED	AUDIT_SUCCESS	\$(UserDisplayName) a modifié l'objet \${ObjectID}(type=\${ObjectType}) sur le dossier \${AdminFolderName}
ADMIN_FOLDER_DELETE_FAILED	AUDIT_FAIL	\$(UserDisplayName) n'a pas pu supprimer le dossier \${AdminFolderName}
ADMIN_FOLDER_DELETED	AUDIT_SUCCESS	\$(UserDisplayName) a supprimé le dossier \${AdminFolderName}

Tableau 2-6. Événements Horizon Administrator (suite)

EventType	Gravité	ModuleAndEventText
ADMIN_GLOBAL_CONFIGURATION_UPDATE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu mettre à jour la configuration générale
ADMIN_GLOBAL_CONFIGURATION_UPDATED	AUDIT_SUCCESS	\${UserDisplayName} a mis à jour la configuration générale (\$ {AttrChangeType} : \${AttrName} = \$ {AttrValue})
ADMIN_GLOBAL_POLICY_UPDATE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu mettre à jour des stratégies générales
ADMIN_GLOBAL_POLICY_UPDATED	AUDIT_SUCCESS	\${UserDisplayName} a mis à jour la stratégie générale (\$ {AttrChangeType} : \${AttrName} = \$ {AttrValue})
ADMIN_PERFMON_CONFIGURATION_UPDATE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu mettre à jour la configuration de contrôle des performances
ADMIN_PERFMON_CONFIGURATION_UPDATED	AUDIT_SUCCESS	\${UserDisplayName} a mis à jour la configuration de contrôle des performances
ADMIN_PERMISSION_ADD_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu ajouter une autorisation à \$ {AdminPermissionEntity} avec le rôle \$ {AdminRoleName} sur le dossier \$ {AdminFolderName}
ADMIN_PERMISSION_ADDED	AUDIT_SUCCESS	\${UserDisplayName} a ajouté une autorisation à \$ {AdminPermissionEntity} avec le rôle \$ {AdminRoleName} sur le dossier \$ {AdminFolderName}
ADMIN_PERMISSION_REMOVE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu supprimer une autorisation à \$ {AdminPermissionEntity} avec le rôle \$ {AdminRoleName} sur le dossier \$ {AdminFolderName}
ADMIN_PERMISSION_REMOVED	AUDIT_SUCCESS	\${UserDisplayName} a supprimé une autorisation à \$ {AdminPermissionEntity} avec le rôle \$ {AdminRoleName} sur le dossier \$ {AdminFolderName}
ADMIN_POOL_POLICY_UPDATE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu mettre à jour des stratégies de pool \${DesktopId}
ADMIN_POOL_POLICY_UPDATED	AUDIT_SUCCESS	\${UserDisplayName} a mis à jour la stratégie de pool \${DesktopId} (\$ {AttrChangeType} : \${AttrName} = \$ {AttrValue})
ADMIN_REMOVE_DESKTOP_ENTITLEMENT	AUDIT_SUCCESS	\${EntitlementDisplay} était non autorisé sur le pool \${DesktopId} par \$ {UserDisplayName}

Tableau 2-6. Événements Horizon Administrator (suite)

EventType	Gravité	ModuleAndEventText
ADMIN_REMOVE_DESKTOP_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu supprimer le pool \${DesktopId}
ADMIN_REMOVE_DESKTOP_SUCCEEDED	AUDIT_SUCCESS	\${UserDisplayName} a supprimé le pool \${DesktopId}
ADMIN_REMOVE_THINAPP_ENTITLEMENT	AUDIT_SUCCESS	L'attribution de l'application \$ {ThinAppDisplayName} a été supprimée du poste de travail \${MachineName} par \${UserDisplayName}
ADMIN_REMOVE_THINAPP_ENTITLEMENT_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu supprimer une autorisation d'application
ADMIN_REMOVE_THINAPP_POOL_ENTITLEMENT	AUDIT_SUCCESS	L'attribution de l'application \$ {ThinAppDisplayName} a été supprimée du pool \${DesktopId} par \$ {UserDisplayName}
ADMIN_RESET_THINAPP_STATE	AUDIT_SUCCESS	L'état de l'application \$ {ThinAppDisplayName} est réinitialisé pour le poste de travail \$ {DesktopDisplayName} par \$ {UserDisplayName}
ADMIN_RESET_THINAPP_STATE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu réinitialiser l'état de l'application \$ {ThinAppDisplayName}
ADMIN_ROLE_ADD_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu ajouter le rôle \${AdminRoleName} avec les privilèges \${AdminPrivilegeName}
ADMIN_ROLE_ADDED	AUDIT_SUCCESS	\${UserDisplayName} a ajouté le rôle \$ {AdminRoleName} avec les privilèges \$ {AdminPrivilegeName}
ADMIN_ROLE_PRIV_UPDATE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu mettre à jour le rôle \${AdminRoleName} avec les privilèges \${AdminPrivilegeName}
ADMIN_ROLE_PRIV_UPDATED	AUDIT_SUCCESS	\${UserDisplayName} a mis à jour le rôle \${AdminRoleName} avec les privilèges \$ {AdminPrivilegeName}
ADMIN_ROLE_REMOVE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu supprimer le rôle \${AdminRoleName}
ADMIN_ROLE_REMOVED	AUDIT_SUCCESS	\${UserDisplayName} a supprimé le rôle \${AdminRoleName}
ADMIN_ROLE_RENAME_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu renommer le rôle \${AdminRoleName} par \${AdminRoleNewName}
ADMIN_ROLE_RENAMED	AUDIT_SUCCESS	\${UserDisplayName} a renommé le rôle \${AdminRoleName} par \$ {AdminRoleNewName}

Tableau 2-6. Événements Horizon Administrator (suite)

EventType	Gravité	ModuleAndEventText
ADMIN_SECURITY_SERVER_ADD_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu ajouter un serveur de sécurité \$ {SecurityServerId}
ADMIN_SECURITY_SERVER_ADDED	AUDIT_SUCCESS	\${UserDisplayName} a ajouté un serveur de sécurité \$ {SecurityServerId}
ADMIN_SECURITY_SERVER_EDIT_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu modifier un serveur de sécurité \$ {SecurityServerId}
ADMIN_SECURITY_SERVER_EDITED	AUDIT_SUCCESS	\${UserDisplayName} a modifié un serveur de sécurité \$ {SecurityServerId} (\$ {AttrChangeType} : \$ {AttrName} = \$ {AttrValue})
ADMIN_SECURITY_SERVER_REMOVE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu supprimer un serveur de sécurité \$ {SecurityServerId}
ADMIN_SECURITY_SERVER_REMOVED	AUDIT_SUCCESS	\${UserDisplayName} a supprimé un serveur de sécurité \$ {SecurityServerId}
ADMIN_SESSION_SENDMSG	AUDIT_SUCCESS	\${UserDisplayName} a envoyé un message (\$ {SessionMessage}) à la session (utilisateur \$ {UserName}, poste de travail \$ {MachineName})
ADMIN_SESSION_SENDMSG_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu envoyer de message (\$ {SessionMessage}) à la session \$ {ObjectId}
ADMIN_SVI_ADD_DEPLOYMENT_GROUP_FAILED	AUDIT_FAIL	Échec de l'ajout du groupe de déploiement pour \$ {SVIParentVM} : \$ {SVISnapshot}
ADMIN_SVI_ADD_DEPLOYMENT_GROUP_SUCCEEDED	AUDIT_SUCCESS	Groupe de déploiement ajouté \$ {SVIDeploymentGroupID} pour \$ {SVIParentVM} : \$ {SVISnapshot}
ADMIN_SVI_ADD_UDD_FAILED	AUDIT_FAIL	Échec de l'ajout du disque de données utilisateur \$ {UserDiskName}
ADMIN_SVI_ADD_UDD_SUCCEEDED	AUDIT_SUCCESS	Disque de données utilisateur ajouté \$ {UserDiskName}
ADMIN_SVI_ADMIN_ADDED	AUDIT_SUCCESS	\${UserDisplayName} a ajouté un domaine QuickPrep SVI \$ {SVIAdminFqdn}(\$ {SVIAdminName})
ADMIN_SVI_ADMIN_REMOVED	AUDIT_SUCCESS	\${UserDisplayName} a supprimé le domaine QuickPrep SVI (id=\$ {SVIAdminID})
ADMIN_SVI_ADMIN_UPDATED	AUDIT_SUCCESS	\${UserDisplayName} a mis à jour le domaine QuickPrep SVI \$ {SVIAdminFqdn}(\$ {SVIAdminName})

Tableau 2-6. Événements Horizon Administrator (suite)

EventType	Gravité	ModuleAndEventText
ADMIN_SVI_ATTACH_UDD_FAILED	AUDIT_FAIL	Échec de la demande d'association du disque de données utilisateur \$ {UserDiskName} à la VM \$ {SVIVMID}
ADMIN_SVI_ATTACH_UDD_SUCCEEDED	AUDIT_SUCCESS	Association demandée du disque de données utilisateur \$ {UserDiskName} à la VM \$ {SVIVMID}
ADMIN_SVI_DELETE_UDD_FAILED	AUDIT_FAIL	Échec de la suppression du disque de données utilisateur \$ {UserDiskName}
ADMIN_SVI_DELETE_UDD_SUCCEEDED	AUDIT_SUCCESS	Disque de données utilisateur supprimé \$ {UserDiskName}
ADMIN_SVI_DETACH_UDD_FAILED	AUDIT_FAIL	Échec de la demande de détachement du disque de données utilisateur \$ {UserDiskName} de la VM \$ {SVIVMID}
ADMIN_SVI_DETACH_UDD_SUCCEEDED	AUDIT_SUCCESS	Détachement demandé du disque de données utilisateur \$ {UserDiskName} de la VM \$ {SVIVMID}
ADMIN_SVI_REBALANCE_VM_FAILED	AUDIT_FAIL	Échec du rééquilibrage de la VM \$ {SVIVMID}
ADMIN_SVI_REBALANCE_VM_SUCCEEDED	AUDIT_SUCCESS	VM rééquilibrée \$ {SVIVMID}
ADMIN_SVI_REFRESH_VM_FAILED	AUDIT_FAIL	Échec de l'actualisation de la machine virtuelle \$ {SVIVMID}
ADMIN_SVI_REFRESH_VM_SUCCEEDED	AUDIT_SUCCESS	VM actualisée \$ {SVIVMID}
ADMIN_SVI_RESYNC_VM_FAILED	AUDIT_FAIL	Échec de la resynchronisation de la machine virtuelle \$ {SVIVMID} pour le groupe de déploiement \$ {SVIDeploymentGroupID}
ADMIN_SVI_RESYNC_VM_SUCCEEDED	AUDIT_SUCCESS	Machine virtuelle resynchronisée \$ {SVIVMID} pour le groupe de déploiement \$ {SVIDeploymentGroupID}
ADMIN_SVI_UPDATE_POOL_DEPLOYMENT_GROUP_FAILED	AUDIT_FAIL	Échec de la mise à jour du pool \$ {DesktopID} pour le groupe de déploiement \$ {SVIDeploymentGroupID}
ADMIN_SVI_UPDATE_POOL_DEPLOYMENT_GROUP_SUCCEEDED	AUDIT_SUCCESS	Mise à jour du pool \$ {DesktopID} pour le groupe de déploiement \$ {SVIDeploymentGroupID}
ADMIN_SVI_UPDATE_UDD_FAILED	AUDIT_FAIL	Échec de la mise à jour du disque de données utilisateur \$ {UserDiskName}
ADMIN_SVI_UPDATE_UDD_SUCCEEDED	AUDIT_SUCCESS	Définir le disque de données utilisateur \$ {UserDiskName} sur le pool \$ {DesktopID} et l'utilisateur sur \$ {UserName}
ADMIN_THINAPP_ADD_FAILED	AUDIT_FAIL	\$ {UserDisplayName} n'a pas pu ajouter l'application \$ {ThinAppDisplayName}

