

Horizon 7-Integration

DEZ 2019

VMware Horizon 7 7.11



vmware®

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

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

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2016–2019 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

Horizon 7-Integration	5
1 Einführung in die Horizon 7-Integration	6
Horizon 7-Komponenten	6
Integrationsschnittstellen für Horizon 7	7
2 Integrieren von Horizon 7 in die Ereignisdatenbank	8
Ereignisdatenbanktabellen und -schemas	8
Horizon Connection Server-Ereignisse	11
Horizon Agent-Ereignisse	17
Horizon Administrator-Ereignisse	18
Ereignismeldungsattribute	28
Beispiele für Datenbankabfragen und -ansichten	29
3 Aktivieren von Horizon 7 für cloudgehostete Abonnements und Dienste	32
4 Bereitstellen von Horizon 7 in VMware Cloud on AWS	34
5 Anpassen der LDAP-Daten	35
Einführung in die LDAP-Konfigurationsdaten	35
Ändern von LDAP-Konfigurationsdaten	36
Exportieren von LDAP-Konfigurationsdaten	36
Definieren eines Desktop-Pools in einer LDIF-Konfigurationsdatei	37
Importieren von LDAP-Konfigurationsdaten	40
6 Untersuchen von PCoIP-Sitzungsstatistiken mit WMI	42
Verwenden von PCoIP-Sitzungsstatistiken	42
Allgemeine PCoIP-Sitzungsstatistiken	43
PCoIP-Audiostatistiken	44
PCoIP-Bildverarbeitungsstatistiken	45
PCoIP-Netzwerkstatistiken	46
PCoIP-USB-Statistiken	47
Beispiele für die Verwendung von PowerShell-Cmdlets für die Untersuchung von PCoIP-Statistiken	48
7 Festlegen von Desktop-Richtlinien mit Sitzungsstartskripts	49
Abrufen von Eingabedaten für ein Sitzungsstartskript	49
Best Practices für die Verwendung von Sitzungsstartskripts	50

Vorbereiten eines Horizon 7-Desktops für die Verwendung eines Sitzungsstartskripts	51
Aktivieren des Skriphostdienstes von VMware View	51
Hinzufügen von Windows-Registrierungseinträgen für ein Sitzungsstartskript	51
Beispiele für Sitzungsstartskripts	54

8 Verwenden des Horizon PowerCLI-Moduls 55

Einrichten des Horizon PowerCLI-Moduls	55
Ausführen von Horizon PowerCLI-Beispielskripten	57

Horizon 7-Integration

Im Dokument *Horizon 7-Integration* wird beschrieben, wie Sie die Horizon 7™-Software mit Drittanbieter-Software wie z. B. Windows PowerShell und Business Intelligence-Berichtsmodulen integrieren.

Zielgruppe

Dieses Dokument ist für alle Benutzer gedacht, die Software für die Zusammenarbeit mit Horizon 7 anpassen oder integrieren möchten. Die Informationen in diesem Dokument sind für erfahrene Windows- bzw. Linux-Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und mit Rechenzentrumsvorgängen vertraut sind.

Einführung in die Horizon 7-Integration

1

Mit Horizon 7 können Systemadministratoren Desktops bereitstellen und den Benutzerzugriff auf diese Desktops steuern. Die Clientsoftware verbindet Benutzer mit virtuellen Maschinen, die in VMware vSphere™ ausgeführt werden, oder mit physischen Systemen, die in Ihrer Netzwerkumgebung ausgeführt werden. Darüber hinaus können Horizon 7-Administratoren Remotedesktopdienstehosts (RDS-Hosts) konfigurieren, mit denen Horizon 7-Desktop- und Anwendungssitzungen für Clientgeräte bereitgestellt werden.

Dieses Kapitel enthält die folgenden Themen:

- [Horizon 7-Komponenten](#)
- [Integrationsschnittstellen für Horizon 7](#)

Horizon 7-Komponenten

Sie können Horizon 7 mit VMware vCenter Server verwenden, um Desktops von virtuellen Maschinen zu erstellen, die auf VMware ESX® - oder auf VMware ESXi™-Hosts ausgeführt werden, und diese Desktops für Endbenutzer bereitstellen. Sie können auch Horizon 7 auf RDS-Hosts zur Bereitstellung von Desktops und Anwendungen für Endbenutzer installieren. Horizon 7 nutzt die vorhandene Active Directory-Infrastruktur für die Benutzerauthentifizierung und -verwaltung.

Nach der Erstellung eines Desktops oder einer Anwendung können autorisierte Endbenutzer mit einer webbasierten oder lokal installierten Clientsoftware eine sichere Verbindung mit zentralen virtuellen Maschinen, physischen Back-End-Systemen oder RDS-Hosts herstellen.

Horizon 7 besteht aus den im Folgenden aufgeführten Hauptkomponenten.

Horizon Connection Server

Ein Softwaredienst, der als Broker für Clientverbindungen fungiert, indem er eingehende Benutzeranforderungen authentifiziert und an die entsprechende virtuelle Maschine, an das physische System oder an den RDS-Host weiterleitet.

Horizon Agent

Ein Softwaredienst, der auf allen virtuellen Gastmaschinen, physischen Systemen oder RDS-Hosts installiert ist, damit diese von Horizon 7 verwaltet werden können. Horizon Agent bietet Funktionen wie eine

	Verbindungsüberwachung, virtuelles Drucken, eine USB-Unterstützung und eine Single-Sign-On-Anmeldung.
Horizon Client	Eine Softwareanwendung, die mit dem Verbindungsserver kommuniziert, damit Benutzer eine Verbindung mit ihren Desktops herstellen können.
Horizon Administrator	Eine Webanwendung, mit der Horizon 7-Administratoren den Verbindungsserver konfigurieren, Desktop- und Anwendungspools bereitstellen, Maschinen verwalten, die Benutzerauthentifizierung steuern, Systemereignisse initiieren und untersuchen sowie Analysen durchführen können.
vCenter Server	Ein Server, der als zentraler Administrator für ESX/ESXi-Hosts fungiert, die über ein Netzwerk miteinander verbunden sind. Eine vCenter Server-Instanz ist die zentrale Komponente für die Konfiguration, Bereitstellung und Verwaltung virtueller Maschinen im Rechenzentrum.
View Composer	Ein Softwaredienst, der auf einer vCenter Server-Instanz installiert ist, damit Horizon 7 mehrere Linked-Clone-Desktops aus einem einzigen zentralen Basis-Image auf schnelle Weise bereitstellen kann.

Integrationsschnittstellen für Horizon 7

Sie können mehrere Schnittstellen für die Integration von Horizon 7 in externe Anwendungen verwenden.

Ereignisdatenbank	Sie können Horizon 7 so konfigurieren, dass Ereignisse in einer Microsoft SQL Server- oder Oracle-Datenbank aufgezeichnet werden. Anschließend haben Sie die Möglichkeit, mit Business Intelligence-Berichterstellungsprogrammen auf diese Datenbank zuzugreifen und diese zu analysieren.
Lightweight Directory Access Protocol (LDAP)	Sie können LDAP-Konfigurationsdaten nach Horizon 7 exportieren und von dort importieren. Sie können Skripts erstellen, mit denen sich diese Konfigurationsdaten ohne direkten Zugriff auf Horizon Administrator aktualisieren lassen.
Windows-Verwaltungsinstrumentation (WMI)	Sie können die Leistungsstatistiken für eine PCoIP-Sitzung untersuchen.

Integrieren von Horizon 7 in die Ereignisdatenbank

2

Sie können Horizon 7 so konfigurieren, dass Ereignisse in einer Microsoft SQL Server- oder Oracle-Datenbank aufgezeichnet werden. Horizon 7 zeichnet Ereignisse wie Endbenutzeraktionen, Administratoraktionen, Warnungen, die Systemausfälle und Fehler melden, sowie statistische Abfragen auf.

Endbenutzeraktionen umfassen die Protokollierung und das Starten von Desktop- und Anwendungssitzungen. Zu den Administratoraktionen gehören das Hinzufügen von Berechtigungen und das Erstellen von Desktop- und Anwendungspools. Ein Beispiel für statistische Abfragen ist die Aufzeichnung der maximalen Anzahl der Benutzer über einen Zeitraum von 24 Stunden.

Anhand von Business Intelligence-Berichterstellungsprogrammen wie Crystal Reports, IBM Cognos, MicroStrategy 9 und Oracle Enterprise Performance Management System können Sie auf die Ereignisdatenbank zugreifen und diese analysieren.

Dieses Kapitel enthält die folgenden Themen:

- [Ereignisdatenbanktabellen und -schemas](#)
- [Horizon Connection Server-Ereignisse](#)
- [Horizon Agent-Ereignisse](#)
- [Horizon Administrator-Ereignisse](#)
- [Ereignismeldungsattribute](#)
- [Beispiele für Datenbankabfragen und -ansichten](#)

Ereignisdatenbanktabellen und -schemas

Horizon 7 verwendet Datenbanktabellen zur Implementierung der Ereignisdatenbank. Die Ereignisdatenbank stellt den Namen dieser Tabellen ein Präfix voran, das Sie bei der Einrichtung der Datenbank definieren.

Ereignisdatenbanktabellen

Die folgende Tabelle zeigt die Datenbanktabellen, die die Ereignisdatenbank in Horizon 7 implementieren.

Tabelle 2-1. Ereignisdatenbanktabellen

Tabellenname	Beschreibung
event	Metadaten und Suchoptimierungsdaten für die letzten Ereignisse.
event_data	Datenwerte für die letzten Ereignisse.
event_data_historical	Datenwerte für alle Ereignisse.
event_historical	Metadaten und Suchoptimierungsdaten für alle Ereignisse.

Horizon 7 zeichnet Einzelheiten zu Ereignissen für alle Datenbanktabellen auf. Nach einem bestimmten Zeitraum nach der Erfassung eines Ereignisdatensatzes löscht Horizon 7 den Datensatz aus den event- und event_data-Tabellen. Sie können mit Horizon Administrator den Zeitraum konfigurieren, in dem ein Datensatz in den event- und event_data-Tabellen gespeichert bleibt.

Wichtig Die Größe der event_historical- und event_data_historical-Tabellen ist in Horizon 7 nicht beschränkt. Sie müssen für diese Tabellen eine Richtlinie zur Speicherplatzverwaltung implementieren.

Ein eindeutiger Primärschlüssel, die Ereignis-ID, identifiziert jedes Ereignis, das Horizon 7 in den event- und event_historical Tabellen aufzeichnet. Horizon 7 erfasst Datenwerte für jedes Ereignis in den event_data- und event_data_historical-Tabellen. Sie können die gesamten Informationen für ein Ereignis abrufen, indem Sie die event- und event_data-Tabellen oder die event_historical- und event_data_historical-Tabellen über die Spalte „EventID“ (Ereignis-ID) verknüpfen.

Die Spalten „EventType“ (Ereignistyp), „Severity“ (Schweregrad) und „Time“ (Uhrzeit) in den event- und event_historical-Tabellen geben den Typ und den Schweregrad eines Ereignisses sowie den Zeitpunkt wieder, an dem es aufgetreten ist.

Informationen zum Einrichten der Ereignisdatenbank finden Sie im Dokument *Horizon 7-Installation*.

Hinweis Informationen zum Löschen von Daten in den Verlaufstabellen finden Sie unter <http://kb.vmware.com/kb/2150309>.