Tableau 2-6. Événements Horizon Administrator (suite)

EventType	Gravité	ModuleAndEventText
ADMIN_THINAPP_ADDED	AUDIT_SUCCESS	\${UserDisplayName} a ajouté l'application \${ThinAppDisplayName}
ADMIN_THINAPP_DESKTOP_AVAILABLE	AUDIT_SUCCESS	L'application \${ThinAppDisplayName} est maintenant disponible sur le poste de travail \${DesktopDisplayName}
ADMIN_THINAPP_DESKTOP_REMOVED	AUDIT_SUCCESS	L'application \${ThinAppDisplayName} a été supprimée du poste de travail \${DesktopDisplayName}
ADMIN_THINAPP_EDITED	AUDIT_SUCCESS	\${UserDisplayName} a modifié l'application \${ThinAppDisplayName}
ADMIN_THINAPP_FAILED_DESKTOP_DELIVERY	AUDIT_FAIL	Échec de la livraison de l'application \${ThinAppDisplayName} au poste de travail \${DesktopDisplayName}
ADMIN_THINAPP_FAILED_DESKTOP_REMOVAL	AUDIT_FAIL	Échec de la suppression de l'application \${ThinAppDisplayName} du poste de travail \${DesktopDisplayName}
ADMIN_THINAPP_GROUP_ADD_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu ajouter le modèle d'application \${ThinAppGroupName}
ADMIN_THINAPP_GROUP_ADDED	AUDIT_SUCCESS	\${UserDisplayName} a ajouté le modèle d'application \${ThinAppGroupName} avec les applications \${ThinAppGroupApplications}
ADMIN_THINAPP_GROUP_EDIT_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu modifier le modèle d'application \${ThinAppGroupName}
ADMIN_THINAPP_GROUP_EDITED	AUDIT_SUCCESS	\${UserDisplayName} a modifié le modèle d'application \${ThinAppGroupName} avec les applications \${ThinAppGroupApplications}
ADMIN_THINAPP_GROUP_REMOVE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu supprimer le modèle d'application \${ThinAppGroupName}
ADMIN_THINAPP_GROUP_REMOVED	AUDIT_SUCCESS	\${UserDisplayName} a supprimé le modèle d'application \${ThinAppGroupName}
ADMIN_THINAPP_REMOVE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu supprimer l'application \${ThinAppDisplayName}
ADMIN_THINAPP_REMOVED	AUDIT_SUCCESS	\${UserDisplayName} a supprimé l'application \${ThinAppDisplayName}

Tableau 2-6. Événements Horizon Administrator (suite)

EventType	Gravité	ModuleAndEventText
ADMIN_THINAPP_REPO_ADD_FAILED	AUDIT_FAIL	\$(UserDisplayName) n'a pas pu ajouter le référentiel \${ThinAppRepositoryName}, le chemin \${ThinAppRepositoryPath}
ADMIN_THINAPP_REPO_ADDED	AUDIT_SUCCESS	\$(UserDisplayName) a ajouté le référentiel \${ThinAppRepositoryName}, le chemin \${ThinAppRepositoryPath}
ADMIN_THINAPP_REPO_EDIT_FAILED	AUDIT_FAIL	\$(UserDisplayName) n'a pas pu modifier le référentiel \${ThinAppRepositoryName}, le chemin \${ThinAppRepositoryPath}
ADMIN_THINAPP_REPO_EDITED	AUDIT_SUCCESS	\$(UserDisplayName) a modifié le référentiel \${ThinAppRepositoryName}, le chemin \${ThinAppRepositoryPath}
ADMIN_THINAPP_REPO_REMOVED	AUDIT_SUCCESS	\$(UserDisplayName) a supprimé le référentiel \${ThinAppRepositoryName}
ADMIN_UNREGISTER_PM	AUDIT_SUCCESS	\$(UserDisplayName) a annulé l'inscription de la machine physique \${MachineName}
ADMIN_UNREGISTER_PM_FAILED	AUDIT_FAIL	\$(UserDisplayName) ne parvient pas à annuler l'inscription de la machine physique \${MachineName}
ADMIN_USER_INFO_UPDATE_FAILED	AUDIT_FAIL	\$(UserDisplayName) n'a pas pu mettre à jour les informations utilisateur avec le serveur AD pour \${UserName}
ADMIN_USER_INFO_UPDATED	AUDIT_SUCCESS	\$(UserDisplayName) a mis à jour les informations utilisateur avec le serveur AD pour \${UserName}
ADMIN_USER_POLICY_DELETE_FAILED	AUDIT_FAIL	\$(UserDisplayName) n'a pas pu supprimer la stratégie de remplacement du pool \${DesktopId} pour l'utilisateur \${UserName}
ADMIN_USER_POLICY_DELETED	AUDIT_SUCCESS	\$(UserDisplayName) a supprimé la stratégie de remplacement du pool \${DesktopId} pour l'utilisateur \${UserName} (\${AttrChangeType}) : \${AttrName} = \${AttrValue})
ADMIN_USER_POLICY_UPDATE_FAILED	AUDIT_FAIL	\$(UserDisplayName) n'a pas pu mettre à jour des stratégies de pool \${DesktopId} pour l'utilisateur \${UserName}
ADMIN_USER_POLICY_UPDATED	AUDIT_SUCCESS	\$(UserDisplayName) a mis à jour la stratégie de pool \${DesktopId} pour l'utilisateur \${UserName} (\${AttrChangeType}) : \${AttrName} = \${AttrValue})

Tableau 2-6. Événements Horizon Administrator (suite)

EventType	Gravité	ModuleAndEventText
ADMIN_USERLOGGEDIN	AUDIT_SUCCESS	L'utilisateur \${UserDisplayName} a ouvert une session sur View Administrator
ADMIN_USERLOGGEDOUT	AUDIT_SUCCESS	L'utilisateur \${UserDisplayName} a fermé une session sur View Administrator
ADMIN_VC_ADD_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu ajouter le serveur VC \${VCAddress}
ADMIN_VC_ADDED	AUDIT_SUCCESS	\${UserDisplayName} a ajouté un serveur VC \${VCAddress}
ADMIN_VC_EDITED	AUDIT_SUCCESS	\${UserDisplayName} a modifié un serveur VC \${VCAddress} (\${AttrChangeType} : \${AttrName} = \${AttrValue})
ADMIN_VC_LICINV_ALARM_DISABLED	AUDIT_SUCCESS	Une alarme sur le serveur VC \${VCAddress} pour le contrôle d'inventaire de licence a été désactivée, car tous les hôtes disposent de licences de poste de travail
ADMIN_VC_REMOVE_FAILED	AUDIT_FAIL	\${UserDisplayName} n'a pas pu supprimer le serveur VC \${VCAddress}
ADMIN_VC_REMOVED	AUDIT_SUCCESS	\${UserDisplayName} a supprimé un serveur VC \${VCAddress}

Attributs de message d'événement

Les messages ModuleAndEventText utilisent certains attributs. Pour déterminer le type de données d'un attribut, vous pouvez examiner sa valeur dans la colonne type dans la table event_data ou event_data_historical.

Tableau 2-7. Attributs utilisés par les messages ModuleAndEventText

Nom d'attribut	Description
AdminFolderName	Nom d'un dossier qui requiert un accès privilégié.
AdminPermissionEntity	Nom d'un objet qui requiert un accès privilégié.
AdminPrivilegeName	Nom d'un privilège administratif.
AdminRoleName	Nom d'un rôle d'administrateur.
AdminRoleNewName	Nouveau nom d'un rôle d'administrateur.
AttrChangeType	Type de modification qui a été appliquée à un attribut générique.
AttrName	Nom d'un attribut générique.
AttrValue	Valeur d'un attribut générique.
BrokerId	Identifiant d'une instance du Serveur de connexion.

Tableau 2-7. Attributs utilisés par les messages ModuleAndEventText (suite)

Nom d'attribut	Description
BrokerName	Nom d'une instance du Serveur de connexion.
DesktopDisplayName	Nom d'affichage d'un pool de postes de travail.
DesktopId	Identificateur d'un pool de postes de travail.
EntitlementDisplay	Nom d'affichage d'un droit de poste de travail.
MachineId	Nom d'une machine virtuelle ou physique.
MachineName	Nom d'une machine virtuelle ou physique.
MaintenanceMode	État du mode de maintenance.
ObjectId	Identifiant d'un objet d'inventaire.
ObjectType	Type d'un objet d'inventaire.
PolicyDisplayName	Nom d'affichage d'une stratégie.
PolicyObject	Identifiant d'un objet de stratégie.
PolicyValue	Valeur d'un objet de stratégie.
ProtocolId	Identifiant d'un protocole d'affichage.
SecurityServerId	Identifiant d'un serveur de sécurité.
SVIAdminFqdn	Nom de domaine complet (FQDN) d'un domaine QuickPrep.
SVIAdminID	Identifiant d'un domaine QuickPrep.
SVIAdminName	Nom d'un domaine QuickPrep.
SVIDeploymentGroupId	Identifiant d'un groupe de déploiement de View Composer.
SVIOperation	Nom d'une opération View Composer.
SVIParentVM	Machine virtuelle parente dans View Composer.
SVIPath	Chemin d'accès d'un objet dans View Composer.
SVISnapshot	Snapshot dans View Composer.
SVIVMID	Identifiant d'une machine virtuelle dans View Composer.
ThinAppDisplayName	Nom d'affichage d'un objet ThinApp.
ThinAppId	Identifiant d'un objet ThinApp.
ThinAppRepositoryName	Nom d'un référentiel ThinApp
ThinAppRepositoryPath	Chemin d'accès d'un référentiel ThinApp.
Heure	Valeur de date et heure.
UserCount	Nombre maximal d'utilisateurs de postes de travail sur une période de 24 heures.
UserDiskName	Nom d'un disque de données utilisateur.
UserDisplayName	Nom d'utilisateur au format DOMAINE\Nom_utilisateur.
UserName	Nom d'un utilisateur dans Active Directory.
VCAddress	URL d'une instance de vCenter Server.

Exemples de requêtes et de vues de base de données

Vous pouvez interroger la base de données event_historical pour afficher les événements d'erreur et d'avertissement, ainsi que des événements récents spécifiques.

Remarque Remplacez le préfixe dbo.VE_ dans les exemples suivants par le préfixe approprié pour votre base de données des événements.

Répertorier les événements d'erreur

La requête suivante affiche tous les événements d'erreur de la table event_historical.

```
CREATE VIEW error_events AS
(
  SELECT ev.EventID, ev.Time, ev.Module, ev.EventType, ev.ModuleAndEventText
    FROM dbo.VE_event_historical AS ev
   WHERE ev.Severity = 'ERROR'
);
```

Répertorier les événements d'avertissement

La requête suivante affiche tous les événements d'avertissement de la table event_historical.

```
CREATE VIEW warning_events AS
(
  SELECT ev.EventID, ev.Time, ev.Module, ev.EventType, ev.ModuleAndEventText
    FROM dbo.VE_event_historical AS ev
   WHERE ev.Severity = 'WARNING'
);
```

Répertorier les événements récents

La requête suivante répertorie tous les événements récents qui sont associés à l'utilisateur Fred dans le domaine MYDOM.

```
CREATE VIEW user_fred_events AS
(
  SELECT ev.EventID, ev.Time, ev.Module, ev.EventType, ev.Severity, ev.Acknowledged
    FROM dbo.VE_event_historical AS ev,
         dbo.VE_event_data_historical AS ed
   WHERE ev.EventID = ed.EventID AND ed.Name = 'UserDisplayName' AND ed.StrValue =
         'MYDOM\Fred'
);
```

La requête suivante répertorie tous les événements récents où l'agent sur une machine est arrêté.

```
CREATE VIEW agent_shutdown_events AS
(
  SELECT ev.EventID, ev.Time, ed.StrValue
    FROM dbo.VE_event_historical AS ev,
         dbo.VE_event_data_historical AS ed
   WHERE ev.EventID = ed.EventID AND ev.EventType = 'AGENT_SHUTDOWN' AND
         ed.Name = 'MachineName'
);
```

La requête suivante répertorie tous les événements récents où un poste de travail n'a pas pu se lancer, car le pool de postes de travail était vide.

```
CREATE VIEW desktop_launch_failure_events AS
(
  SELECT ev.EventID, ev.Time, ed1.StrValue, ed2.StrValue
    FROM dbo.VE_event_historical AS ev,
         dbo.VE_event_data_historical AS ed1,
         dbo.VE_event_data_historical AS ed2
   WHERE ev.EventID = ed1.EventID AND ev.EventID = ed2.EventID AND
         ev.EventType = 'BROKER_POOL_EMPTY' AND
         ed1.Name = 'UserDisplayName' AND ed2.Name = 'DesktopId'
);
```

La requête suivante répertorie tous les événements récents où un administrateur a supprimé un pool de postes de travail.

```
CREATE VIEW desktop_pool_removed_events AS
(
  SELECT ev.EventID, ev.Time, ed1.StrValue, ed2.StrValue
    FROM dbo.VE_event_historical AS ev,
         dbo.VE_event_data_historical AS ed1,
         dbo.VE_event_data_historical AS ed2
   WHERE ev.EventID = ed1.EventID AND ev.EventID = ed2.EventID AND
         ev.EventType = 'ADMIN_DESKTOP_REMOVED' AND
         ed1.Name = 'UserDisplayName' AND ed2.Name = 'DesktopId'
);
```

La requête suivante répertorie tous les événements récents où un administrateur a ajouté un référentiel ThinApp.

```
CREATE VIEW thinapp_repository_added_events AS
(
  SELECT ev.EventID, ev.Time, ed1.StrValue, ed2.StrValue, ed3.StrValue
    FROM dbo.VE_event_historical AS ev,
         dbo.VE_event_data_historical AS ed1,
         dbo.VE_event_data_historical AS ed2,
         dbo.VE_event_data_historical AS ed3
   WHERE ev.EventID = ed1.EventID AND ev.EventID = ed2.EventID AND ev.EventID = ed3.EventID
  AND
```

```
ev.EventType = 'ADMIN_THINAPP_REPO_ADDED' AND  
ed1.Name = 'UserDisplayName' AND ed2.Name = 'ThinAppRepositoryName' AND  
ed3.Name = 'ThinAppRepositoryPath'  
);
```


Déploiement d' Horizon 7 sur VMware Cloud on AWS

3

Vous pouvez déployer Horizon 7 sur VMware Cloud on AWS afin de mettre à l'échelle des postes de travail et des applications Horizon 7 sur une plate-forme Cloud élastique.

VMware Cloud on AWS vous permet de créer des centres de données vSphere sur Amazon Web Services. Ces centres de données vSphere intègrent vCenter Server pour gérer votre centre de données, vSAN pour le stockage et VMware NSX pour la mise en réseau. Vous pouvez connecter un centre de données sur site à votre SDDC (Software-Defined Data Center) de Cloud et gérer les deux à partir d'une interface vSphere Client unique. À l'aide de votre compte AWS connecté, vous pouvez accéder à des services AWS, tels qu'EC2 et S3, à partir des machines virtuelles dans votre SDDC. Pour plus d'informations, consultez la documentation d'VMware Cloud on AWS à l'adresse <https://docs.vmware.com/fr/VMware-Cloud-on-AWS/index.html>.

En option, vous pouvez également utiliser la fonctionnalité Architecture Cloud Pod dans Horizon 7 pour connecter un espace à partir d'un centre de données sur site à un espace dans un centre de données déployé sur VMware Cloud on AWS. Vous pouvez utiliser Horizon 7 comme une plate-forme sécurisée et adaptée à l'entreprise pour les postes de travail virtuels, les postes de travail publiés et les applications que vous pouvez déployer et gérer sur site. Vous pouvez utiliser la fonctionnalité Architecture Cloud Pod pour la mise à l'échelle sur plusieurs espaces et sites pour la gestion fédérée à grande échelle dans des centres de données qui sont à la fois sur site et dans des Clouds privés.

Vous pouvez déployer Horizon 7 sur un environnement de Cloud hybride lorsque vous étirez Architecture Cloud Pod sur des centres de données sur site et des instances de VMware Cloud on AWS. Cela permet aux utilisateurs d'Horizon 7 d'externaliser la gestion de l'infrastructure SDDC sur la plate-forme VMware Cloud. Comme l'architecture Horizon 7 est la même sur site et dans VMware Cloud on AWS, l'expérience de gestion et de déploiement reste la même sur site et dans le Cloud privé. Il n'est pas nécessaire d'acheter un nouveau matériel et vous pouvez utiliser l'option de paiement à l'utilisation pour une facturation horaire sur VMware Cloud on AWS.

Les fonctionnalités suivantes d'Horizon 7 sont prises en charge pour un déploiement d'Horizon 7 sur VMware Cloud on AWS :

- Pools automatisés avec des machines virtuelles complètes
- Batteries de serveurs manuelles d'hôte RDS
- Dispositifs Unified Access Gateway

Les fonctionnalités suivantes ne sont pas prises en charge pour un déploiement d'Horizon 7 sur VMware Cloud on AWS :

- Pools de postes de travail de clone lié
- Pools de postes de travail de clone instantané
- Pools de postes de travail manuels
- Batteries de serveurs d'hôte RDS de clone lié
- Batteries de serveurs d'hôte RDS de clone instantané
- CBRC (Content-Based Read Cache)
- Serveur de sécurité
- Postes de travail non gérés
- Horizon Persona Management
- VMware ThinApp
- Sécurité basée sur la virtualisation (VBS)
- Terminaux vTPM (Trusted Platform Module)

Ce chapitre aborde les rubriques suivantes :

- [Scénarios de déploiement d'Horizon 7 sur VMware Cloud on AWS](#)
- [Configuration du réseau pour Horizon 7 sur VMware Cloud on AWS](#)
- [Configuration de VMware Cloud on AWS pour le déploiement d'Horizon 7](#)
- [Configuration de la connexion et du pare-feu pour le déploiement d'Horizon 7 sur VMware Cloud on AWS](#)
- [Préparation d'Active Directory pour le déploiement d'Horizon 7 sur VMware Cloud on AWS](#)
- [Environnements Horizon 7 sur VMware Cloud on AWS](#)
- [Lier Horizon 7 sur VMware Cloud on AWS avec Horizon 7 sur site](#)
- [Lier des espaces Horizon 7 sur VMware Cloud on AWS](#)
- [Prise en main d'un déploiement de Cloud hybride pour Horizon 7](#)

Scénarios de déploiement d' Horizon 7 sur VMware Cloud on AWS

Vous pouvez déployer Horizon 7 sur VMware Cloud on AWS pour les scénarios suivants.

Extension et rafales du centre de données

Utilisez ce scénario si vous disposez d'une infrastructure Horizon 7 sur site existante et que vous devez augmenter la capacité, mais ne souhaitez pas acheter de matériel supplémentaire. En étendant le déploiement d'Horizon 7 à VMware Cloud on AWS, vous pouvez utiliser la capacité de

Cloud et toujours gérer des déploiements sur site et de Cloud privé dans un seul espace fédéré. Vous pouvez également utiliser la plate-forme de Cloud afin de fournir une capacité temporaire pour les fournisseurs et les travailleurs saisonniers. Le déploiement sur site est facultatif. Selon vos besoins, vous pouvez décider de consolider et de déplacer tout le déploiement sur site vers VMware Cloud on AWS.

Localité des applications

Utilisez ce scénario lorsque vous souhaitez déplacer des applications publiées sensibles à la latence vers VMware Cloud on AWS et que vous voulez que les postes de travail virtuels et les hôtes RDS soient colocalisés avec vos applications publiées. Vous pouvez également disposer d'autres applications publiées qui sont toujours sur site. Lorsque vous étendez votre déploiement d'Horizon 7 à VMware Cloud on AWS, vous pouvez permettre aux utilisateurs finaux de se connecter au poste de travail virtuel ou à l'hôte RDS le plus proche pour lancer l'application, qu'elle se trouve sur site ou sur VMware Cloud on AWS.

Récupération d'urgence et continuité d'activité

Utilisez ce scénario si vous souhaitez créer une infrastructure de récupération d'urgence. La création d'une infrastructure de récupération d'urgence sur site peut être coûteuse. Lorsque vous utilisez VMware Cloud on AWS, vous payez pour l'utilisation de l'infrastructure de récupération d'urgence pendant les heures d'inactivité de l'infrastructure principale ou lorsque vous avez besoin d'un petit pilote lors des opérations normales pour un objectif de temps de récupération (RTO) rapide pendant un événement d'urgence. Le fait de disposer d'une architecture Horizon 7 unifiée sur le site principal sur site et le site de récupération d'urgence sur VMware Cloud on AWS simplifie le processus de basculement. De plus, lorsque vous utilisez la fonctionnalité Architecture Cloud Pod pour déployer Horizon 7 sur plusieurs instances de VMware Cloud on AWS, la haute disponibilité est présente sur plusieurs nœuds de Cloud.

Configuration du réseau pour Horizon 7 sur VMware Cloud on AWS

Pour configurer un déploiement de Cloud hybride, vous devez configurer le réseau logique qui peut prendre en charge un déploiement d'Horizon 7 sur VMware Cloud on AWS.

Incluez les composants suivants dans la configuration du réseau logique.

Composant de gestion

Le composant de gestion pour le réseau inclut vCenter Server.

Composant de calcul

Le composant de calcul pour le réseau inclut les composants suivants :

- Dispositifs Unified Access Gateway
- Équilibrage de charge

- Serveurs de connexion Horizon
- Machines virtuelles

Composants NSX

Les composants NSX dans le réseau fournissent une sécurité de périphérie de réseau et des services de passerelle pour isoler un réseau virtualisé et configurer des règles de pare-feu. Lorsque vous utilisez des composants NSX, vous ne pouvez pas disposer de plus de 1 000 ports.

- Routeur logique distribué (DLR) NSX
- NSX Edge
- VPN IPSec

Composants sur site

Les composants sur site incluent les connexions d'Horizon Client et les connexions de poste de travail virtuel ou publié et d'application à partir d'Internet.

Configuration de VMware Cloud on AWS pour le déploiement d' Horizon 7

Vous devez créer une instance SDDC sur VMware Cloud on AWS et déployer Horizon 7 sur cette instance SDDC.

Pour créer une instance SDDC sur VMware Cloud on AWS, reportez-vous à la documentation de VMware Cloud on AWS <https://docs.vmware.com/fr/VMware-Cloud-on-AWS/index.html>.

Par défaut, un cluster à hôte unique sur le SDDC de Cloud est supprimé dans les 30 jours. Pour un environnement de production, il est recommandé d'utiliser au moins quatre hôtes dans un cluster.

Configuration de la connexion et du pare-feu pour le déploiement d' Horizon 7 sur VMware Cloud on AWS

Pour configurer un déploiement de Cloud hybride, vous devez suivre ces règles de connexion et de pare-feu.

connexion

Utilisez la console de VMC dans VMware Cloud on AWS pour créer un réseau privé virtuel dans le réseau de gestion de SDDC vers votre réseau de gestion sur site, configurer la passerelle de gestion avec des règles de pare-feu et spécifier des adresses de serveur DNS pour le réseau de gestion. Votre équipe de mise en réseau peut configurer le VPN sur site en utilisant les informations que vous téléchargez depuis le SDDC.