Ereignisdatenbankschemas

Die folgende Tabelle zeigt das Schema für die event- und event_historical-Datenbanktabellen.

Tabelle 2-2. Schema für die event- und event_historical-Tabellen

Spaltenname	Oracle-Datentyp	SQL Server-Datentyp	Beschreibung
Acknowledged	SMALLINT	tinyint	Gibt an, ob Horizon 7 das Ereignis bestätigt hat. ■ 0 = Falsch ■ 1 = Wahr
DesktopId	NVARCHAR2(512)	nvarchar(512)	Desktop-ID des zugeordneten Pools.
EventID	INTEGER	int	Eindeutiger Primärschlüssel für das Ereignis.
Ereignistyp	NVARCHAR2(512)	nvarchar(512)	Name des Ereignisses, der einem Element im Meldungskatalog entspricht. Beispiel: BROKER_USERLOGGEDIN.

Tabelle 2-2. Schema für die event- und event_historical-Tabellen (Fortsetzung)

Spaltenname	Oracle-Datentyp	SQL Server-Datentyp	Beschreibung
FolderPath	NVARCHAR2(512)	nvarchar(512)	Der vollständige Pfad des Ordners, der das zugeordnete Objekt enthält.
GroupId	NVARCHAR2(512)	nvarchar(512)	Die SID der zugeordneten Gruppe in Active Directory.
LUNId	NVARCHAR2(512)	nvarchar(512)	ID der LUN, die das zugeordnete Objekt speichert.
MachineId	NVARCHAR2(512)	nvarchar(512)	ID des zugeordneten physischen Computers oder der zugeordneten virtuellen Maschine.
Modul	NVARCHAR2(512)	nvarchar(512)	Horizon 7-Komponente, die das Ereignis ausgelöst hat. Beispielsweise Administrator, Broker, Tunnel, Framework, Client oder Agent.
ModuleAndEventText	NVARCHAR2(512)	nvarchar(512)	Ereignismeldung mit Werten für Attributparameter.
Node	NVARCHAR2(512)	nvarchar(512)	Name des Knoten des virtuellen Geräts.
Schweregrad	NVARCHAR2(512)	nvarchar(512)	Schweregrad. Beispielsweise INFO, WARNING, ERROR, AUDIT_SUCCESS, AUDIT_FAIL.
Quelle	NVARCHAR2(512)	nvarchar(512)	Bezeichner für die Quelle des Ereignisses.
ThinAppId	NVARCHAR2(512)	nvarchar(512)	ID des zugeordneten ThinApp™-Objekts.
Uhrzeit	ZEITSTEMPEL	datetime	Zeitpunkt, an dem das Ereignis aufgetreten ist, gemessen ab 1. Januar 1970.
UserDiskPathId	NVARCHAR2(512)	nvarchar(512)	ID für die Benutzerfestplatte.
UserSID	NVARCHAR2(512)	nvarchar(512)	Die SID des zugeordneten Benutzers in Active Directory.

Die folgende Tabelle zeigt das Schema für die event_data- und event_data_historical-Datenbanktabellen.

Tabelle 2-3. Schema für die event_data- und event_data_historical-Tabellen

Spaltenname	Oracle-Datentyp	SQL Server-Datentyp	Beschreibung
BooleanValue	SMALLINT	tinyint	Wert eines booleschen Attributs. ■ 0 = Falsch ■ 1 = Wahr
EventID	INTEGER	int	Eindeutiger Primärschlüssel für das Ereignis.
IntValue	INTEGER	int	Wert eines Ganzzahlattributs.
Name	NVARCHAR2(512)	nvarchar(512)	Attributname (z. B. UserDisplayName).
StrValue	NVARCHAR2(512)	nvarchar(512)	Wert eines Zeichenfolgenattributs. Für andere Arten von Attributen enthält diese Spalte eine Interpretation des Datentyps als Zeichenfolge.

Tabelle 2-3. Schema für die event_data- und event_data_historical-Tabellen (Fortsetzung)

Spaltenname	Oracle-Datentyp	SQL Server-Datentyp	Beschreibung
TimeValue	ZEITSTEMPEL	datetime	Wert eines Datums/Uhrzeit-Attributs.
Typ	SMALLINT	tinyint	Der Datentyp des Attributs. <ul style="list-style-type: none"> ■ 0 = Zeichenfolge ■ 1 = Ganzzahl ■ 2 = Zeitangabe ■ 3 = Boolescher Wert

Horizon Connection Server-Ereignisse

Horizon Connection Server-Ereignisse zeichnen Informationen im Zusammenhang mit dem Verbindungsserver auf, wie z. B. Desktop- und Anwendungssitzungen, Fehler der Benutzerauthentifizierung und Bereitstellungsfehler.

Das Ereignis `BROKER_DAILY_MAX_DESKTOP_SESSIONS` zeichnet die maximale Anzahl der gleichzeitigen Desktop-Sitzungen über einen Zeitraum von 24 Stunden auf. Wenn ein Benutzer mehrere Desktop-Sitzungen gleichzeitig ausführt, wird jede Desktop-Sitzung separat gezählt.

Das Ereignis `BROKER_DAILY_MAX_APP_USERS` zeichnet die maximale Anzahl gleichzeitiger Benutzer über einen Zeitraum von 24 Stunden auf. Wenn ein Benutzer mehrere Anwendungen gleichzeitig ausführt, wird der Benutzer nur einmal gezählt. Es kann sein, dass kurzlebige Sitzungen nicht in der Zählung enthalten sind, da die Abfrage alle fünf Minuten durchgeführt wird.

Die Ereignisse `BROKER_VC_DISABLED` und `BROKER_VC_ENABLED` zeichnen den Status des vCenter-Treibers auf, den Horizon 7 zur Nachverfolgung einer vCenter Server-Instanz verwendet.

Die Ereignisse `BROKER_VC_STATUS_*` zeichnen den Status der vCenter Server-Instanz auf.

Die folgende Tabelle enthält alle Ereignistypen des Verbindungsservers.

Tabelle 2-4. Verbindungsserver-Ereignisse

Ereignistyp	Schweregrad	ModuleAndEventText
<code>BROKER_AGENT_OFFLINE</code>	WARNUNG	Der Agent, der auf Computer \${MachineName} ausgeführt wird, hat nicht auf Anfragen reagiert. Kennzeichnung als „Offline“
<code>BROKER_AGENT_ONLINE</code>	WARNUNG	Der Agent, der auf Computer \${MachineName} ausgeführt wird, reagiert zwar wieder, hat aber keine Startmeldung gesendet
<code>BROKER_APPLICATION_LAUNCH_FAILURE</code>	FEHLER	Start von Pool \${PoolId} zur Benutzer \$ {UserDisplayName} nicht möglich: Bei der Verarbeitung der Anforderung ist im Broker ein Fehler aufgetreten; wenden Sie sich zur Unterstützung an den Support
<code>BROKER_APPLICATION_MISSING</code>	WARNUNG	Mindestens \${ApplicationMissingCount} Anwendungen, darunter \${ApplicationExecutable}, sind nicht auf \$ {MachineName} in Pool \${PoolId} installiert

Tabelle 2-4. Verbindungsserver-Ereignisse (Fortsetzung)

Ereignistyp	Schweregrad	ModuleAndEventText
BROKER_APPLICATION_NOT_ENTITLED	AUDIT_FAIL	Start von Pool \${PoolId} für Benutzer \$ {UserDisplayName} nicht möglich: Benutzer ist nicht für den Zugriff auf diesen Pool berechtigt
BROKER_APPLICATION_PROTOCOL_NOT_SUPPORTED	AUDIT_FAIL	Start von Pool \${PoolId} für Benutzer \$ {UserDisplayName} nicht möglich: Das angeforderte Protokoll \${ProtocolId} wird nicht unterstützt
BROKER_APPLICATION_REQUEST	INFO	Benutzer \${UserDisplayName} hat Anwendung \$ {ApplicationId} angefordert
BROKER_APPLICATION_SESSION_REQUEST	INFO	Benutzer \${UserDisplayName} hat eine Anwendungssitzung von Pool \${PoolId} angefordert
BROKER_DAILY_MAX_DESKTOP_SESSIONS	INFO	\$(Time): In den letzten 24 Stunden belief sich die maximale Anzahl paralleler Desktop-Sitzungen auf \$ {UserCount})
BROKER_DAILY_MAX_APP_USERS	INFO	\$(Time): In den letzten 24 Stunden belief sich die maximale Anzahl an Benutzern mit parallelen Anwendungssitzungen auf \${UserCount})
BROKER_DESKTOP_LAUNCH_FAILURE	FEHLER	Start von Pool \${DesktopId} zur Benutzer \$ {UserDisplayName} nicht möglich: Bei der Verarbeitung der Anforderung ist im Broker ein Fehler aufgetreten; wenden Sie sich zur Unterstützung an den Support
BROKER_DESKTOP_NOT_ENTITLED	AUDIT_FAIL	Start von Pool \${DesktopId} für Benutzer \$ {UserDisplayName} nicht möglich: Benutzer ist nicht für den Zugriff auf diesen Pool berechtigt
BROKER_DESKTOP_PROTOCOL_NOT_SUPPORTED	AUDIT_FAIL	Start von Pool \${DesktopId} für Benutzer \$ {UserDisplayName} nicht möglich: Das angeforderte Protokoll \${ProtocolId} wird nicht unterstützt
BROKER_DESKTOP_REQUEST	INFO	Benutzer \${UserDisplayName} hat Pool \${DesktopId} angefordert
BROKER_EVENT_HANDLING_STARTED	INFO	Broker \${BrokerName} hat mit der Verarbeitung der Ereignisse begonnen
BROKER_EVENT_HANDLING_STOPPED	INFO	\$(BrokerName) hat die Verarbeitung der Ereignisse abgebrochen
BROKER_MACHINE_ALLOCATED	INFO	Benutzer \${UserDisplayName} hat Pool \${DesktopId} angefordert; zugewiesener Computer \${MachineName}
BROKER_MACHINE_ASSIGNED_UNAVAILABLE	AUDIT_FAIL	Start von Pool \${DesktopId} für Benutzer \$ {UserDisplayName} nicht möglich: Der zugewiesene Computer \${MachineName} ist nicht verfügbar
BROKER_MACHINE_CANNOT_CONNECT	AUDIT_FAIL	Start von Pool \${DesktopId} für Benutzer \$ {UserDisplayName} nicht möglich: Verbindung mit Computer \${MachineName} über \${ProtocolId} nicht möglich
BROKER_MACHINE_CONFIGURED_VIDEO_SETTINGS	INFO	Video-Einstellungen für Computer/VM \$ {MachineName} in Pool \${DesktopId} erfolgreich konfiguriert

Tabelle 2-4. Verbindungsserver-Ereignisse (Fortsetzung)

Ereignistyp	Schweregrad	ModuleAndEventText
BROKER_MACHINE_NOT_READY	WARNUNG	Start von Pool \${DesktopId} für Benutzer \$ {UserDisplayName} nicht möglich: Computer \$ {MachineName} ist zur Zulassung von Verbindungen nicht bereit
BROKER_MACHINE_OPERATION_DELETED	INFO	Computer \${MachineName} wurde gelöscht
BROKER_MACHINE_PROTOCOL_NOT_SUPPORTED	AUDIT_FAIL	Start von Pool \${DesktopId} für Benutzer \$ {UserDisplayName} nicht möglich: Computer \$ {MachineName} bietet keine Unterstützung für Protokoll \${ProtocolId}
BROKER_MACHINE_PROTOCOL_UNAVAILABLE	AUDIT_FAIL	Start von Pool \${DesktopId} für Benutzer \$ {UserDisplayName} nicht möglich: Computer \$ {MachineName} hat Protokoll \${ProtocolId} nicht als "Bereit" gemeldet
BROKER_MACHINE_REJECTED_SESSION	WARNUNG	Start von Pool \${DesktopId} für Benutzer \$ {UserDisplayName} nicht möglich: Computer \$ {MachineName} hat die Anforderung zum Sitzungsstart abgelehnt
BROKER_MACHINE_SESSION_TIMEOUT	WARNUNG	Zeitüberschreitung bei Sitzung für Benutzer \$ {UserDisplayName}
BROKER_MULTIPLE_DESKTOPS_FOR_KIOSK_USER	WARNUNG	Benutzer \${UserDisplayName} ist für den Zugriff auf mehrere Desktop-Pools berechtigt
BROKER_POOL_CANNOT_ASSIGN	AUDIT_FAIL	Start von Pool \${DesktopId} für Benutzer \$ {UserDisplayName} nicht möglich: Es sind keine Computer verfügbar, denen der Benutzer zugewiesen werden kann
BROKER_POOL_COMANAGER_REQUIRED	AUDIT_FAIL	Start von Pool \${DesktopId} für Benutzer \$ {UserDisplayName} nicht möglich: Für Protokoll \$ {ProtocolId} ist keine Mitbestimmungsoption verfügbar
BROKER_POOL_EMPTY	AUDIT_FAIL	Start von Pool \${DesktopId} für Benutzer \$ {UserDisplayName} nicht möglich: Der Desktop-Pool ist leer
BROKER_POOL_NO_MACHINE_ASSIGNED	AUDIT_FAIL	Start von Pool \${DesktopId} für Benutzer \$ {UserDisplayName} nicht möglich: Diesem Benutzer ist kein Computer zugewiesen
BROKER_POOL_NO_RESPONSES	AUDIT_FAIL	Start von Pool \${DesktopId} für Benutzer \$ {UserDisplayName} nicht möglich: Keiner der Computer in diesem Desktop-Pool reagiert
BROKER_POOL_OVERLOADED	AUDIT_FAIL	Start von Pool \${DesktopId} für Benutzer \$ {UserDisplayName} nicht möglich: Alle reagierenden Computer werden aktuell verwendet
BROKER_POOL_POLICY_VIOLATION	AUDIT_FAIL	Start von Pool \${DesktopId} für Benutzer \$ {UserDisplayName} nicht möglich: Dieser Desktop-Pool lässt keine Onlinesitzungen zu

Tabelle 2-4. Verbindungsserver-Ereignisse (Fortsetzung)

Ereignistyp	Schweregrad	ModuleAndEventText
BROKER_POOL_PROTOCOL_NOT_SUPPORTED	AUDIT_FAIL	Start von Pool \${DesktopId} für Benutzer \${UserDisplayName} nicht möglich: Es sind keine Computer verfügbar, die das Protokoll \${ProtocolId} unterstützen
BROKER_POOL_PROTOCOL_UNAVAILABLE	AUDIT_FAIL	Start von Pool \${DesktopId} für Benutzer \${UserDisplayName} nicht möglich: Es sind keine Computer verfügbar, die das Protokoll \${ProtocolId} als "Bereit" gemeldet haben
BROKER_POOL_TUNNEL_NOT_SUPPORTED	AUDIT_FAIL	Start von Pool \${DesktopId} für Benutzer \${UserDisplayName} nicht möglich: Tunneling wird nicht unterstützt für Protokoll \${ProtocolId}
BROKER_PROVISIONING_ERROR_CONFIG_CLEARED	INFO	Das zuvor gemeldete Konfigurationsproblem liegt für Pool \${DesktopId} nicht mehr vor
BROKER_PROVISIONING_ERROR_CONFIG_SET	FEHLER	Bereitstellungsfehler bei Pool \${DesktopId} aufgrund eines Konfigurationsproblems
BROKER_PROVISIONING_ERROR_DISK_CLEARED	INFO	Das zuvor gemeldete Festplattenproblem liegt für Pool \${DesktopId} nicht mehr vor
BROKER_PROVISIONING_ERROR_DISK_LC_RESERVATION_CLEARED	INFO	Der zuvor gemeldete Fehler aufgrund des für verknüpfte Klon reservierten verfügbaren Speicherplatzes auf der Festplatte liegt für Pool \${DesktopId} nicht mehr vor
BROKER_PROVISIONING_ERROR_DISK_LC_RESERVATION_SET	FEHLER	Bereitstellungsfehler für Pool \${DesktopId}, da der verfügbare Speicherplatz auf der Festplatte für verknüpfte Klon reserviert ist
BROKER_PROVISIONING_ERROR_DISK_SECT	WARNUNG	Bereitstellungsfehler bei Pool \${DesktopId} aufgrund eines Festplattenproblems
BROKER_PROVISIONING_ERROR_LICENCE_CLEARED	INFO	Das zuvor gemeldete Lizenzierungsproblem liegt für Pool \${DesktopId} nicht mehr vor
BROKER_PROVISIONING_ERROR_LICENCE_SET	FEHLER	Bereitstellungsfehler bei Pool \${DesktopId} aufgrund eines Lizenzierungsproblems
BROKER_PROVISIONING_ERROR_NETWORKING_CLEARED	INFO	Das zuvor gemeldete Netzwerkproblem mit Horizon Agent liegt für Pool \${DesktopId} nicht mehr vor
BROKER_PROVISIONING_ERROR_NETWORKING_SET	FEHLER	Bereitstellungsfehler bei Pool \${DesktopId} aufgrund eines Netzwerkproblems mit Horizon Agent
BROKER_PROVISIONING_ERROR_RESOURCE_CLEARED	INFO	Das zuvor gemeldete Ressourcenproblem liegt für Pool \${DesktopId} nicht mehr vor
BROKER_PROVISIONING_ERROR_RESOURCE_SET	FEHLER	Bereitstellungsfehler bei Pool \${DesktopId} aufgrund eines Ressourcenproblems
BROKER_PROVISIONING_ERROR_TIMEOUT_CUSTOMIZATION_CLEARED	INFO	Die zuvor gemeldete Zeitüberschreitung bei der Anpassung liegt für Pool \${DesktopId} nicht mehr vor
BROKER_PROVISIONING_ERROR_TIMEOUT_CUSTOMIZATION_SET	FEHLER	Bereitstellungsfehler bei Pool \${DesktopId} aufgrund einer Zeitüberschreitung bei der Anpassung

Tabelle 2-4. Verbindungsserver-Ereignisse (Fortsetzung)

Ereignistyp	Schweregrad	ModuleAndEventText
BROKER_PROVISIONING_ERROR_VM_CLONING	FEHLER	Bereitstellungsfehler für Computer \${MachineName}: Klonen für Computer fehlgeschlagen
BROKER_PROVISIONING_ERROR_VM_CUSTOMIZATION_ERROR	FEHLER	Bereitstellungsfehler für Computer \${MachineName}: Anpassung für Computer fehlgeschlagen
BROKER_PROVISIONING_ERROR_VM_CUSTOMIZATION_NETWORKING	FEHLER	Bereitstellungsfehler für Computer \${MachineName}: Anpassungsfehler aufgrund fehlender Netzwerkkommunikation zwischen Horizon Agent und dem Verbindungsserver
BROKER_PROVISIONING_ERROR_VM_CUSTOMIZATION_TIMEOUT	FEHLER	Bereitstellungsfehler für Computer \${MachineName}: Zeitüberschreitung bei Anpassungsvorgang
BROKER_PROVISIONING_SVI_ERROR_COMPOSER_AGENT_INIT_FAILED	FEHLER	Bereitstellungsfehler für Computer \${MachineName}: Initialisierung für View Composer-Agent fehlgeschlagen
BROKER_PROVISIONING_SVI_ERROR_RECONFIG_FAILED	FEHLER	Bereitstellungsfehler für Computer \${MachineName}: Neukonfigurationsvorgang ist fehlgeschlagen
BROKER_PROVISIONING_SVI_ERROR_REFIT_FAILED	FEHLER	Bereitstellungsfehler für Computer \${MachineName}: Neuanpassung \${SVIOperation} fehlgeschlagen
BROKER_PROVISIONING_SVI_ERROR_REMOVING_VM	FEHLER	Bereitstellungsfehler für Computer \${MachineName}: Computer kann nicht aus Bestandsliste entfernt werden
BROKER_PROVISIONING_VERIFICATION_FAILED_USER_ASSIGNED	WARNUNG	Fehler bei Bereitstellungsverifizierung für Computer \${MachineName}: Der Benutzer ist bereits einem Computer im Pool \${DesktopId} zugewiesen
BROKER_PROVISIONING_VERIFICATION_FAILED_USER_CANNOT_BE_ASSIGNED	WARNUNG	Fehler bei Bereitstellungsverifizierung für Computer \${MachineName}: Es kann kein Benutzer zugewiesen werden, da der Pool \${DesktopId} nicht persistent ist
BROKER_PROVISIONING_VERIFICATION_FAILED_VMNAME_IN_USE	WARNUNG	Fehler bei Bereitstellungsverifizierung für Computer \${MachineName}: In Pool \${DesktopId} liegt bereits ein Computer mit dem Namen \${MachineName} vor
BROKER_SECURITY_SERVER_ADD_FAILED	AUDIT_FAIL	Sicherheitsserver \${SecurityServerId} konnte nicht hinzugefügt werden
BROKER_SECURITY_SERVER_ADD_FAILED_PASSWORD_EXPIRED	AUDIT_FAIL	Sicherheitsserver \${SecurityServerId} konnte nicht hinzugefügt werden; Kennwort für die Kombination ist abgelaufen
BROKER_SECURITY_SERVER_ADD_FAILED_PASSWORD_INCORRECT	AUDIT_FAIL	Sicherheitsserver \${SecurityServerId} konnte nicht hinzugefügt werden; Kennwort für die Kombination ist falsch
BROKER_SECURITY_SERVER_ADD_FAILED_PASSWORD_NOT_SET	AUDIT_FAIL	Sicherheitsserver \${SecurityServerId} konnte nicht hinzugefügt werden; Kennwort für die Kombination wurde nicht festgelegt
BROKER_SECURITY_SERVER_ADDED	AUDIT_SUCCESS	Sicherheitsserver \${SecurityServerId} hinzugefügt
BROKER_SVI_ARCHIVE_UDD_FAILED	AUDIT_FAIL	Benutzerdaten-Festplatte \${UserDiskName} konnte nicht unter Speicherort \${SVIPath} archiviert werden
BROKER_SVI_ARCHIVE_UDD_SUCCEEDED	AUDIT_SUCCESS	Benutzerdaten-Festplatte \${UserDiskName} wurde unter Speicherort \${SVIPath} archiviert

Tabelle 2-4. Verbindungsserver-Ereignisse (Fortsetzung)