Vous devez configurer les connexions VPN suivantes entre les composants dans le réseau logique :

- Configurez une connexion VPN entre le composant de gestion et le composant sur site.

- Configurez une connexion VPN entre le composant de calcul et le composant sur site.
- Configurez une connexion VPN entre le composant de calcul et le composant de gestion.

Vous pouvez également utiliser AWS Direct Connect pour établir une connexion entre Horizon 7 et VMware Cloud on AWS. Pour plus d'informations sur la configuration des VPN ou sur l'utilisation d'AWS Direct Connect, consultez le document *Démarrage de VMware Cloud sur AWS*.

Règles de pare-feu

Vous pouvez exécuter l'accélérateur de règle de pare-feu dans VMware Cloud on AWS pour que tous les VPN créent toutes les règles de pare-feu requises.

Le tableau suivant décrit les règles de pare-feu pour la passerelle de gestion sur VMware Cloud on AWS :

Tableau 3-1. Règles de pare-feu de passerelle de gestion

Nom de la règle	Nom du service	Ports	Action	Source	Destination
Any SSO	SSO (TCP 7444)	7444	Allow	Any	vCenter
vCenter (ANY) to Management-On-Prem	Any (All Traffic)	Any	Allow	vCenter	Compute/On-prem subnet
ESXi (ANY) to Management-On-Prem	Any (All Traffic)	Any	Allow	ESXi	Compute/On-prem subnet
Management-On-Prem to vCenter (HTTPS)	HTTPS (TCP 443)	443	Allow	Compute/On-prem subnet	vCenter
Management-On-Prem to vCenter (ICMP)	ICMP (All ICMP)	Any	Allow	Compute/On-prem subnet	vCenter
Management-On-Prem to ESXi (Provisioning)	Provisioning (TCP 902)	902	Allow	Compute/On-prem subnet	ESXi
Management-On-Prem to ESXi (Remote Console)	Remote Console (TCP 903)	903	Allow	Compute/On-prem subnet	ESXi
Management-On-Prem to ESXi (ICMP)	ICMP (All ICMP)	Any	Allow	Compute/On-prem subnet	ESXi
Default Deny All	Any (All Traffic)	Any	Deny	Any	Any

Le tableau suivant décrit les règles de pare-feu pour la passerelle de calcul sur VMware Cloud on AWS :

Tableau 3-2. Règles de pare-feu de passerelle de calcul

Nom de la règle	Nom du service	Ports	Action	Source	Destination
Compute (ANY) to Internet and VPN	Any (All Traffic)	Any	Allow	Any	All Internet and VPN
Management-On-Prem (ANY) to BackEnd	Any (All Traffic)	Any	Allow	On-Premises Management subnet	Management Subnet

Préparation d'Active Directory pour le déploiement d'Horizon 7 sur VMware Cloud on AWS

Si vous déployez Horizon 7 dans un environnement de Cloud hybride en liant l'espace sur site avec l'espace VMware Cloud on AWS, vous devez préparer l'annuaire Active Directory (AD) Microsoft sur site pour qu'il accède à l'annuaire AD sur VMware Cloud on AWS.

Si l'espace Horizon 7 sur VMware Cloud on AWS est autonome, vous pouvez ignorer la préparation de l'annuaire AD sur site.

Vous pouvez utiliser les scénarios suivants pour préparer Active Directory pour votre déploiement de Cloud hybride :

- Si vous voulez que les contrôleurs de domaine AD sur site entretiennent l'espace Horizon 7 sur VMware Cloud on AWS, la durée d'accès peut être ralentie à cause de la latence entre le site et VMware Cloud on AWS.
- Sur VMware Cloud on AWS, déployez un contrôleur de domaine AD en lecture seule.
- Configurez une approbation entre l'annuaire AD de Microsoft AWS à votre annuaire AD existant. Lorsque vous autorisez l'annuaire AD de Microsoft AWS à accéder à l'annuaire AD sur site, l'annuaire AD Microsoft AWS peut servir de domaine de ressources. Le fait de configurer une approbation permet à vos utilisateurs de se connecter avec l'authentification unique à l'aide de leurs informations d'identification professionnelles existantes aux services AWS.

Environnements Horizon 7 sur VMware Cloud on AWS

Vous pouvez déployer Horizon 7 sur VMware Cloud on AWS tout seul ou en tant que déploiement de Cloud hybride. Un déploiement de Cloud hybride se produit lorsque vous déployez Horizon 7 sur site et sur VMware Cloud on AWS.

Pour plus d'informations sur l'installation de composants d'Horizon 7, reportez-vous au document *Installation d'Horizon 7*.

Environnement Horizon 7 sur VMware Cloud on AWS

Lorsque vous configurez l'environnement Horizon 7 sur VMware Cloud on AWS, vous devez installer les composants suivants :

- Serveurs Active Directory, DNS, DHCP ou KMS.

- Éventuellement, installez des serveurs de licences RDS.
- Serveur de connexion Horizon ou serveur de répliques version 7.5.
 - Utilisez cloudadmin@vmc.local comme informations d'identification de vCenter Server.
 - Pour un cluster à nœud unique, définissez la stratégie de stockage VM vSAN sur « Pas de redondance de données ».
 - N'activez pas View Storage Accelerator.
- Horizon Agent
- Un dispositif Unified Access Gateway connecté au Serveur de connexion est requis uniquement si votre déploiement prend en charge les utilisateurs distants.
 - Utilisez Unified Access Gateway version 3.3.
 - Ne déployez qu'une seule carte réseau avec l'assistant de déploiement OVF. Pour plusieurs cartes réseau, utilisez le script PowerShell pour inclure le mot de passe et coder les caractères spéciaux dans le fichier de configuration .INI. Pour plus d'informations, consultez la documentation d'Unified Access Gateway à l'adresse <https://docs.vmware.com/fr/Unified-Access-Gateway/index.html>.
 - Déployez les cartes réseau dans les dossiers Compute-ResourcePool, WorkloadDatastore et Workloads.
 - Spécifiez netmask0-2 pour les cartes réseau.
- Un équilibrage de charge si vous utilisez deux Serveurs de connexion ou plus.
- En option, base de données des événements sur Microsoft SQL Server 2016

Environnement Horizon 7 sur site

Éventuellement, si vous souhaitez un déploiement de Cloud hybride, vous pouvez déployer un environnement Horizon 7 sur site. Reportez-vous au document *Installation d'Horizon 7* sur les étapes de configuration d'un environnement Horizon 7.

Lier Horizon 7 sur VMware Cloud on AWS avec Horizon 7 sur site

L'espace Horizon 7 sur site et l'espace Horizon 7 sur VMware Cloud on AWS peuvent être gérés séparément. Toutefois, si vous souhaitez gérer les déploiements sous la forme d'un Cloud hybride, vous devez utiliser Architecture Cloud Pod pour lier l'espace sur site avec l'espace sur VMware Cloud on AWS.

Prérequis

- Déployez Horizon 7 version 7.0 ou ultérieure sur un environnement sur site et sur VMware Cloud on AWS.

Procédure

- 1 Utilisez Architecture Cloud Pod pour connecter l'espace Horizon 7 sur site à l'espace Horizon 7 sur VMware Cloud on AWS. Pour plus d'informations sur l'utilisation et la configuration d'Architecture Cloud Pod, reportez-vous au document *Administration d'Architecture Cloud Pod dans Horizon 7*.

Remarque Il n'est pas nécessaire que la version d'Horizon 7 déployée sur site et la version d'Horizon 7 déployée sur VMware Cloud on AWS soient les mêmes.

- 2 Configurez des ports et des règles de pare-feu.
- 3 En option, lorsque vous utilisez Architecture Cloud Pod, vous pouvez déployer un équilibrage de charge global entre les deux espaces.
- 4 En option, vous pouvez déployer n'importe quel nombre d'espaces Horizon 7 sur site et les lier avec n'importe quel nombre d'espaces Horizon 7 sur VMware Cloud on AWS. Le nombre maximal d'espaces doit respecter les limites définies pour les espaces dans Architecture Cloud Pod. Reportez-vous à l'article de la base de connaissances de VMware « VMware Horizon 7 Sizing Limits and Recommendations (Limites et recommandations de dimensionnement de VMware Horizon 7) » <https://kb.vmware.com/s/article/2150348>.

Lier des espaces Horizon 7 sur VMware Cloud on AWS

Vous pouvez utiliser la fonctionnalité Architecture Cloud Pod pour connecter des espaces Horizon 7 qu'ils soient sur site ou sur VMware Cloud on AWS. Lorsque vous déployez plusieurs espaces Horizon 7 sur VMware Cloud on AWS, vous pouvez les gérer de manière indépendante ou ensemble en les liant à Architecture Cloud Pod. Pour plus d'informations sur l'utilisation et la configuration d'Architecture Cloud Pod, reportez-vous au document *Administration d'Architecture Cloud Pod dans Horizon 7*.

Prérequis

- Déployez Horizon 7 version 7.0 ou ultérieure sur VMware Cloud on AWS.

Procédure

- 1 Architecture Cloud Pod permet de lier n'importe quel nombre d'espaces Horizon 7 sur VMware Cloud on AWS. Le nombre maximal d'espaces doit respecter les limites définies pour les espaces dans Architecture Cloud Pod. Reportez-vous à l'article de la base de connaissances de VMware « VMware Horizon 7 Sizing Limits and Recommendations (Limites et recommandations de dimensionnement de VMware Horizon 7) » <https://kb.vmware.com/s/article/2150348>.
- 2 Configurez des ports et des règles de pare-feu.
- 3 En option, lorsque vous utilisez Architecture Cloud Pod, vous pouvez déployer un équilibrage de charge global entre les deux espaces.

Prise en main d'un déploiement de Cloud hybride pour Horizon 7

Vous pouvez configurer un déploiement de Cloud hybride pour Horizon 7 si vous disposez d'une infrastructure Horizon 7 sur site existante et que vous devez augmenter la capacité, mais ne souhaitez pas acheter de matériel supplémentaire. L'extension des charges de travail Horizon 7 à VMware Cloud on AWS vous permet d'utiliser la capacité de Cloud pour les charges de travail Horizon 7, tout en gérant des déploiements sur site et de VMware Cloud dans un seul espace fédéré.

Prérequis

- Créez une instance de SDDC (Software-Defined Data Center) sur VMware Cloud on AWS. Consultez la documentation de VMware Cloud on AWS <https://docs-staging.vmware.com/en/VMware-Cloud-on-AWS/index.html>.
- Configurez des règles de VPN et de pare-feu pour permettre à l'instance du Serveur de connexion sur VMware Cloud on AWS de communiquer avec l'instance du Serveur de connexion sur site. Reportez-vous à la section [Configuration de la connexion et du pare-feu pour le déploiement d'Horizon 7 sur VMware Cloud on AWS](#).
- Préparez Microsoft Active Directory (AD) et choisissez de configurer une approbation à sens unique ou une approbation bidirectionnelle. Reportez-vous à la section [Préparation d'Active Directory pour le déploiement d'Horizon 7 sur VMware Cloud on AWS](#).
- Configurez l'environnement Horizon 7 sur VMware Cloud on AWS. Reportez-vous à la section [Environnements Horizon 7 sur VMware Cloud on AWS](#).
- Configurez l'environnement Horizon 7 sur site. Reportez-vous à la section [Environnements Horizon 7 sur VMware Cloud on AWS](#).