Ereignistyp	Schweregrad	ModuleAndEventText
BROKER_SVI_ATTACH_UDD_FAILED	AUDIT_FAIL	Benutzerdaten-Festplatte \${UserDiskName} konnte nicht mit VM \${SVIVMID} verknüpft werden
BROKER_SVI_ATTACH_UDD_SUCCEEDED	AUDIT_SUCCESS	Benutzerdaten-Festplatte \${UserDiskName} wurde mit VM \${SVIVMID} verknüpft
BROKER_SVI_DETACH_UDD_FAILED	AUDIT_FAIL	Benutzerdaten-Festplatte \${UserDiskName} konnte nicht von VM \${SVIVMID} getrennt werden
BROKER_SVI_DETACH_UDD_SUCCEEDED	AUDIT_SUCCESS	Benutzerdatenfestplatte \${UserDiskName} wurde von VM \${SVIVMID} getrennt
BROKER_USER_AUTHFAILED_ACCOUNT_DISABLED	AUDIT_FAIL	Benutzer \${UserDisplayName} konnte nicht authentifiziert werden, da das Konto deaktiviert wurde
BROKER_USER_AUTHFAILED_ACCOUNT_EXPIRED	AUDIT_FAIL	Benutzer \${UserDisplayName} konnte nicht authentifiziert werden, da das Konto abgelaufen ist
BROKER_USER_AUTHFAILED_ACCOUNT_LOCKED_OUT	AUDIT_FAIL	Benutzer \${UserDisplayName} konnte nicht authentifiziert werden, da das Konto gesperrt wurde
BROKER_USER_AUTHFAILED_ACCOUNT_RESTRICTION	AUDIT_FAIL	Benutzer \${UserDisplayName} konnte nicht authentifiziert werden, da eine Einschränkung für das Konto besteht
BROKER_USER_AUTHFAILED_BAD_USER_PASSWORD	AUDIT_FAIL	Benutzer \${UserDisplayName} konnte aufgrund eines ungültigen Benutzernamens oder Kennworts nicht authentifiziert werden
BROKER_USER_AUTHFAILED_GENERAL	AUDIT_FAIL	Benutzer \${UserDisplayName} konnte nicht authentifiziert werden
BROKER_USER_AUTHFAILED_NO_LOGON_SERVERS	AUDIT_FAIL	Benutzer \${UserDisplayName} konnte nicht authentifiziert werden, da keine Anmeldeserver verfügbar sind
BROKER_USER_AUTHFAILED_PASSWORD_EXPIRED	AUDIT_FAIL	Benutzer \${UserDisplayName} konnte nicht authentifiziert werden, da das Kennwort abgelaufen ist
BROKER_USER_AUTHFAILED_PASSWORD_MUST_CHANGE	AUDIT_FAIL	Benutzer \${UserDisplayName} konnte nicht authentifiziert werden, da das Kennwort geändert werden muss
BROKER_USER_AUTHFAILED_SECUREID_ACCESS_DENIED	AUDIT_FAIL	SecurID-Zugriff verweigert für Benutzer \${UserDisplayName}
BROKER_USER_AUTHFAILED_SECUREID_NEWPIN_REJECTED	AUDIT_FAIL	SecurID-Zugriff verweigert für Benutzer \${UserDisplayName}, da die neue PIN abgelehnt wurde
BROKER_USER_AUTHFAILED_SECUREID_WRONG_NEXTTOKEN	AUDIT_FAIL	SecurID-Zugriff verweigert für Benutzer \${UserDisplayName} aufgrund eines falsch eingegebenen nächsten Tokens
BROKER_USER_AUTHFAILED_SECUREID_WRONG_STATE	AUDIT_FAIL	SecurID-Zugriff verweigert für Benutzer \${UserDisplayName} aufgrund eines inkorrekten Status
BROKER_USER_AUTHFAILED_TIME_RESTRICTION	AUDIT_FAIL	Benutzer \${UserDisplayName} konnte nicht authentifiziert werden, da eine Zeitbeschränkung besteht

Tabelle 2-4. Verbindungsserver-Ereignisse (Fortsetzung)

Ereignistyp	Schweregrad	ModuleAndEventText
BROKER_USER_NOT_AUTHORIZED	AUDIT_FAIL	Benutzer \${UserDisplayName} wurde authentifiziert, ist aber nicht für die Durchführung des Vorgangs berechtigt
BROKER_USER_NOT_ENTITLED	AUDIT_FAIL	Benutzer \${UserDisplayName} wurde authentifiziert, ist aber nicht für den Zugriff auf Pools berechtigt
BROKER_USERCHANGEDPASSWORD	AUDIT_SUCCESS	Kennwort für \${UserDisplayName} wurde vom Benutzer geändert
BROKER_USERLOGGEDIN	AUDIT_SUCCESS	Benutzer \${UserDisplayName} hat sich angemeldet
BROKER_USERLOGGEDOUT	AUDIT_SUCCESS	Benutzer \${UserDisplayName} hat sich abgemeldet
BROKER_VC_DISABLED	INFO	vCenter unter Adresse \${VCAddress} wurde vorübergehend deaktiviert
BROKER_VC_ENABLED	INFO	vCenter unter Adresse \${VCAddress} wurde aktiviert
BROKER_VC_STATUS_CHANGED_CANNOT_LOGIN	WARNUNG	Anmeldung bei vCenter unter der Adresse \${VCAddress} nicht möglich
BROKER_VC_STATUS_CHANGED_DOWN	INFO	vCenter unter Adresse \${VCAddress} ist nicht aktiv
BROKER_VC_STATUS_CHANGED_INVALID_CREDENTIALS	WARNUNG	vCenter unter Adresse \${VCAddress} verfügt über ungültige Anmeldeinformationen
BROKER_VC_STATUS_CHANGED_NOT_YET_CONNECTED	INFO	Verbindung mit vCenter unter Adresse \${VCAddress} noch nicht hergestellt
BROKER_VC_STATUS_CHANGED_RECONNECTING	INFO	Verbindung mit vCenter unter Adresse \${VCAddress} wird erneut hergestellt
BROKER_VC_STATUS_CHANGED_UNKNOWN	WARNUNG	Der Status von vCenter unter Adresse \${VCAddress} ist unbekannt
BROKER_VC_STATUS_CHANGED_UP	INFO	vCenter unter Adresse \${VCAddress} ist aktiv

Horizon Agent-Ereignisse

Horizon Agent-Ereignisse zeichnen Horizon Agent-bezogene Informationen auf, z. B. welche Benutzer sich bei einem bestimmten Computer angemeldet oder abgemeldet haben, ob Horizon Agent auf einem bestimmten Computer heruntergefahren wurde und ob Horizon Agent eine Startmeldung von einem bestimmten Computer an den Horizon Connection Server gesendet hat.

Tabelle 2-5. Horizon Agent-Ereignisse

Ereignistyp	Schweregrad	ModuleAndEventText
AGENT_CONNECTED	INFO	Benutzer \${UserDisplayName} hat sich an einer neuen Sitzung auf Computer \${MachineName} angemeldet
AGENT_DISCONNECTED	INFO	Benutzer \${UserDisplayName} hat die Verbindung zu Computer \${MachineName} getrennt
AGENT_ENDED	INFO	Benutzer \${UserDisplayName} hat sich von Computer \${MachineName} abgemeldet

Tabelle 2-5. Horizon Agent-Ereignisse (Fortsetzung)

Ereignistyp	Schweregrad	ModuleAndEventText
AGENT_PENDING	INFO	Der auf Computer \${MachineName} ausgeführte Agent hat eine zugewiesene Sitzung für Benutzer \${UserDisplayName} akzeptiert
AGENT_PENDING_EXPIRED	WARNUNG	Die laufende Sitzung auf Computer \${MachineName} für Benutzer \${UserDisplayName} ist abgelaufen
AGENT_RECONFIGURED	INFO	Computer \${MachineName} wurde erfolgreich neu konfiguriert
AGENT_RECONNECTED	INFO	Benutzer \${UserDisplayName} hat die Verbindung zu Computer \${MachineName} erneut hergestellt
AGENT_RESUME	INFO	Der Agent auf Computer \${MachineName} hat eine Fortsetzungsmeldung gesendet
AGENT_SHUTDOWN	INFO	Der auf Computer \${MachineName} ausgeführte Agent wurde heruntergefahren; dieser Computer ist nicht mehr verfügbar
AGENT_STARTUP	INFO	Der auf Computer \${MachineName} ausgeführte Agent hat den Verbindungsserver kontaktiert und eine Startmeldung gesendet
AGENT_SUSPEND	INFO	Der Agent auf Computer \${MachineName} hat eine Anhalte-Meldung gesendet

Horizon Administrator-Ereignisse

Horizon Administrator-Ereignisse zeichnen Informationen zu Aktionen auf, die Benutzer in Horizon Administrator initiieren.

Tabelle 2-6. Horizon Administrator-Ereignisse

Ereignistyp	Schweregrad	ModuleAndEventText
ADMIN_ADD_DESKTOP_ENTITLEMENT	AUDIT_SUCCESS	\${EntitlementDisplay} wurde von \${UserDisplayName} zum Zugriff auf Pool \${DesktopId} berechtigt
ADMIN_ADD_LICENSE	AUDIT_SUCCESS	\${UserDisplayName} hat eine Lizenz hinzugefügt
ADMIN_ADD_LICENSE_FAILED	AUDIT_FAIL	\${UserDisplayName} konnte keine Lizenz hinzufügen
ADMIN_ADD_PM	AUDIT_SUCCESS	\${UserDisplayName} hat den physischen Computer \${MachineName} zu Pool \${DesktopId} hinzugefügt
ADMIN_ADD_PM_FAILED	AUDIT_FAIL	\${UserDisplayName} konnte den physischen Computer \${MachineName} nicht zu Pool \${DesktopId} hinzufügen
ADMIN_ADD_THINAPP_ENTITLEMENT	AUDIT_SUCCESS	Die Anwendung \${ThinAppDisplayName} wurde durch \${UserDisplayName} dem Desktop \${MachineName} zugewiesen

Tabelle 2-6. Horizon Administrator-Ereignisse (Fortsetzung)

Ereignistyp	Schweregrad	ModuleAndEventText
ADMIN_ADD_THINAPP_ENTITLEMENT_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte die Anwendungsberechtigung nicht hinzufügen
ADMIN_ADD_THINAPP_POOL_ENTITLEMENT	AUDIT_SUCCESS	Die Anwendung \$(ThinAppDisplayName) wurde durch \$(UserDisplayName) dem Pool \${DesktopId} zugewiesen
ADMIN_ADMINISTRATOR_REMOVE_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte nicht alle Berechtigungen für Administrator \$ {AdminPermissionEntity} entfernen
ADMIN_ADMINISTRATOR_REMOVED	AUDIT_SUCCESS	\$(UserDisplayName) hat alle Berechtigungen für Administrator \$ {AdminPermissionEntity} entfernt
ADMIN_CONNECTION_BROKER_UPDATE_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte den Verbindungs-Broker \${BrokerId} nicht aktualisieren
ADMIN_CONNECTION_BROKER_UPDATED	AUDIT_SUCCESS	\$(UserDisplayName) hat den Verbindungs-Broker \${BrokerId} aktualisiert: (\${AttrChangeType}): \$ {AttrName} = \${AttrValue})
ADMIN_CONNECTION_SERVER_BACKUP_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte die Sicherung für den Verbindungs-Broker \$ {BrokerId} nicht initiieren
ADMIN_CONNECTION_SERVER_BACKUP_INITIATED	AUDIT_SUCCESS	\$(UserDisplayName) hat eine Sicherung für den Verbindungs-Broker \${BrokerId} initiiert
ADMIN_CONNECTION_SERVER_DISABLE_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte den Verbindungs-Broker \${BrokerId} nicht deaktivieren
ADMIN_CONNECTION_SERVER_DISABLED	AUDIT_SUCCESS	\$(UserDisplayName) deaktiviert den Verbindungs-Broker \${BrokerId}
ADMIN_CONNECTION_SERVER_ENABLE_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte den Verbindungs-Broker \${BrokerId} nicht aktivieren
ADMIN_CONNECTION_SERVER_ENABLED	AUDIT_SUCCESS	\$(UserDisplayName) aktiviert den Verbindungs-Broker \${BrokerId}
ADMIN_DATABASE_CONFIGURATION_ADD_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte die Datenbankkonfiguration nicht hinzufügen
ADMIN_DATABASE_CONFIGURATION_HINZUGEFGUT	AUDIT_SUCCESS	\$(UserDisplayName) hat die Datenbankkonfiguration hinzugefügt
ADMIN_DATABASE_CONFIGURATION_DELETE_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte die Datenbankkonfiguration nicht löschen
ADMIN_DATABASE_CONFIGURATION_DELETE_FAILED	AUDIT_SUCCESS	\$(UserDisplayName) hat die Datenbankkonfiguration gelöscht

Tabelle 2-6. Horizon Administrator-Ereignisse (Fortsetzung)

Ereignistyp	Schweregrad	ModuleAndEventText
ADMIN_DATABASE_CONFIGURATION_UPDATE_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte die Datenbankkonfiguration nicht aktualisieren
ADMIN_DATABASE_CONFIGURATION_UPDATED	AUDIT_SUCCESS	\$(UserDisplayName) hat die Datenbankkonfiguration aktualisiert
ADMIN_DEFAULT_DESKTOPPOOL_ASSIGN	AUDIT_SUCCESS	\$(UserDisplayName) hat den Pool \$ {DesktopId} für den Standard-Desktop \$ {UserName} zugewiesen
ADMIN_DEFAULT_DESKTOPPOOL_ASSIGN_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte den Pool \$ {DesktopId} für den Standard-Desktop nicht \$(UserName) zuweisen
ADMIN_DEFAULT_DESKTOPPOOL_UNASSIGN	AUDIT_SUCCESS	\$(UserDisplayName) hat die Pool-Zuweisung für den Standard-Desktop an \$ {UserName} entfernt
ADMIN_DEFAULT_DESKTOPPOOL_UNASSIGN_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte die Pool-Zuweisung für den Standard-Desktop an \$ {UserName} nicht entfernen
ADMIN_DESKTOP_ADDED	AUDIT_SUCCESS	\$(UserDisplayName) hat den Pool \$ {DesktopId} hinzugefügt
ADMIN_DESKTOP_ASSIGN	AUDIT_SUCCESS	\$(UserDisplayName) hat den Desktop \$ {MachineName} dem Benutzer \$ {UserName} zugewiesen
ADMIN_DESKTOP_ASSIGN_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte den Desktop \$ {MachineName} dem Benutzer \$ {UserName} nicht zuweisen
ADMIN_DESKTOP_EDITED	AUDIT_SUCCESS	\$(UserDisplayName) hat den Pool \$ {DesktopId} ((\$ {AttrChangeType})) bearbeitet: \$ {AttrName} = \$ {AttrValue})
ADMIN_DESKTOP_MAINTENANCE_MODE_UPDATE_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte den Desktop \$ {MachineName} nicht auf den Wartungsmodus \$ {MaintenanceMode} aktualisieren
ADMIN_DESKTOP_MAINTENANCE_MODE_UPDATED	AUDIT_SUCCESS	\$(UserDisplayName) hat den Desktop \$ {MachineName} auf den Wartungsmodus \$ {MaintenanceMode} aktualisiert
ADMIN_DESKTOP_UNASSIGN	AUDIT_SUCCESS	\$(UserDisplayName) hat die Zuweisung für Desktop \$ {MachineName} entfernt
ADMIN_DESKTOP_UNASSIGN_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte die Zuweisung für Desktop \$ {MachineName} nicht entfernen
ADMIN_ENABLE_DESKTOP_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte den Pool \$ {DesktopId} nicht auf \$ {EnableStatus} setzen

Tabelle 2-6. Horizon Administrator-Ereignisse (Fortsetzung)

Ereignistyp	Schweregrad	ModuleAndEventText
ADMIN_ENABLE_DESKTOP_SUCCEEDED	AUDIT_SUCCESS	\${UserDisplayName} hat den Pool \${DesktopId} auf \${EnableStatus} gesetzt
ADMIN_ENABLED_DESKTOP_PROVISION_FAILED	AUDIT_FAIL	\${UserDisplayName} konnte die Bereitstellung für Pool \${DesktopId} nicht auf \${EnableStatus} setzen
ADMIN_ENABLED_DESKTOP_PROVISION_SUCCEEDED	AUDIT_SUCCESS	\${UserDisplayName} hat die Bereitstellung für Pool \${DesktopId} auf \${EnableStatus} gesetzt
ADMIN_EVENT_CONFIGURATION_UPDATE_FAILED	AUDIT_FAIL	\${UserDisplayName} konnte die Ereigniskonfiguration nicht aktualisieren
ADMIN_EVENT_CONFIGURATION_UPDATED	AUDIT_SUCCESS	\${UserDisplayName} hat die globale Konfiguration aktualisiert
ADMIN_FOLDER_ADD_FAILED	AUDIT_FAIL	\${UserDisplayName} konnte den Ordner \${AdminFolderName} nicht hinzufügen
ADMIN_FOLDER_ADDED	AUDIT_SUCCESS	\${UserDisplayName} hat den Ordner \${AdminFolderName} hinzugefügt
ADMIN_FOLDER_CHANGE_FAILED	AUDIT_FAIL	\${UserDisplayName} konnte das Objekt \${ObjectID}(type=\${ObjectType}) nicht in den Ordner \${AdminFolderName} ändern
ADMIN_FOLDER_CHANGED	AUDIT_SUCCESS	\${UserDisplayName} hat das Objekt \${ObjectID}(type=\${ObjectType}) in den Ordner \${AdminFolderName} geändert
ADMIN_FOLDER_DELETE_FAILED	AUDIT_FAIL	\${UserDisplayName} konnte den Ordner \${AdminFolderName} nicht löschen
ADMIN_FOLDER_DELETED	AUDIT_SUCCESS	\${UserDisplayName} hat den Ordner \${AdminFolderName} gelöscht
ADMIN_GLOBAL_CONFIGURATION_UPDATE_FAILED	AUDIT_FAIL	\${UserDisplayName} konnte die globale Konfiguration nicht aktualisieren
ADMIN_GLOBAL_CONFIGURATION_UPDATED	AUDIT_SUCCESS	\${UserDisplayName} hat die globale Konfiguration (\${AttrChangeType}) aktualisiert: \${AttrName} = \${AttrValue})
ADMIN_GLOBAL_POLICY_UPDATE_FAILED	AUDIT_FAIL	\${UserDisplayName} konnte die globalen Richtlinien nicht aktualisieren
ADMIN_GLOBAL_POLICY_UPDATED	AUDIT_SUCCESS	\${UserDisplayName} hat die globale Richtlinie (\${AttrChangeType}) aktualisiert: \${AttrName} = \${AttrValue})
ADMIN_PERFMON_CONFIGURATION_UPDATE_FAILED	AUDIT_FAIL	\${UserDisplayName} konnte die Konfiguration der Leistungsüberwachung nicht aktualisieren
ADMIN_PERFMON_CONFIGURATION_UPDATED	AUDIT_SUCCESS	\${UserDisplayName} hat die Konfiguration der Leistungsüberwachung aktualisiert

Tabelle 2-6. Horizon Administrator-Ereignisse (Fortsetzung)

Ereignistyp	Schweregrad	ModuleAndEventText
ADMIN_PERMISSION_ADD_FAILED	AUDIT_FAIL	<p>{UserDisplayName} konnte die Berechtigung zu \$</p> <p>{AdminPermissionEntity} mit der Rolle \$</p> <p>{AdminRoleName} nicht in Ordner \$</p> <p>{AdminFolderName} hinzufügen</p>
ADMIN_PERMISSION_ADDED	AUDIT_SUCCESS	<p>{UserDisplayName} hat die Berechtigung zu \$</p> <p>{AdminPermissionEntity} mit der Rolle \$</p> <p>{AdminRoleName} in Ordner \$</p> <p>{AdminFolderName} hinzugefügt</p>
ADMIN_PERMISSION_REMOVE_FAILED	AUDIT_FAIL	<p>{UserDisplayName} konnte die Berechtigung zu \$</p> <p>{AdminPermissionEntity} mit der Rolle \$</p> <p>{AdminRoleName} nicht in Ordner \$</p> <p>{AdminFolderName} entfernen</p>
ADMIN_PERMISSION_REMOVED	AUDIT_SUCCESS	<p>{UserDisplayName} hat die Berechtigung zu \$</p> <p>{AdminPermissionEntity} mit der Rolle \$</p> <p>{AdminRoleName} in Ordner \$</p> <p>{AdminFolderName} entfernt</p>
ADMIN_POOL_POLICY_UPDATE_FAILED	AUDIT_FAIL	<p>{UserDisplayName} konnte die Richtlinien für Pool \$</p> <p>{DesktopId} nicht aktualisieren</p>
ADMIN_POOL_POLICY_UPDATED	AUDIT_SUCCESS	<p>{UserDisplayName} hat die Richtlinie (\$</p> <p>{AttrChangeType} für Pool \$</p> <p>{DesktopId} aktualisiert: \$</p> <p>{AttrName} = \$</p> <p>{AttrValue})</p>
ADMIN_REMOVE_DESKTOP_ENTITLEMENT	AUDIT_SUCCESS	<p>{EntitlementDisplay} wurde von \$</p> <p>{UserDisplayName} die Berechtigung zum Zugriff auf Pool \$</p> <p>{DesktopId} entzogen</p>
ADMIN_REMOVE_DESKTOP_FAILED	AUDIT_FAIL	<p>{UserDisplayName} konnte den Pool \$</p> <p>{DesktopId} nicht entfernen</p>
ADMIN_REMOVE_DESKTOP_SUCCEEDED	AUDIT_SUCCESS	<p>{UserDisplayName} hat den Pool \$</p> <p>{DesktopId} entfernt</p>
ADMIN_REMOVE_THINAPP_ENTITLEMENT	AUDIT_SUCCESS	<p>Die Zuweisung für die Anwendung \$</p> <p>{ThinAppDisplayName} zu Desktop \$</p> <p>{MachineName} wurde durch \$</p> <p>{UserDisplayName} aufgehoben</p>
ADMIN_REMOVE_THINAPP_ENTITLEMENT_FAILED	AUDIT_FAIL	<p>{UserDisplayName} konnte die Anwendungsberechtigung nicht entfernen</p>
ADMIN_REMOVE_THINAPP_POOL_ENTITLEMENT	AUDIT_SUCCESS	<p>Die Zuweisung für die Anwendung \$</p> <p>{ThinAppDisplayName} zu Pool \$</p> <p>{DesktopId} wurde durch \$</p> <p>{UserDisplayName} aufgehoben</p>
ADMIN_RESET_THINAPP_STATE	AUDIT_SUCCESS	<p>Der Status der Anwendung \$</p> <p>{ThinAppDisplayName} wird für Desktop \$</p> <p>{DesktopDisplayName} durch \$</p> <p>{UserDisplayName} zurückgesetzt</p>