Procédure

- 1 Sur un Serveur de connexion, initialisez Architecture Cloud Pod et joignez le Serveur de connexion à une fédération d'espaces. Reportez-vous à la section [Lier Horizon 7 sur VMware Cloud on AWS avec Horizon 7 sur site](#). Pour plus d'informations sur la configuration d'Architecture Cloud Pod, reportez-vous au document *Administration d'Architecture Cloud Pod dans Horizon 7*.
- 2 Pour partager facilement des images et des images ISO, vous pouvez utiliser la bibliothèque de contenu vCenter sur chaque serveur vCenter Server.
- 3 Sur chaque Serveur de connexion, créez un pool de postes de travail de machines virtuelles complètes avec CBRC désactivé. Pour plus d'informations sur la création d'un pool de postes de travail de machines virtuelles complètes, reportez-vous au document *Configuration des postes de travail virtuels dans Horizon 7*.

Suivant

- Utilisez Horizon Client pour démarrer un poste de travail configuré avec le protocole d'affichage VMware Blast, PCoIP ou RDP.

Personnalisation des données LDAP

4

Vous pouvez utiliser les outils de ligne de commande VMware et Microsoft pour importer des données de configuration LDAP vers Horizon 7 ou les exporter depuis celui-ci. Ces outils de ligne de commande importent et exportent des données de configuration LDAP dans des fichiers de configuration LDAP au format LDIF (Data Interchange Format).

Cette fonctionnalité est destinée aux administrateurs avancés qui souhaitent effectuer des opérations de configuration automatique en masse. Pour créer des scripts afin de mettre à jour la configuration de Horizon 7, utilisez Horizon 7 PowerCLI.

Ce chapitre aborde les rubriques suivantes :

- [Présentation des données de configuration LDAP](#)
- [Modification des données de configuration LDAP](#)

Présentation des données de configuration LDAP

Toutes les données de configuration de Horizon 7 sont stockées dans un annuaire LDAP. Chaque instance standard ou répliquée du Horizon Connection Server contient un référentiel de configuration LDAP local et un accord de réplication entre chaque instance du Serveur de connexion. Cela permet de garantir que les modifications apportées à un référentiel sont répliquées automatiquement vers tous les autres référentiels.

Lorsque vous utilisez Horizon Administrator pour modifier la configuration d'Horizon 7, les données LDAP appropriées sont mises à jour dans le référentiel. Par exemple, si vous ajoutez un pool de postes de travail, Horizon 7 stocke des informations sur les utilisateurs, les groupes d'utilisateurs et les droits dans LDAP. Les instances du Serveur de connexion gèrent automatiquement les autres données de configuration LDAP et utilisent les informations du référentiel pour contrôler les opérations d'Horizon 7.

Vous pouvez utiliser des fichiers de configuration LDIF pour effectuer un certain nombre de tâches, comme le transfert des données de configuration entre des instances du Serveur de connexion et la sauvegarde de votre configuration Horizon 7 pour pouvoir restaurer l'état d'une instance du Serveur de connexion.

Vous pouvez également utiliser des fichiers de configuration LDIF pour définir un grand nombre d'objets Horizon 7, tels que des pools de postes de travail, puis ajouter ces objets à vos instances du Serveur de connexion sans utiliser Horizon Administrator pour effectuer cette tâche manuellement.

Dans Horizon 7 3.1 et versions ultérieures, Horizon 7 effectue des sauvegardes régulières du référentiel LDAP.

Les données de configuration LDAP sont transférées en texte brut ASCII et sont conformes à la norme Internet Engineering Task Force (IETF) RFC 2849.

Modification des données de configuration LDAP

Vous pouvez exporter des données de configuration LDAP sur une instance du Horizon Connection Server vers un fichier de configuration LDIF, modifier le fichier de configuration LDIF et importer le fichier de configuration LDIF modifié dans d'autres instances du Serveur de connexion pour effectuer des opérations automatiques de configuration en bloc.

Vous pouvez obtenir des exemples de syntaxe LDIF pour n'importe quel élément de données de configuration LDAP dans Horizon en examinant le contenu d'un fichier de configuration LDIF exporté. Par exemple, vous pouvez extraire les données d'un pool de postes de travail et les utiliser comme modèle pour créer un grand nombre de pools de postes de travail.

Exporter des données de configuration LDAP

Vous pouvez utiliser l'utilitaire de ligne de commande `vdmexport` pour exporter des données de configuration à partir d'une instance du Horizon Connection Server standard ou réplica vers un fichier de configuration LDIF.

Par défaut, l'utilitaire de ligne de commande `vdmexport` est installé dans le répertoire `C:\Program Files\VMware\VMware View\Server\tools\bin`.

Procédure

- 1 Connectez-vous à une instance du Serveur de connexion standard ou réplica.

Option	Action
View 3.1 et versions antérieures	Connectez-vous en tant qu'administrateur et soyez membre du groupe d'utilisateurs Administrateurs locaux.
View 4.5 et versions ultérieures	Connectez-vous en tant qu'utilisateur dans le rôle Administrateurs ou Administrateurs (lecture seule).
	Remarque Vous devez être connecté en tant qu'utilisateur dans le rôle Administrateurs ou Administrateurs (lecture seule) pour exporter les données de configuration à partir du référentiel de configuration View.

- 2 À l'invite de commande, tapez la commande `vdmexport` et utilisez l'option `-f` pour spécifier le nom du fichier de configuration LDIF à exporter.

Par exemple : `vdmexport -f myexport.LDF`

Vous pouvez également rediriger le résultat au lieu d'utiliser l'option `-f`.

Par exemple : `vdmexport > myexport.LDF`

La commande `vdmexport` écrit la configuration de votre instance du Serveur de connexion dans le fichier que vous spécifiez. La commande affiche des erreurs si votre rôle ne dispose pas de privilèges suffisants pour afficher les données dans le référentiel de configuration.

Définition d'un pool de postes de travail dans un fichier de configuration LDIF

Vous pouvez définir un pool de postes de travail dans un fichier de configuration LDIF et importer le fichier de configuration LDIF personnalisé pour créer un grand nombre de pools de postes de travail.

Remarque Vous pouvez également créer des fichiers de configuration LDIF personnalisés pour d'autres objets définis dans le référentiel LDAP, notamment des paramètres de configuration générale, des paramètres de configuration pour une instance du Horizon Connection Server ou un serveur de sécurité spécifique, ainsi que des paramètres de configuration pour un utilisateur spécifique.

Pour définir un pool de postes de travail dans un fichier de configuration LDIF, vous devez ajouter les entrées suivantes au fichier.

- Une entrée de VM de poste de travail virtuel pour chaque poste de travail virtuel dans le pool de postes de travail
- Une entrée de pool de VM pour chaque pool de postes de travail
- Une entrée d'application de poste de travail qui définit le droit du pool de postes de travail

Vous associez chaque entrée de pool de VM à une entrée d'application de poste de travail dans une relation un-à-un. Une entrée d'application de poste de travail ne peut pas être partagée entre des entrées de pool de VM, et une entrée de pool de VM ne peut être associée qu'à une seule entrée d'application de poste de travail.

Le tableau suivant décrit les attributs que vous devez spécifier lorsque vous modifiez une définition de pool de postes de travail dans un fichier de configuration LDIF.

Tableau 4-1. Attributs importants pour la définition d'un pool de postes de travail

Entrée	Attribut	Description
VM de poste de travail virtuel Pool de VM Application de poste de travail	cn	Nom commun d'une entrée. Si vous voulez que les noms soient générés automatiquement, spécifiez des chaînes d'identificateur unique universel (GUID). Vous pouvez utiliser n'importe quel générateur GUID fiable, tel que le mécanisme fourni par .NET (par exemple, en appelant System.Guid.NewGuid().ToString() dans Visual Basic).
Application de poste de travail	member	<p>Liste des utilisateurs et des groupes Active Directory (AD) autorisés à accéder au pool de postes de travail. L'attribut est indiqué sous la forme d'une référence SID (Security Identifier) Windows. Une valeur member de <SID=S-1-2-3-4> représente un utilisateur ou un groupe AD dont la valeur SID est S-1-2-3-4.</p> <p>Dans le format LDIF, le signe « inférieur à » (<) est réservé. Vous devez donc placer deux fois le signe « deux-points » (::) après le nom de l'attribut et spécifier la valeur SID au format base64 (par exemple, PFNJRD1TLTEtMi0zLTQ+IA==). Comme cet attribut est à valeurs multiples, vous pouvez l'utiliser sur plusieurs lignes pour représenter chaque entrée dans une liste de SID.</p>

Exemples d'entrées de pool de postes de travail d'un fichier de configuration LDIF

L'exemple suivant est un extrait d'un fichier de configuration LDIF. Il indique des exemples d'entrées d'un pool de postes de travail nommé Pool1, qui contient deux postes de travail virtuels nommés VM1 et VM2. L'entrée du pool de postes de travail est couplée avec l'entrée de l'application de poste de travail, qui est également nommée Pool1.

```
#
# Virtual Desktop VM entry VM1
#
DN: CN=vm1,OU=Servers,DC=vdi,DC=vmware,DC=int
changetype: add
objectClass: top
objectClass: pae-Server
objectClass: pae-WinServer
objectClass: pae-ThinWinServer
objectClass: pae-VM
cn: vm1
description: sample virtual desktop entry
pae-VmSuspended:: IA==
pae-OptIgnoreProcessList: 0
pae-MOID: vm-1
pae-VmState: READY
pae-ServerManaged: 1
pae-SSOEnabled: 1
pae-DisplayName: virtual desktop 1
pae-TunneledConnection: 1
pae-pwdEncryption: KERB5
ipHostNumber: vm1
pae-ClientProtVersion: 1
pae-WinDomain: NULL
```

```

pae-thinProto: XP_RDP
pae-Services: SESSION |, HEARTBEAT |, EVENTS |, USED |
pae-VmPath: /New Datacenter/vm/vm-1
pae-OptSuspendTimeout: 0
pae-OptDisconnectLimitTimeout: 0
pae-OptMaximumSessions: 0
pae-Disabled: 0

#
# Virtual Desktop VM entry VM2
#
DN: CN=vm2,OU=Servers,DC=vdi,DC=vmware,DC=int
changetype: add
objectClass: top
objectClass: pae-Server
objectClass: pae-WinServer
objectClass: pae-ThinWinServer
objectClass: pae-VM
cn: vm2
description: sample virtual desktop entry
pae-VmSuspended:: IA==
pae-OptIgnoreProcessList: 0
pae-MOID: vm-2
pae-VmState: READY
pae-ServerManaged: 1
pae-SSOEnabled: 1
pae-DisplayName: virtual desktop 2
pae-TunneledConnection: 1
pae-pwdEncryption: KERB5
ipHostNumber: vm2
pae-ClientProtVersion: 1
pae-WinDomain: NULL
pae-thinProto: XP_RDP
pae-Services: SESSION |, HEARTBEAT |, EVENTS |, USED |
pae-VmPath: /New Datacenter/vm/vm-2
pae-OptSuspendTimeout: 0
pae-OptDisconnectLimitTimeout: 0
pae-OptMaximumSessions: 0
pae-Disabled: 0
#
# Further Virtual Desktop VM entries as required
#
#
# VM Pool entry Pool1
#
DN: CN=Pool1,OU=Server Groups,DC=vdi,DC=vmware,DC=int
changetype: add
objectClass: top
objectClass: pae-ServerPool
cn: Pool1
pae-VCDN: CN=b180b93b-2dd3-4b58-8a81-b8534a4b7565,OU=VirtualCenter,OU=Properties,DC=vdi,
DC=vmware,DC=int
pae-MemberDN: CN=vm1,OU=Servers,DC=vdi,DC=vmware,DC=int
pae-MemberDN: CN=vm2,OU=Servers,DC=vdi,DC=vmware,DC=int
pae-VmPowerPolicy: remainon

```

```

pae-VmProvEnabled: 1
pae-VmProvSuspendOnError: 1
pae-VmStartClone: 1
pae-VmPoolCalculatedValues: 1
pae-ServerPoolType: 0
pae-VmMinimumCount: 0
pae-VmHeadroomCount: 0
pae-VmMaximumCount: 0
pae-Disabled: 0

#
# Desktop Application entry Pool1 -- one entry is required for each VM Pool
#
DN: CN=Pool1,OU=Applications,DC=vdi,DC=vmware,DC=int
changetype: add
objectClass: top
objectClass: pae-Entity
objectClass: pae-App
objectClass: pae-WinApp
objectClass: pae-ThinWinApp
objectClass: pae-DesktopApplication
cn: Pool1
member:: PFNJRd1TLTETMi0zLTQ+IA==
pae-Icon: /thinapp/icons/desktop.gif
pae-URL: \
pae-Servers: CN=Pool1,OU=Server Groups,DC=vdi,DC=vmware,DC=int
pae-ServerProtocolLevel: OSX_NETOP
pae-ServerProtocolLevel: OS2_NETOP
pae-ServerProtocolLevel: NT4_NETOP
pae-ServerProtocolLevel: WIN2K_NETOP
pae-ServerProtocolLevel: NT4_RDP
pae-ServerProtocolLevel: WIN2K_RDP
pae-ServerProtocolLevel: XP_RDP
pae-Disabled: 0

```

Utiliser la commande vdmimport pour importer des données de configuration LDAP

Dans View 4.5 et versions ultérieures, vous pouvez utiliser la commande `vdmimport` pour importer des données de configuration à partir d'un fichier de configuration LDIF vers une instance du Horizon Connection Server standard ou réplique.