Tabelle 2-6. Horizon Administrator-Ereignisse (Fortsetzung)

Ereignistyp	Schweregrad	ModuleAndEventText
ADMIN_RESET_THINAPP_STATE_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte den Anwendungsstatus für \$ {ThinAppDisplayName} nicht zurücksetzen
ADMIN_ROLE_ADD_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte die Rolle \$ {AdminRoleName} mit den Berechtigungen \$ {AdminPrivilegeName} nicht hinzufügen
ADMIN_ROLE_ADDED	AUDIT_SUCCESS	\$(UserDisplayName) hat die Rolle \$ {AdminRoleName} mit den Berechtigungen \$ {AdminPrivilegeName} hinzugefügt
ADMIN_ROLE_PRIV_UPDATE_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte die Rolle \$ {AdminRoleName} nicht auf die Berechtigungen \$ {AdminPrivilegeName} aktualisieren
ADMIN_ROLE_PRIV_UPDATED	AUDIT_SUCCESS	\$(UserDisplayName) hat die Rolle \$ {AdminRoleName} auf die Berechtigungen \$ {AdminPrivilegeName} aktualisiert
ADMIN_ROLE_REMOVE_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte die Rolle \$ {AdminRoleName} nicht entfernen
ADMIN_ROLE_REMOVED	AUDIT_SUCCESS	\$(UserDisplayName) hat Rolle \$ {AdminRoleName} entfernt
ADMIN_ROLE_RENAME_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte die Rolle \$ {AdminRoleName} nicht in \$ {AdminRoleNewName} umbenennen
ADMIN_ROLE_RENAMED	AUDIT_SUCCESS	\$(UserDisplayName) hat Rolle \$ {AdminRoleName} in \$ {AdminRoleNewName} umbenannt
ADMIN_SECURITY_SERVER_ADD_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte den Sicherheitsserver \$ {SecurityServerId} nicht hinzufügen
ADMIN_SECURITY_SERVER_ADDED	AUDIT_SUCCESS	\$(UserDisplayName) hat den Sicherheitsserver \$ {SecurityServerId} hinzugefügt
ADMIN_SECURITY_SERVER_EDIT_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte den Sicherheitsserver \$ {SecurityServerId} nicht bearbeiten
ADMIN_SECURITY_SERVER_EDITED	AUDIT_SUCCESS	\$(UserDisplayName) hat den Sicherheitsserver \$ {SecurityServerId} ((\$ {AttrChangeType})) bearbeitet: \$ {AttrName} = \$ {AttrValue}
ADMIN_SECURITY_SERVER_REMOVE_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte den Sicherheitsserver \$ {SecurityServerId} nicht entfernen

Tabelle 2-6. Horizon Administrator-Ereignisse (Fortsetzung)

Ereignistyp	Schweregrad	ModuleAndEventText
ADMIN_SECURITY_SERVER_REMOVED	AUDIT_SUCCESS	\$(UserDisplayName) hat den Sicherheitsserver \${SecurityServerId} entfernt
ADMIN_SESSION_SENDMSG	AUDIT_SUCCESS	\$(UserDisplayName) hat die Meldung (\$ {SessionMessage}) an die Sitzung (Benutzer \${UserName} und Desktop \$ {MachineName}) gesendet
ADMIN_SESSION_SENDMSG_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte die Meldung (\${SessionMessage}) nicht an die Sitzung \${ObjectId} senden
ADMIN_SVI_ADD_DEPLOYMENT_GROUP_FAILED	AUDIT_FAIL	Bereitstellungsgruppe für \${SVIParentVM} konnte nicht hinzugefügt werden: \$ {SVISnapshot}
ADMIN_SVI_ADD_DEPLOYMENT_GROUP_SUCCEEDED	AUDIT_SUCCESS	Bereitstellungsgruppe \$ {SVIDeploymentGroupID} für \$ {SVIParentVM} hinzugefügt : \$ {SVISnapshot}
ADMIN_SVI_ADD_UDD_FAILED	AUDIT_FAIL	Benutzerdaten-Festplatte \$ {UserDiskName} konnte nicht hinzugefügt werden
ADMIN_SVI_ADD_UDD_SUCCEEDED	AUDIT_SUCCESS	Benutzerdaten-Festplatte \$ {UserDiskName} hinzugefügt
ADMIN_SVI_ADMIN_ADDED	AUDIT_SUCCESS	\$(UserDisplayName) hat die SVI QuickPrep-Domäne \${SVIAdminFqdn}(\$ {SVIAdminName}) hinzugefügt
ADMIN_SVI_ADMIN_REMOVED	AUDIT_SUCCESS	\$(UserDisplayName) hat die SVI QuickPrep-Domäne (id=\${SVIAdminID}) entfernt
ADMIN_SVI_ADMIN_UPDATED	AUDIT_SUCCESS	\$(UserDisplayName) hat die SVI QuickPrep-Domäne \${SVIAdminFqdn}(\$ {SVIAdminName}) aktualisiert
ADMIN_SVI_ATTACH_UDD_FAILED	AUDIT_FAIL	Verknüpfen der Benutzerdaten-Festplatte \${UserDiskName} mit VM \${SVIVMID} konnte nicht angefordert werden
ADMIN_SVI_ATTACH_UDD_SUCCEEDED	AUDIT_SUCCESS	Verknüpfen der Benutzerdaten-Festplatte \${UserDiskName} mit VM \${SVIVMID} angefordert
ADMIN_SVI_DELETE_UDD_FAILED	AUDIT_FAIL	Benutzerdaten-Festplatte \$ {UserDiskName} konnte nicht gelöscht werden
ADMIN_SVI_DELETE_UDD_SUCCEEDED	AUDIT_SUCCESS	Benutzerdaten-Festplatte \$ {UserDiskName} gelöscht

Tabelle 2-6. Horizon Administrator-Ereignisse (Fortsetzung)

Ereignistyp	Schweregrad	ModuleAndEventText
ADMIN_SVI_DETACH_UDD_FAILED	AUDIT_FAIL	Trennen der Benutzerdaten-Festplatte \$ {UserDiskName} von VM \${SVIVMID} konnte nicht angefordert werden
ADMIN_SVI_DETACH_UDD_SUCCEEDED	AUDIT_SUCCESS	Trennen der Benutzerdaten-Festplatte \$ {UserDiskName} von VM \${SVIVMID} angefordert
ADMIN_SVI_REBALANCE_VM_FAILED	AUDIT_FAIL	VM \${SVIVMID} konnte nicht neu verteilt werden
ADMIN_SVI_REBALANCE_VM_SUCCEEDED	AUDIT_SUCCESS	VM \${SVIVMID} neu verteilt
ADMIN_SVI_REFRESH_VM_FAILED	AUDIT_FAIL	VM \${SVIVMID} konnte nicht aktualisiert werden
ADMIN_SVI_REFRESH_VM_SUCCEEDED	AUDIT_SUCCESS	VM \${SVIVMID} aktualisiert
ADMIN_SVI_RESYNC_VM_FAILED	AUDIT_FAIL	VM \${SVIVMID} konnte nicht mit Bereitstellungsgruppe \$ {SVIDeploymentGroupID} neu synchronisiert werden
ADMIN_SVI_RESYNC_VM_SUCCEEDED	AUDIT_SUCCESS	VM \${SVIVMID} wurde mit Bereitstellungsgruppe \$ {SVIDeploymentGroupID} neu synchronisiert
ADMIN_SVI_UPDATE_POOL_DEPLOYMENT_GROUP_FAILED	AUDIT_FAIL	Pool \${DesktopID} konnte für die Bereitstellungsgruppe \$ {SVIDeploymentGroupID} nicht aktualisiert werden
ADMIN_SVI_UPDATE_POOL_DEPLOYMENT_GROUP_SUCCEEDED	AUDIT_SUCCESS	Pool \${DesktopID} wurde für die Bereitstellungsgruppe \$ {SVIDeploymentGroupID} aktualisiert
ADMIN_SVI_UPDATE_UDD_FAILED	AUDIT_FAIL	Benutzerdaten-Festplatte \$ {UserDiskName} konnte nicht aktualisiert werden
ADMIN_SVI_UPDATE_UDD_SUCCEEDED	AUDIT_SUCCESS	Pool für Benutzerdaten-Festplatte \$ {UserDiskName} auf \${DesktopID} und Benutzer auf \${UserName} festgelegt
ADMIN_THINAPP_ADD_FAILED	AUDIT_FAIL	\${UserDisplayName} konnte die Anwendung \${ThinAppDisplayName} nicht hinzufügen
ADMIN_THINAPP_ADDED	AUDIT_SUCCESS	\${UserDisplayName} hat die Anwendung \${ThinAppDisplayName} hinzugefügt
ADMIN_THINAPP_DESKTOP_AVAILABLE	AUDIT_SUCCESS	Die Anwendung \${ThinAppDisplayName} ist jetzt auf Desktop \$ {DesktopDisplayName} verfügbar
ADMIN_THINAPP_DESKTOP_REMOVED	AUDIT_SUCCESS	Die Anwendung \${ThinAppDisplayName} wurde von Desktop \$ {DesktopDisplayName} entfernt

Tabelle 2-6. Horizon Administrator-Ereignisse (Fortsetzung)

Ereignistyp	Schweregrad	ModuleAndEventText
ADMIN_THINAPP_EDITED	AUDIT_SUCCESS	\${UserDisplayName} hat die Anwendung \${ThinAppDisplayName} bearbeitet
ADMIN_THINAPP_FAILED_DESKTOP_DELIVERY	AUDIT_FAIL	Die Anwendung \${ThinAppDisplayName} konnte nicht an den Desktop \$ {DesktopDisplayName} übermittelt werden
ADMIN_THINAPP_FAILED_DESKTOP_REMOVAL	AUDIT_FAIL	Anwendung \${ThinAppDisplayName} konnte nicht vom Desktop \$ {DesktopDisplayName} entfernt werden
ADMIN_THINAPP_GROUP_ADD_FAILED	AUDIT_FAIL	\${UserDisplayName} konnte die Anwendungsvorlage \$ {ThinAppGroupName} nicht hinzufügen
ADMIN_THINAPP_GROUP_ADDED	AUDIT_SUCCESS	\${UserDisplayName} hat die Anwendungsvorlage \$ {ThinAppGroupName} mit den Anwendungen \$ {ThinAppGroupApplications} hinzugefügt
ADMIN_THINAPP_GROUP_EDIT_FAILED	AUDIT_FAIL	\${UserDisplayName} konnte die Anwendungsvorlage \$ {ThinAppGroupName} nicht bearbeiten
ADMIN_THINAPP_GROUP_EDITED	AUDIT_SUCCESS	\${UserDisplayName} hat die Anwendungsvorlage \$ {ThinAppGroupName} mit den Anwendungen \$ {ThinAppGroupApplications} bearbeitet
ADMIN_THINAPP_GROUP_REMOVE_FAILED	AUDIT_FAIL	\${UserDisplayName} konnte die Anwendungsvorlage \$ {ThinAppGroupName} nicht entfernen
ADMIN_THINAPP_GROUP_REMOVED	AUDIT_SUCCESS	\${UserDisplayName} hat die Anwendungsvorlage \$ {ThinAppGroupName} entfernt
ADMIN_THINAPP_REMOVE_FAILED	AUDIT_FAIL	\${UserDisplayName} konnte die Anwendung \${ThinAppDisplayName} nicht entfernen
ADMIN_THINAPP_REMOVED	AUDIT_SUCCESS	\${UserDisplayName} hat die Anwendung \${ThinAppDisplayName} entfernt
ADMIN_THINAPP_REPO_ADD_FAILED	AUDIT_FAIL	\${UserDisplayName} konnte das Repository \${ThinAppRepositoryName}, Pfad \${ThinAppRepositoryPath} nicht hinzufügen
ADMIN_THINAPP_REPO_ADDED	AUDIT_SUCCESS	\${UserDisplayName} hat Repository \$ {ThinAppRepositoryName}, Pfad \$ {ThinAppRepositoryPath} hinzugefügt

Tabelle 2-6. Horizon Administrator-Ereignisse (Fortsetzung)

Ereignistyp	Schweregrad	ModuleAndEventText
ADMIN_THINAPP_REPO_EDIT_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte das Repository \${ThinAppRepositoryName}, Pfad \${ThinAppRepositoryPath} nicht bearbeiten
ADMIN_THINAPP_REPO_EDITED	AUDIT_SUCCESS	\$(UserDisplayName) hat Repository \${ThinAppRepositoryName}, Pfad \${ThinAppRepositoryPath} bearbeitet
ADMIN_THINAPP_REPO_REMOVED	AUDIT_SUCCESS	\$(UserDisplayName) hat Repository \${ThinAppRepositoryName} entfernt
ADMIN_UNREGISTER_PM	AUDIT_SUCCESS	\$(UserDisplayName) hat den physischen Computer \${MachineName} aus der Registrierung entfernt
ADMIN_UNREGISTER_PM_FAILED	AUDIT_FAIL	\$(UserDisplayName) kann den physischen Computer \${MachineName} nicht aus der Registrierung entfernen
ADMIN_USER_INFO_UPDATE_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte die Benutzerinformationen für \${UserName} nicht mit AD Server aktualisieren
ADMIN_USER_INFO_UPDATED	AUDIT_SUCCESS	\$(UserDisplayName) hat die Benutzerinformationen für \${UserName} mit AD Server aktualisiert
ADMIN_USER_POLICY_DELETE_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte die Außerkraftsetzungsrichtlinien für Pool \${DesktopId} für Benutzer \${UserName} nicht löschen
ADMIN_USER_POLICY_DELETED	AUDIT_SUCCESS	\$(UserDisplayName) hat die Außerkraftsetzungsrichtlinie für Pool \${DesktopId} für Benutzer \${UserName} (\${AttrChangeType}) gelöscht: \${AttrName} = \${AttrValue}
ADMIN_USER_POLICY_UPDATE_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte die Richtlinien für Pool \${DesktopId} für Benutzer \${UserName} nicht aktualisieren
ADMIN_USER_POLICY_UPDATED	AUDIT_SUCCESS	\$(UserDisplayName) hat die Richtlinie für Pool \${DesktopId} für Benutzer \${UserName} (\${AttrChangeType}) aktualisiert: \${AttrName} = \${AttrValue}
ADMIN_USERLOGGEDIN	AUDIT_SUCCESS	Benutzer \${UserDisplayName} hat sich bei View Administrator angemeldet
ADMIN_USERLOGGEDOUT	AUDIT_SUCCESS	Benutzer \${UserDisplayName} hat sich von View Administrator abgemeldet
ADMIN_VC_ADD_FAILED	AUDIT_FAIL	\$(UserDisplayName) konnte die VC Server-Instanz \${VCAddress} nicht hinzufügen

Tabelle 2-6. Horizon Administrator-Ereignisse (Fortsetzung)

Ereignistyp	Schweregrad	ModuleAndEventText
ADMIN_VC_ADDED	AUDIT_SUCCESS	\${UserDisplayName} hat die VC Server-Instanz \${VCAddress} hinzugefügt
ADMIN_VC_EDITED	AUDIT_SUCCESS	\${UserDisplayName} hat die VC Server-Instanz \${VCAddress} ((\$ {AttrChangeType})) bearbeitet: \$ {AttrName} = \$ {AttrValue})
ADMIN_VC_LICINV_ALARM_DISABLED	AUDIT_SUCCESS	Der Alarm auf VC Server \${VCAddress} für die Überwachung der Lizenz-Bestandsliste wurde deaktiviert, da alle Hosts über Desktop-Lizenzen verfügen
ADMIN_VC_REMOVE_FAILED	AUDIT_FAIL	\${UserDisplayName} konnte die VC Server-Instanz \${VCAddress} nicht entfernen
ADMIN_VC_REMOVED	AUDIT_SUCCESS	\${UserDisplayName} hat die VC Server-Instanz \${VCAddress} entfernt

Ereignismeldungsattribute

ModuleAndEventText-Meldungen verwenden bestimmte Attribute. Um den Datentyp für ein Attribut zu bestimmen, ermitteln Sie dessen Wert in der Spalte „Type“ (Typ) der event_data- oder event_data_historical-Tabelle.

Tabelle 2-7. Von ModuleAndEventText-Meldungen verwendete Attribute

Attributname	Beschreibung
AdminFolderName	Name eines Ordners, der einen privilegierten Zugriff erfordert.
AdminPermissionEntity	Name eines Objekts, das einen privilegierten Zugriff erfordert.
AdminPrivilegeName	Name einer administrativen Berechtigung.
AdminRoleName	Name einer Administratorrolle.
AdminRoleNewName	Neuer Name einer Administratorrolle.
AttrChangeType	Typ der Änderung für ein generisches Attribut.
AttrName	Name eines generischen Attributs.
AttrValue	Wert eines generischen Attributs.
BrokerId	Bezeichner einer Verbindungsserver-Instanz.
BrokerName	Name einer Verbindungsserver-Instanz.
DesktopDisplayName	Anzeigenname eines Desktop-Pools.
DesktopId	Bezeichner eines Desktop-Pools.
EntitlementDisplay	Anzeigenname einer Desktop-Berechtigung.
MachineId	Bezeichner eines physischen Computers oder einer virtuellen Maschine.
MachineName	Bezeichner eines physischen Computers oder einer virtuellen Maschine.

Tabelle 2-7. Von ModuleAndEventText-Meldungen verwendete Attribute (Fortsetzung)

Attributname	Beschreibung
MaintenanceMode	Status des Wartungsmodus.
ObjectID	Bezeichner eines Bestandsobjekts.
Objekttyp	Typ eines Bestandsobjekts.
PolicyDisplayName	Anzeigenname einer Richtlinie.
PolicyObject	Bezeichner eines Richtlinienobjekts.
PolicyValue	Wert eines Richtlinienobjekts.
ProtocolId	Bezeichner eines Anzeigeprotokolls.
SecurityServerId	Bezeichner eines Sicherheitsservers.
SVIAdminFqdn	FQDN einer QuickPrep-Domäne.
SVIAdminID	Bezeichner einer QuickPrep-Domäne.
SVIAdminName	Name einer QuickPrep-Domäne.
SVIDeploymentGroupID	Bezeichner einer View Composer-Bereitstellungsgruppe.
SVIOperation	Name eines View Composer-Vorgangs.
SVIParentVM	Übergeordnete virtuelle Maschine in View Composer.
SVIPath	Pfad eines Objekts in View Composer.
SVISnapshot	Snapshot in View Composer.
SVIVMID	Bezeichner einer virtuellen Maschine in View Composer.
ThinAppDisplayName	Anzeigenname eines ThinApp-Objekts.
ThinAppId	Bezeichner eines ThinApp-Objekts.
ThinAppRepositoryName	Name eines ThinApp-Repository.
ThinAppRepositoryPath	Pfad eines ThinApp-Repository.
Uhrzeit	Datums-/Uhrzeitwert.
UserCount	Maximale Anzahl von Desktop-Benutzern in einem 24-Stunden-Zeitraum.
UserDiskName	Name einer Benutzerdatenfestplatte.
UserDisplayName	Benutzername im Format DOMÄNE\Benutzername.
UserName	Name eines Benutzers in Active Directory.
VCAddress	URL des vCenter Server.

Beispiele für Datenbankabfragen und -ansichten

Sie können die event_historical-Datenbank für die Anzeige von Fehlerereignissen, Warnmeldungen und bestimmten aktuellen Ereignissen abfragen.

Hinweis Ersetzen Sie in den folgenden Beispielen das Präfix dbo.VE_ durch das entsprechende Präfix Ihrer Ereignisdatenbank.

Auflisten von Fehlerereignissen

Die folgende Abfrage ermittelt alle Fehlerereignisse aus der event_historical-Tabelle.

```
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'
);
```

Auflisten von Warnereignissen

Die folgende Abfrage ermittelt alle Warnereignisse aus der event_historical-Tabelle.

```
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'
);
```

Auflisten aktueller Ereignisse

Die folgende Abfrage ermittelt alle aktuellen Ereignisse, die mit dem Benutzer „Fred“ in der Domäne MYDOM verknüpft sind.

```
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'
);
```

Die folgende Abfrage ermittelt alle aktuellen Ereignisse, bei denen der Agent auf einem Computer heruntergefahren wurde.

```
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'
);
```

Die folgende Abfrage ermittelt alle aktuellen Ereignisse, bei denen ein Desktop nicht gestartet werden konnte, da der Desktop-Pool leer war.

```
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'
);
```

Die folgende Abfrage ermittelt alle aktuellen Ereignisse, bei denen ein Administrator einen Desktop-Pool entfernt hat.

```
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'
);
```

Die folgende Abfrage ermittelt alle aktuellen Ereignisse, bei denen ein Administrator ein ThinApp-Repository hinzugefügt hat.

```
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'
);
```

Aktivieren von Horizon 7 für cloudgehostete Abonnements und Dienste

3

Sie können Ihre Horizon 7-Bereitstellung für die Verwendung eines cloudgehosteten Abonnements aktivieren, das die Nutzung von cloudgehosteten Diensten für die Verwendung mit cloudverbundenen Horizon 7-Pods beinhaltet. Sie müssen die virtuelle Horizon 7 Cloud Connector-Appliance verwenden, um Ihre Horizon 7-Bereitstellung mit der von VMware Horizon Cloud Service bereitgestellten cloudbasierten Verwaltungsebene zu verbinden.

Abonnementlizenzen für Horizon 7

Horizon 7-Abonnementlizenzen sind mit dem eigenständigen Horizon 7-Paket und als Teil des Workspace ONE-Enterprise-Pakets verfügbar.

Die Horizon 7-Abonnementlizenz bietet die gleichen Horizon 7-Produktkomponenten mit flexibleren Einsatzoptionen. Horizon 7-Abonnementlizenzen ermöglichen die Horizon 7-Bereitstellung im Datencenter der Kunden, in der Private Cloud und auf VMware Cloud on AWS. Nachdem Sie die virtuelle Horizon 7 Cloud Connector-Appliance so konfiguriert haben, dass Ihr Pod mit Horizon Cloud verbunden wird, können Sie die Abonnementlizenz-Laufzeit in Horizon Console anzeigen.