Par défaut, l'utilitaire de ligne de commande `vdmimport` est installé dans le répertoire `C:\Program Files\VMware\VMware View\Server\tools\bin`.

Prérequis

- Vérifiez que vous disposez de View 4.5 ou version ultérieure. Si vous disposez d'une version antérieure, reportez-vous à la section [Utiliser la commande LDIFDE pour importer des données de configuration LDAP](#).
- Exportez des données de configuration LDAP vers un fichier de configuration LDIF. Reportez-vous à la section [Exporter des données de configuration LDAP](#).

Procédure

- 1 Connectez-vous à une instance du Serveur de connexion en tant qu'utilisateur disposant du rôle Administrateurs.

Vous devez être connecté tant qu'utilisateur bénéficiant du rôle Administrateurs pour pouvoir importer des données de configuration dans le référentiel de configuration View.

- 2 À l'invite de commande, tapez la commande `vdmimport` et utilisez l'option `-f` pour spécifier le fichier de configuration LDIF à importer.

Par exemple : `vdmimport -f myexport.LDF`

Après l'exécution de la commande `vdmimport`, la configuration de votre instance du Serveur de connexion est mise à jour avec les données du fichier, et le nombre d'enregistrements mis à jour s'affiche. Des erreurs sont affichées si certains enregistrements n'ont pas pu être mis à jour, car votre rôle ne disposait pas des privilèges suffisants.

Utiliser la commande LDIFDE pour importer des données de configuration LDAP

Vous pouvez utiliser la commande Microsoft LDIFDE pour importer des données de configuration à partir d'un fichier de configuration LDIF vers une instance du Horizon Connection Server standard ou réplica.

Dans les versions antérieures à View 4.5, vous devez utiliser la commande Microsoft LDIFDE pour importer des données de configuration à partir d'un fichier de configuration LDIF. La commande `vdmimport` n'est pas prise en charge dans les versions antérieures à View 4.5.

Si vous disposez de View 4.5 ou version ultérieure, utilisez la commande `vdmimport` plutôt que la commande LDIFDE. La commande `vdmimport` n'affiche pas le grand nombre de messages d'erreur produits en exécutant la commande LDIFDE. Pour plus d'informations, reportez-vous à la section [Utiliser la commande vdmimport pour importer des données de configuration LDAP](#).

Comme la commande LDIFDE n'effectue pas de mise à jour, de création ou de suppression des enregistrements LDAP qui ne sont pas définis dans le fichier de configuration LDIF, elle vous permet de personnaliser un fichier de configuration LDIF afin que seuls les enregistrements sélectionnés soient affectés lorsque vous importez le fichier. Pour obtenir des informations complètes sur l'utilisation de la commande LDIFDE, accédez à <http://support.microsoft.com/kb/237677>.

Prérequis

Exportez des données de configuration LDAP vers un fichier de configuration LDIF. Reportez-vous à la section [Exporter des données de configuration LDAP](#).

Procédure

- 1 Connectez-vous à une instance du Serveur de connexion.

Option	Action
View 3.1 ou version antérieure	Connectez-vous en tant qu'administrateur et soyez membre du groupe d'utilisateurs Administrateurs locaux.
View 4.5 ou version ultérieure	Connectez-vous en tant qu'utilisateur disposant du rôle d'administrateur.
	Remarque Vous devez être connecté tant qu'utilisateur bénéficiant du rôle Administrateurs pour pouvoir importer des données de configuration dans le référentiel de configuration Horizon.

- 2 À l'invite de commande, tapez la commande LDIFDE et utilisez l'option `-f` pour spécifier un fichier de configuration LDIF existant.

Par exemple : `LDIFDE -i -f myexport.LDF -s 127.0.0.1 -z`

Après l'exécution de la commande LDIFDE, la configuration de votre instance du Serveur de connexion est mise à jour avec les données du fichier, et le nombre d'enregistrements mis à jour s'affiche.

Des messages d'erreur s'affichent lorsqu'une entrée existante du référentiel est remplacée. Vous pouvez ignorer ces messages d'erreur. Des messages d'erreur s'affichent également si un enregistrement ne peut pas être mis à jour, car votre rôle ne dispose pas des privilèges suffisants.

Examen des statistiques de session PColP avec WMI

5

Vous pouvez utiliser Windows Management Instrumentation (WMI) pour examiner les statistiques de performances d'une session PColP à l'aide de l'une des interfaces de programmation prises en charge, telles que C#, C++, PowerShell, VBScript, VB .NET et WMIC (Windows Management Instrumentation Command-Line).

Vous pouvez également utiliser l'outil Microsoft WMI Code Creator pour générer du code VBScript, C# et VB .NET capable d'accéder aux compteurs de performances PColP. Pour plus d'informations sur WMI, WMIC et l'outil WMI Code Creator, accédez à <http://technet.microsoft.com/en-us/library/bb742610.aspx> et <http://www.microsoft.com/downloads/en/details.aspx?familyid=2cc30a64-ea15-4661-8da4-55bbc145c30e&displaylang=en> (contenus en anglais).

Ce chapitre aborde les rubriques suivantes :

- Utilisation des statistiques de session PColP
- Statistiques générales de session PColP
- Statistiques audio PColP
- Statistiques de création d'images PColP
- Statistiques de réseau PColP
- Statistiques PColP USB
- Exemples d'utilisation de cmdlets PowerShell pour examiner les statistiques PColP

Utilisation des statistiques de session PColP

L'espace de noms WMI des statistiques de session PColP est `root\CIMV2`. Les noms des statistiques sont modifiés par l'ajout du suffixe (Serveur) ou (Client), selon que la statistique est enregistrée sur le serveur PColP ou le client PColP.

Vous pouvez utiliser le moniteur de performances Windows (PerfMon) avec les compteurs pour calculer les moyennes sur une période d'échantillonnage définie. Vous devez disposer des privilèges d'administrateur pour accéder à distance aux compteurs de performances.

Toutes les statistiques sont réinitialisées à 0 lorsqu'une session PColP est fermée. Si la propriété WMI `SessionDurationSeconds` est une valeur non nulle et reste constante, le serveur PColP a été arrêté de force ou s'est bloqué. Si la propriété `SessionDurationSeconds` passe d'une valeur non nulle à 0, la session PColP est fermée.

Pour éviter une erreur de division par zéro, vérifiez que le dénominateur des expressions pour le calcul du pourcentage de bande passante ou de perte de paquets ne corresponde pas à zéro.

Les statistiques USB sont enregistrées pour les clients zéro, mais pas pour les clients légers ou les clients logiciels.

Statistiques générales de session PCoIP

Le nom de classe WMI pour les statistiques générales de session PCoIP est `Win32_PerfRawData_TeradiciPerf_PCoIPSessionGeneralStatistics`.

Tableau 5-1. Statistiques générales de session

Nom de propriété WMI	Description
BytesReceived	Nombre total, en octets, de données PCoIP reçues depuis le démarrage de la session PCoIP.
BytesSent	Nombre total, en octets, de données PCoIP transmises depuis le démarrage de la session PCoIP.
PacketsReceived	Nombre total de paquets reçus avec succès depuis le démarrage de la session PCoIP. Les paquets n'ont pas tous la même taille.
PacketsSent	Nombre total de paquets transmis depuis le démarrage de la session PCoIP. Les paquets n'ont pas tous la même taille.
RXPacketsLost	Nombre total de paquets reçus qui ont été perdus depuis le démarrage de la session PCoIP.
SessionDurationSeconds	Nombre total de secondes pendant lequel la session PCoIP a été ouverte.
TXPacketsLost	Nombre total de paquets transmis qui ont été perdus depuis le démarrage de la session PCoIP.

Calcul de la bande passante pour les données PCoIP reçues

Pour calculer la bande passante en kilobits par seconde pour les données PCoIP reçues pendant l'intervalle de temps entre l'instant t_1 et le l'instant t_2 , utilisez la formule suivante.

$$(\text{BytesReceived}[t_2] - \text{BytesReceived}[t_1]) * 8 / (1024 * (t_2 - t_1))$$

Calcul de la bande passante pour les données PCoIP transmises

Pour calculer la bande passante en kilobits par seconde pour les données PCoIP transmises pendant l'intervalle de temps entre l'instant t_1 et l'instant t_2 , utilisez la formule suivante.

$$(\text{BytesSent}[t_2] - \text{BytesSent}[t_1]) * 8 / (1024 * (t_2 - t_1))$$

Calcul de la perte de paquets pour les données PCoIP reçues

Utilisez la formule suivante pour calculer le pourcentage de paquets reçus qui sont perdus.

$$100 / (1 + ((\text{PacketsReceived}[t2] - \text{PacketsReceived}[t1]) / (\text{RXPacketsLost}[t2] - \text{RXPacketsLost}[t1])))$$

Calcul de la perte de paquets pour les données PCoIP transmises

Utilisez la formule suivante pour calculer le pourcentage de paquets transmis qui sont perdus.

$$100 * (\text{TXPacketsLost}[t2] - \text{TXPacketsLost}[t1]) / (\text{PacketsSent}[t2] - \text{PacketsSent}[t1])$$

Statistiques audio PCoIP

Le nom de classe WMI des statistiques audio PCoIP est
Win32_PerfRawData_TeradiciPerf_PCoIPSessionAudioStatistics.

Remarque Les statistiques audio n'incluent pas les données audio contenues dans les données USB.

Tableau 5-2. Statistiques audio PCoIP

Nom de la propriété WMI	Description
AudioBytesReceived	Nombre total d'octets de données audio reçus depuis le démarrage de la session PCoIP.
AudioBytesSent	Nombre total d'octets de données audio envoyés depuis le démarrage de la session PCoIP.
AudioRXBkbitPersec	Moyenne de bande passante pour les paquets audio entrants durant la période d'échantillonnage, en secondes.
AudioTXBkbitPersec	Moyenne de la bande passante pour les paquets audio sortants pendant la période d'échantillonnage, en secondes.
AudioTXBWLimitkbitPersec	Limite de bande passante de transmission en kilobits par seconde pour les paquets audio sortants. La limite est définie par un paramètre GPO.

Calcul de la bande passante pour les données audio reçues

Utilisez la formule suivante pour calculer la bande passante en kilobits par seconde pour les données audio reçues pendant l'intervalle de temps entre l'instant t1 et l'instant t2.

$$(\text{AudioBytesReceived}[t2] - \text{AudioBytesReceived}[t1]) * 8 / (1024 * (t2 - t1))$$

N'utilisez pas AudioRXBkbitPersec pour ce calcul.

Calcul de la bande passante pour les données audio transmises

Utilisez la formule suivante pour calculer la bande passante en kilobits par seconde pour les données audio transmises pendant l'intervalle de temps entre l'instant t_1 et l'instant t_2 .

$$(\text{AudioBytesSent}[t_2] - \text{AudioBytesSent}[t_1]) * 8 / (1024 * (t_2 - t_1))$$

N'utilisez pas `AudioTXBkbitPersec` pour ce calcul.

Statistiques de création d'images PCoIP

Le nom de classe WMI des statistiques de création d'images PCoIP est `Win32_PerfRawData_TeradiciPerf_PCoIPSessionImagingStatistics`.

Tableau 5-3. Statistiques de création d'images PCoIP

Nom de la propriété WMI	Description
<code>ImagingBytesReceived</code>	Nombre total d'octets de données de création d'images reçus depuis le démarrage de la session PCoIP.
<code>ImagingBytesSent</code>	Nombre total d'octets de données de création d'images transmis depuis le démarrage de la session PCoIP.
<code>ImagingDecoderCapabilitykbitPersec</code>	Capacité de traitement estimée du décodeur d'image en kilobits par seconde. Cette statistique est mise à jour une fois par seconde.
<code>ImagingEncodedFramesPersec</code>	Nombre de trames d'images codées sur une période d'échantillonnage d'une seconde.
<code>ImagingActiveMinimumQuality</code>	Valeur codée de qualité la plus faible sur une échelle de 0 à 100. Cette statistique est mise à jour une fois par seconde. Ce compteur ne correspond pas au paramètre de GPO pour la qualité minimale.
<code>ImagingRXBkbitPersec</code>	Moyenne de bande passante pour les paquets d'images entrants durant la période d'échantillonnage, en secondes.
<code>ImagingTXBkbitPersec</code>	Moyenne de bande passante pour les paquets d'images sortants durant la période d'échantillonnage, en secondes.

Calcul de la bande passante pour les données de création d'images reçues

Utilisez la formule suivante pour calculer la bande passante en kilobits par seconde pour les données de création d'images reçues pendant l'intervalle de temps entre l'instant t_1 et l'instant t_2 .

$$(\text{ImagingBytesReceived}[t_2] - \text{ImagingBytesReceived}[t_1]) * 8 / (1024 * (t_2 - t_1))$$

N'utilisez pas `ImagingRXBkbitPersec` pour ce calcul.

Calcul de la bande passante pour les données de création d'images transmises

Utilisez la formule suivante pour calculer la bande passante en kilobits par seconde pour les données de création d'images transmises pendant l'intervalle de temps entre l'instant t1 et l'instant t2.

$$(\text{ImagingBytesSent}[t2] - \text{ImagingBytesSent}[t1]) * 8 / (1024 * (t2 - t1))$$

N'utilisez pas `ImagingTXBwkbPersec` pour ce calcul.

Statistiques de réseau PCoIP

Le nom de classe WMI des statistiques de réseau PCoIP est `Win32_PerfRawData_TeradiciPerf_PCoIPSessionNetworkStatistics`.

Tableau 5-4. Statistiques de réseau PCoIP

Nom de la propriété WMI	Description
<code>RoundTripLatencys</code>	Latence de parcours circulaire, en millisecondes, entre le serveur PCoIP et le client PCoIP.
<code>RXBwkbPersec</code>	Moyenne de bande passante globale pour les paquets PCoIP entrants durant la période d'échantillonnage, en secondes.
<code>RXBWPeakkbPersec</code>	Bande passante maximale en kilobits par seconde pour les paquets PCoIP entrants durant une période d'échantillonnage d'une seconde.
<code>RXPacketLossPercent</code>	Pourcentage de paquets reçus perdus pendant une période d'échantillonnage.
<code>TXBwkbPersec</code>	Moyenne de bande passante globale pour les paquets PCoIP sortants durant la période d'échantillonnage, en secondes.
<code>TXBWActiveLimitkbPersec</code>	Estimation de bande passante réseau disponible en kilobits par seconde. Cette statistique est mise à jour une fois par seconde.
<code>TXBWLimitkbPersec</code>	<p>Limite de bande passante de transmission, en kilobits par seconde, pour les paquets sortants. La limite correspond au minimum des valeurs suivantes.</p> <ul style="list-style-type: none"> ■ Limite de bande passante GPO pour le client PCoIP ■ Limite de bande passante GPO pour le serveur PCoIP ■ Limite de bande passante pour la connexion de réseau local ■ Limite de bande passante négociée pour le microprogramme Zero Client en fonction des limites de chiffrement
<code>TXPacketLossPercent</code>	Pourcentage de paquets transmis perdus pendant une période d'échantillonnage.

Calcul de la bande passante pour les données de réseau reçues

Utilisez la formule suivante pour calculer la bande passante en kilobits par seconde pour les données reçues pendant l'intervalle de temps entre l'instant t1 et l'instant t2.

```
(BytesReceived[t2]-BytesReceived[t1]) * 8 / (1024 * (t2-t1))
```

N'utilisez pas `RXBWkbitPersec` pour ce calcul.

Calcul de la bande passante pour les données de réseau transmises

Utilisez la formule suivante pour calculer la bande passante en kilobits par seconde pour les données transmises pendant l'intervalle de temps entre l'instant t1 et l'instant t2.

```
(BytesSent[t2]-BytesSent[t1]) * 8 / (1024 * (t2-t1))
```

N'utilisez pas `TXBWkbitPersec` pour ce calcul.

Calcul de la perte de paquets pour les données de réseau reçues

Utilisez la formule suivante pour calculer le pourcentage de perte de paquets pour les données reçues pendant l'intervalle de temps entre l'instant t1 et l'instant t2.

```
PacketsReceived during interval = (PacketsReceived[t2]-PacketsReceived[t1])
```

```
RXPacketsLost during interval = (RXPacketsLost[t2]-RXPacketsLost[t1])
```

```
RXPacketsLost % = RXPacketsLost during interval /  
(RXPacketsLost during interval + PacketsReceived during interval) * 100
```

N'utilisez pas `RXPacketLostPercent` ou `RXPacketLostPercent_Base` pour ce calcul.

Calcul de la perte de paquets pour les données de réseau transmises

Utilisez la formule suivante pour calculer le pourcentage de perte de paquets pour les données transmises pendant l'intervalle de temps entre l'instant t1 et l'instant t2.

```
PacketsSent during interval = (PacketsSent[t2]-PacketsSent[t1])
```

```
TXPacketsLost during interval = (TXPacketsLost[t2]-TXPacketsLost[t1])
```

```
TXPacketsLost % = TXPacketsLost during interval /  
(TXPacketsLost during interval + PacketsSent during interval) * 100
```

N'utilisez pas `TXPacketLostPercent` ou `TXPacketLostPercent_Base` pour ce calcul.

Utilisez cette formule pour empêcher le pourcentage de perte de paquets de dépasser les 100 %. Ce calcul est nécessaire, car `PacketsLost` et `PacketsSent` sont asynchrones.

Statistiques PCoIP USB

Le nom de classe WMI des statistiques PCoIP USB est `Win32_PerfRawData_TeradiciPerf_PCoIPSessionUSBStatistics`.

Tableau 5-5. Statistiques PCoIP USB

Nom de la propriété WMI	Description
<code>USBBytesReceived</code>	Nombre total, en octets, de données USB reçues depuis le démarrage de la session PCoIP.
<code>USBBytesSent</code>	Nombre total, en octets, de données USB transmises depuis le démarrage de la session PCoIP.
<code>USBRXBWkbitPersec</code>	Moyenne de bande passante pour les paquets USB entrants pendant la période d'échantillonnage, en secondes.
<code>USBTXBWkbitPersec</code>	Moyenne de bande passante pour les paquets USB sortants pendant la période d'échantillonnage, en secondes.

Calcul de la bande passante pour les données USB reçues

Utilisez la formule suivante pour calculer la bande passante en kilobits par seconde pour les données USB reçues pendant l'intervalle de temps entre l'instant `t1` et l'instant `t2`.

```
(USBBytesReceived[t2]-USBBytesReceived[t1]) * 8 / (1024 * (t2-t1))
```

N'utilisez pas `USBRXBWkbitPersec` pour ce calcul.

Calcul de la bande passante pour les données USB transmises

Utilisez la formule suivante pour calculer la bande passante en kilobits par seconde pour les données USB transmises pendant l'intervalle de temps entre l'instant `t1` et l'instant `t2`.

```
(USBBytesSent[t2]-USBBytesSent[t1]) * 8 / (1024 * (t2-t1))
```

N'utilisez pas `USBTXBWkbitPersec` pour ce calcul.

Exemples d'utilisation de cmdlets PowerShell pour examiner les statistiques PCoIP

Vous pouvez utiliser les cmdlets PowerShell pour examiner les statistiques PCoIP.

Dans l'exemple suivant, la cmdlet `Get-WmiObject` récupère les statistiques de réseau PCoIP pour le client `cm-02`.

```
Get-WmiObject -namespace "root\cimv2" -computername cm-02 -class  
Win32_PerfRawData_TeradiciPerf_PCoIPSessionNetworkStatistics
```

Dans l'exemple suivant, la cmdlet `Get-WmiObject` récupère les statistiques de session générale PCoIP pour le poste de travail `dt-03`, en cas de perte de paquets transmis.

```
Get-WmiObject -namespace "root\cimv2" -computername desktop-03 -query "select * from  
Win32_PerfRawData_TeradiciPerf_PCoIPSessionGeneralStatistics where TXPacketsLost > 0"
```

Définition de stratégies de poste de travail avec des scripts de démarrage de session

6

Les scripts de démarrage de session vous permettent de configurer des paramètres de poste de travail Horizon 7 spécifiques avant le démarrage d'une session de poste de travail en fonction des informations provenant d'Horizon Client et du Horizon Connection Server.

Par exemple, au lieu de configurer plusieurs pools de postes de travail avec des stratégies différentes, vous pouvez utiliser un script de démarrage de session pour configurer des stratégies de poste de travail en fonction de l'emplacement du périphérique client et de l'utilisateur. Un script de démarrage de session peut activer des lecteurs mappés, la redirection de Presse-papiers et d'autres fonctionnalités de poste de travail pour un utilisateur dont l'adresse IP est située dans le domaine interne de votre organisation, tout en désactivant ces fonctionnalités pour un utilisateur dont l'adresse IP est située dans un domaine externe.

Ce chapitre aborde les rubriques suivantes :

- [Obtention de données d'entrée pour un script de démarrage de session](#)
- [Meilleures pratiques pour l'utilisation de scripts de démarrage de session](#)
- [Préparation d'un poste de travail Horizon 7 pour utiliser un script de démarrage de session](#)
- [Exemples de scripts de démarrage de session](#)

Obtention de données d'entrée pour un script de démarrage de session

Les scripts de démarrage de session ne peuvent pas s'exécuter de manière interactive. Un script de démarrage de session s'exécute dans un environnement créé par Horizon 7 et doit obtenir ses données d'entrée à partir de cet environnement.

Les scripts de démarrage de session collectent les données d'entrée à partir des variables d'environnement sur l'ordinateur client. Les variables d'environnement de démarrage de session ont le préfixe `VDM_StartSession_`. Par exemple, la variable d'environnement de démarrage de session qui contient l'adresse IP du système client est `VDM_StartSession_IP_Address`. Vous devez vous assurer qu'un script de démarrage de session valide l'existence des variables d'environnement qu'il utilise.

Pour obtenir la liste des variables semblables aux variables d'environnement de démarrage de session, reportez-vous à la section « Envoi d'informations sur le système client à des postes de travail distants » du document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Meilleures pratiques pour l'utilisation de scripts de démarrage de session

Suivez ces meilleures pratiques lors de l'utilisation de scripts de démarrage de session.

Conditions d'utilisation des scripts de démarrage de session

Utilisez des scripts de démarrage de session seulement lorsque vous avez besoin de configurer des stratégies de poste de travail avant le démarrage d'une session.

Nous vous recommandons d'utiliser les paramètres de stratégie de groupe Horizon Agent `CommandsToRunOnConnect` et `CommandsToRunOnReconnect` pour exécuter des scripts de commande après une connexion/reconnexion de session de poste de travail. L'exécution de scripts au sein d'une session de poste de travail, au lieu de l'utilisation de scripts de démarrage de session, répond à la plupart des cas d'utilisation.

Pour plus d'informations, reportez-vous à la section « Exécution de commandes sur les postes de travail Horizon » du document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Gérer les délais d'expiration de démarrage de session

Assurez-vous que vos scripts de démarrage de session s'exécutent rapidement.

Si vous définissez la valeur de `WaitScriptsOnStartSession` dans le Registre Windows, l'exécution de votre script de démarrage de session doit se terminer avant qu'Horizon Agent puisse répondre au message `StartSession` envoyé par le Horizon Connection Server. Un script dont l'exécution prend un certain temps est susceptible de provoquer l'expiration de la demande `StartSession`.

Si un délai d'expiration se produit et que le pool utilise des attributions flottantes, le Serveur de connexion tente de connecter l'utilisateur à une autre machine virtuelle. En cas d'expiration du délai et si aucune machine virtuelle n'est disponible, le Serveur de connexion rejette la demande de connexion.

Nous vous recommandons de définir un délai d'expiration fixe pour l'opération de l'hôte de script afin qu'une erreur spécifique puisse être renvoyée en cas d'exécution trop longue d'un script.

Rendre les scripts de démarrage de session accessibles

Le chemin d'accès dans lequel vous configurez vos scripts de démarrage de session doit être accessible uniquement au compte SYSTÈME et aux administrateurs locaux. Définissez la liste de contrôle d'accès de la clé de base pour que seuls ces comptes puissent y accéder.

Nous vous recommandons de placer les scripts de démarrage de session dans le répertoire `View_Agent_install_path\scripts`, par exemple :

```
%ProgramFiles%\VMware\VMware View\Agent\scripts\sample.vbs
```

Par défaut, ce répertoire est accessible uniquement aux comptes SYSTÈME et Administrateur.

Préparation d'un poste de travail Horizon 7 pour utiliser un script de démarrage de session

Pour préparer un poste de travail Horizon 7 afin d'utiliser un script de démarrage de session, vous devez activer le service d'hôte de script VMware View et ajouter des entrées dans le Registre Windows.

Vous devez configurer tous les postes de travail Horizon 7 qui ont besoin d'exécuter des scripts de démarrage de session. Horizon 7 ne fournit pas de mécanisme pour propager les modifications du Registre, les modifications de configuration du service d'hôte de script VMware View et les scripts de démarrage de session vers plusieurs machines virtuelles de poste de travail Horizon 7.

Activer le service d'hôte de script VMware View

Vous devez activer le service d'hôte de script VMware View sur chaque machine virtuelle de poste de travail Horizon 7 sur laquelle vous souhaitez que Horizon 7 exécute un script de démarrage de session. Le service d'hôte de script VMware View est désactivé par défaut.

Lorsque vous configurez le service d'hôte de script VMware View, vous pouvez éventuellement spécifier le compte d'utilisateur sous lequel s'exécute le script de démarrage de session. Les scripts de démarrage de session s'exécutent dans le contexte du service d'hôte de script VMware View. Par défaut, le service d'hôte de script VMware View est configuré pour fonctionner en tant qu'utilisateur SYSTÈME.

Important Les scripts de démarrage de session sont exécutés en dehors d'une session d'utilisateur de poste de travail et non par le compte d'utilisateur de poste de travail. Les informations sont envoyées directement à partir de l'ordinateur client au sein d'un script exécuté en tant qu'utilisateur SYSTÈME.

Procédure

- 1 Connectez-vous à la machine virtuelle de poste de travail Horizon 7.
- 2 À l'invite de commande, tapez `services.msc` pour démarrer l'outil Services Windows.
- 3 Dans le volet de détails, cliquez avec le bouton droit sur l'entrée du service d'hôte de script VMware View, puis sélectionnez **Propriétés**.
- 4 Sous l'onglet **Général**, sélectionnez **Automatique** dans le menu déroulant **Type de démarrage**.
- 5 (Facultatif) Si vous ne voulez pas que le compte Système local exécute le script de démarrage de session, sélectionnez l'onglet **Ouvrir une session**, puis **Ce compte**, et tapez le nom d'utilisateur et le mot de passe du compte pour exécuter le script de démarrage de session.
- 6 Cliquez sur **OK** et quittez l'outil Services Windows.

Ajouter des entrées de Registre Windows pour un script de démarrage de session

Vous devez ajouter les entrées de Registre Windows sur chaque machine virtuelle de poste de travail Horizon sur laquelle vous voulez qu'Horizon exécute un script de démarrage de session.

Prérequis

- Vérifiez que le chemin d'accès dans lequel vous avez configuré vos scripts de démarrage de session n'est accessible qu'au compte SYSTÈME et aux administrateurs locaux. Pour plus d'informations, reportez-vous à la section [Rendre les scripts de démarrage de session accessibles](#).
- Assurez-vous que vos scripts de démarrage de session s'exécutent rapidement. Si vous définissez la valeur de WaitScriptsOnStartSession dans le Registre Windows, l'exécution de votre script de démarrage de session doit se terminer avant qu'Horizon Agent puisse répondre au message StartSession envoyé par le Horizon Connection Server. Pour plus d'informations, reportez-vous à la section [Gérer les délais d'expiration de démarrage de session](#).

Procédure

- 1 Connectez-vous à la machine virtuelle de poste de travail Horizon.
- 2 À l'invite de commande, tapez `regedit` pour démarrer l'Éditeur du Registre de Windows.
- 3 Dans le Registre, accédez à `HKLM\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents`.
- 4 Ajoutez le chemin d'accès au script de démarrage de session au Registre.

- a Dans la zone de navigation, cliquez avec le bouton droit sur `ScriptEvents`, sélectionnez **Nouveau > Clé**, puis créez une clé nommée `StartSession`.
- b Dans la zone de navigation, cliquez avec le bouton droit sur `StartSession`, sélectionnez **Nouveau > Valeur de chaîne**, puis créez une valeur de chaîne qui identifie le script de démarrage de session à exécuter, par exemple, `SampleScript`.

Pour exécuter plusieurs scripts de démarrage de session, créez une entrée de valeur de chaîne pour chaque script sous la clé `StartSession`. Vous ne pouvez pas spécifier l'ordre dans lequel ces scripts s'exécutent. Si les scripts doivent s'exécuter dans un ordre particulier, appelez-les à partir d'un script de contrôle unique.

- c Dans la zone de rubrique, cliquez avec le bouton droit sur l'entrée de la nouvelle valeur de chaîne, puis sélectionnez **Modifier**.
- d Dans le champ **Données de valeur**, tapez la ligne de commande qui appelle le script de démarrage de session, puis cliquez sur **OK**.

Tapez le chemin complet du script de démarrage de session et de tous les fichiers dont il a besoin.

- 5 Ajoutez et activez une valeur de démarrage de session dans le Registre.
 - a Accédez à `HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration`.
 - b (Facultatif) Si la clé `Configuration` n'existe pas, cliquez avec le bouton droit sur **Agent**, sélectionnez **Nouveau > Clé**, puis créez la clé.
 - c Dans la zone de navigation, cliquez avec le bouton droit sur `Configuration`, sélectionnez **Nouveau > Valeur DWORD (32 bits)**, puis tapez `RunScriptsOnStartSession`.

- d Dans la zone de rubrique, cliquez avec le bouton droit sur l'entrée de la nouvelle valeur DWORD, puis sélectionnez **Modifier**.
- e Dans la zone de texte **Données de valeur**, tapez 1 pour activer le script de démarrage de session, puis cliquez sur **OK**.

Vous pouvez taper 0 pour désactiver cette fonctionnalité. La valeur par défaut est 0.

- f (Facultatif) Pour qu'Horizon Agent retarde la réponse StartSession, ajoutez une deuxième valeur DWORD à la clé Configuration nommée WaitScriptsOnStartSession.

Une valeur de donnée de 1 pour WaitScriptsOnStartSession force Horizon Agent à retarder l'envoi d'une réponse StartSession et provoque un échec si les scripts ne se terminent pas. Une valeur de 0 signifie qu'Horizon Agent n'attend pas que les scripts se terminent ou vérifient les codes de sortie de script avant d'envoyer la réponse StartSession. La valeur par défaut est 0.

- 6 Définissez une valeur de Registre pour spécifier les valeurs de délai d'expiration en secondes plutôt qu'en minutes, afin d'empêcher des scripts d'arriver à expiration.

Le fait de définir cette valeur de délai d'expiration en secondes vous permet de configurer également la valeur du délai d'expiration du service d'hôte de script VMware View en secondes. Par exemple, si vous définissez le délai d'expiration du service d'hôte de script VMware View sur 30 secondes, vous pouvez garantir qu'un script de démarrage de session est terminé ou expiré avant la fin d'un délai d'expiration du Serveur de connexion.

- a Accédez à HKLM\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents.
- b Ajoutez une valeur DWORD nommée TimeoutsInMinutes.
- c Définissez une valeur de donnée de 0.

- 7 (Facultatif) Pour permettre au service d'hôte de script VMware View de déclencher l'expiration du script de démarrage de session, définissez une valeur de délai d'expiration.

- a Accédez à HKLM\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents\StartSession.
- b Dans la zone de rubrique, cliquez avec le bouton droit sur la clé Par défaut (@) et sélectionnez **Modifier**.
- c Dans la zone de texte **Données de valeur**, tapez la valeur de délai d'expiration de votre choix, puis cliquez sur **OK**.

Une valeur de 0 signifie qu'aucun délai d'expiration n'est défini.

- 8 Quittez l'Éditeur du Registre, puis redémarrez le système.

Exemples de scripts de démarrage de session

Ces exemples de scripts de démarrage de session montrent comment écrire des variables d'environnement dans un fichier, tester la fonctionnalité de délai d'expiration et tester un code de sortie non nul.

L'exemple de script Visual Basic suivant écrit toutes les variables d'environnement fournies au script dans un fichier. Vous pouvez utiliser cet exemple de script pour afficher les données d'exemple dans votre propre environnement. Vous pouvez enregistrer ce script sous la forme `C:\sample.vbs`.

```
Option Explicit
Dim WshShell, FSO, outFile, strOutputFile, objUserEnv, strEnv

strOutputFile = "c:\setvars.txt"

Set FSO = CreateObject("Scripting.FileSystemObject")
Set outFile = FSO.CreateTextFile(strOutputFile, TRUE)
outFile.WriteLine("Script was called at (" & Now & ")")

Set WshShell = CreateObject( "WScript.Shell" )
Set objUserEnv = WshShell.Environment("PROCESS")
For Each strEnv In objUserEnv
    outFile.WriteLine(strEnv)
Next

outFile.Close
```

L'exemple de script suivant teste la fonctionnalité de délai d'expiration.

```
Option Explicit
WScript.Sleep 60000
```

L'exemple de script suivant teste un code de sortie non nul.

```
Option Explicit
WScript.Quit 2
```