Hinweis Die Abonnementlizenz für Horizon 7 wird von VMware erst nach der Bereitstellung der virtuellen Horizon 7 Cloud Connector-Appliance verwaltet. Sie erhalten den Lizenzschlüssel für VMware Horizon 7 nicht mit dieser Abonnementlizenz. Sie erhalten mit dieser Abonnementlizenz jedoch Lizenzschlüssel für vSphere, vCenter Server, vSAN, App Volumes und Dynamic Environment Manager. Sie erhalten diese Schlüssel in einer E-Mail mit folgendem Betreff: Willkommen beim lokalen VMware Horizon-Abonnement.

Cloudgehostete Dienste für Horizon 7-Pods

Nachdem Sie die virtuelle Horizon 7 Cloud Connector-Appliance für die Verbindung Ihres Pods mit VMware Horizon Cloud Service konfiguriert haben, können Sie auch cloudgehostete Verwaltung, Funktionen und Workflows nutzen, die von Horizon Cloud bereitgestellt werden und Ihnen gemäß dieser Abonnementlizenz zur Verfügung stehen. Informationen zu diesen cloudgehosteten Diensten finden Sie unter [Einführung in Horizon Cloud](#) in der VMware Horizon Cloud Service-Dokumentation.

Horizon 7 Cloud Connector

Bei Horizon 7 Cloud Connector handelt es sich um eine virtuelle Appliance, die neben dem Horizon 7-Pod bereitgestellt wird und den Horizon 7-Pod mit VMware Horizon Cloud Service verbindet. Horizon 7 Cloud Connector ist eine erforderliche Komponente, die Ihre Horizon 7-Pods mit VMware Horizon Cloud Service verbindet. Horizon 7 Cloud Connector ist für cloudgehostete Dienste erforderlich, einschließlich Horizon 7-Abonnementlizenzen, des Systemzustands-Dashboards, Horizon Help Desk Tool und anderer cloudgehosteter Verwaltungsfunktionen und -Workflows in Horizon Cloud.

Sie benötigen ein aktives My VMware-Konto zum Kauf einer Horizon 7-Lizenz von <https://my.vmware.com>. Anschließend erhalten Sie eine E-Mail mit dem Link zum Herunterladen von Horizon 7 Cloud Connector als OVA-Datei.

Wenn Sie die virtuelle Horizon 7 Cloud Connector-Appliance von vSphere Web Client bereitstellen, koppeln Sie den Cloud Connector mit dem Verbindungsserver-Pod, den Sie mit dem Horizon Cloud Service verbinden möchten. Im Rahmen des Kopplungsvorgangs stellt die virtuelle Horizon 7 Cloud Connector-Appliance eine Verbindung zwischen dem Verbindungsserver und Horizon Cloud Service her, um die Horizon 7-Abonnementlizenz und andere cloudgehostete Verwaltungsdienste zu verwalten. Mit einer Horizon 7-Abonnementlizenz müssen Sie keinen Horizon 7-Lizenzschlüssel für die Produktaktivierung von VMware Horizon 7 manuell eingeben. Allerdings müssen Sie die Lizenzschlüssel verwenden, um unterstützende Komponenten wie vSphere, vCenter Server, App Volumes usw. zu aktivieren.

Hinweis Die virtuelle Horizon 7 Cloud Connector-Appliance unterstützt keine IPv6-Umgebung.

Weitere Informationen zum Bereitstellen der virtuellen Horizon 7 Cloud Connector-Appliance und zum Herstellen dieser Verbindung zwischen einem Horizon 7-Pod und VMware Horizon Cloud Service finden Sie in den folgenden Themen in der Horizon Cloud Service-Dokumentation:

- [End-to-End-Workflow, wenn Ihr allererster cloudverbundener Pod durch die Verbindung von Horizon Cloud mit einem vorhandenen, manuell bereitgestellten Horizon 7-Pod entstanden ist](#)
- [Horizon Cloud mit einem vorhandenen manuell bereitgestellten Horizon 7-Pod verbinden.](#)

Bereitstellen von Horizon 7 in VMware Cloud on AWS

4

VMware Cloud on AWS ist ein Clouddienst, über den Sie Horizon 7-Desktops und -Anwendungen bereitstellen können.

Weitere Informationen zur Bereitstellung von Horizon 7 auf VMware Cloud on AWS finden Sie im „Bereitstellungshandbuch für Horizon 7 auf VMware Cloud in AWS“ unter <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vmw-deploy-horizon-seven-on-vmware-cloud-on-aws.pdf>.

Eine Liste der Horizon 7-Funktionen, die auf VMware Cloud on AWS unterstützt werden, finden Sie im VMware Knowledgebase-Artikel <https://kb.vmware.com/s/article/58539>.

Weitere Informationen zu VMware Cloud on AWS finden Sie in der Dokumentation zu VMware Cloud on AWS unter <https://docs.vmware.com/de/VMware-Cloud-on-AWS/index.html>.

Weitere Informationen zu den Auswirkungen des SDDC-Upgrades auf eine Horizon 7-Bereitstellung auf VMware Cloud on AWS finden Sie im VMware-Knowledgebase-Artikel <https://kb.vmware.com/s/article/74599>.

Weitere Informationen zum Aktualisieren der FTT-Ebene der vSAN-Speicherrichtlinie für eine Horizon 7-Bereitstellung auf VMware Cloud on AWS finden Sie im VMware-Knowledgebase-Artikel <https://kb.vmware.com/s/article/76366>.

Anpassen der LDAP-Daten

5

Sie können mit den VMware- und Microsoft-Befehlszeilenprogrammen LDAP-Konfigurationsdaten in und aus Horizon 7 importieren oder exportieren. Diese Befehlszeilenprogramme importieren und exportieren LDAP-Konfigurationsdaten in Konfigurationsdateien mit dem LDAP-Datenaustauschformat (LDAP Data Interchange Format, LDIF).

Diese Funktion ist für die Verwendung von erfahrenen Administratoren vorgesehen, die automatische Massenkonfigurationsvorgänge durchführen möchten. Zum Erstellen von Skripts für die Aktualisierung der Horizon 7-Konfiguration verwenden Sie Horizon 7 PowerCLI.

Dieses Kapitel enthält die folgenden Themen:

- [Einführung in die LDAP-Konfigurationsdaten](#)
- [Ändern von LDAP-Konfigurationsdaten](#)

Einführung in die LDAP-Konfigurationsdaten

Alle Horizon 7-Konfigurationsdaten wird in einem LDAP-Verzeichnis gespeichert. Jede Standard- oder Replikatinstanz des Horizon Connection Server enthält ein lokales LDAP-Konfigurations-Repository und eine Replikationsvereinbarung zwischen den einzelnen Verbindungsserver-Instanzen. Dadurch wird sichergestellt, dass Änderungen an einem Repository automatisch auf alle anderen Repositories repliziert werden.

Wenn Sie Horizon Administrator für die Änderung der Horizon 7-Konfiguration verwenden, werden die entsprechenden LDAP-Daten im Repository aktualisiert. Wenn Sie beispielsweise einen Desktop-Pool hinzufügen, speichert Horizon 7 Informationen über Benutzer, Benutzergruppen und Berechtigungen in LDAP. Verbindungsserver-Instanzen verwalten andere LDAP-Konfigurationsdaten automatisch und verwenden die Informationen im Repository zur Steuerung von Horizon 7-Vorgängen.

Mit LDIF-Konfigurationsdateien können Sie eine Reihe von Aufgaben wie das Übertragen von Konfigurationsdaten zwischen Verbindungsserver-Instanzen und das Sichern Ihrer Horizon 7-Konfiguration durchführen, um den Zustand einer Verbindungsserver-Instanz wiederherstellen zu können.

Sie können mithilfe von LDIF-Konfigurationsdateien auch eine große Anzahl an Horizon 7-Objekten wie z. B. Desktop-Pools definieren und diese Objekte zu Ihren Verbindungsserver-Instanzen hinzufügen, ohne dies manuell mit Horizon Administrator durchführen zu müssen.

Horizon 7 führt regelmäßige Sicherungen des LDAP-Repository durch.

LDAP-Konfigurationsdaten werden als reiner ASCII-Text übertragen und entsprechen dem IETF-Standard (Internet Engineering Task Force) RFC 2849.

Ändern von LDAP-Konfigurationsdaten

Sie können LDAP-Konfigurationsdaten auf einer Horizon Connection Server-Instanz in eine LDIF-Konfigurationsdatei exportieren, die LDIF-Konfigurationsdatei ändern und die geänderte LDIF-Konfigurationsdatei zur Durchführung von automatischen Massenkonfigurationsvorgängen in andere Verbindungsserver-Instanzen importieren.

Beispiele für die LDIF-Syntax finden Sie für jedes Element der Horizon-LDAP-Konfigurationsdaten in einer exportierten LDIF-Konfigurationsdatei. Sie können daraus z. B. die Daten für einen Desktop-Pool extrahieren und mit diesen Daten als Vorlage eine große Anzahl von Desktop-Pools erstellen.

Exportieren von LDAP-Konfigurationsdaten

Mit dem Befehlszeilendienstprogramm `vdmexport` können Sie die Konfigurationsdaten aus einer Standard- oder Replikatinstanz des Verbindungsservers in eine LDIF-Konfigurationsdatei exportieren.

Verfahren

- 1 Melden Sie sich als Benutzer mit der Rolle „Administratoren“ oder „Administratoren (Nur Lesezugriff)“ bei einer Standard- oder Replikat-Verbindungsserver-Instanz an.

Um Konfigurationsdaten aus dem Repository der Horizon-Konfiguration exportieren zu können, müssen Sie als Benutzer mit der Rolle „Administratoren“ oder „Administratoren (Nur Lesezugriff)“ angemeldet sein.

- 2 Geben Sie an der Eingabeaufforderung den Befehl `vdmexport` ein.

Standardmäßig wird das Befehlszeilendienstprogramm `vdmexport` im Verzeichnis `C:\Program Files\VMware\VMware View\Server\tools\bin` installiert.

Der Befehl `vdmexport` bietet die folgenden Optionen.

Option	Bezeichnung
<code>-f</code>	Name der Ausgabedatei für das lokale LDAP-Backup.
<code>-v</code>	Die Ausgabedatei ist wortgetreu (nicht verschlüsselt).
<code>-c</code>	Ähnlich wie die Option <code>-v</code> , aber sensible Attributwerte sind nicht in der Ausgabedatei enthalten.
<code>-k</code>	Gibt nur Kiosk-Clienteeinträge und zugehörige FSPs aus.
<code>-g</code>	Name der Ausgabedatei für globales Cloud-Pod-Architektur-LDAP-Backup.

Der folgende Befehl exportiert beispielsweise eine lokale LDIF-Konfigurationsdatei.

```
vdmexport -f mylocalexport.LDF
```

Mit dem folgenden Befehl wird eine globale Cloud-Pod-Architektur-LDIF-Konfigurationsdatei exportiert.

```
vdmexport -g myglobalexport.LDF
```

Der Befehl `vdmexport` schreibt die Konfiguration Ihrer Verbindungsserver-Instanz in die angegebene Datei. Der Befehl zeigt Fehler an, wenn Ihre Rolle nicht über ausreichende Berechtigungen zur Anzeige der Daten im Konfigurations-Repository verfügt.

Definieren eines Desktop-Pools in einer LDIF-Konfigurationsdatei

Sie können einen Desktop-Pool in einer LDIF-Konfigurationsdatei definieren und die angepasste LDIF-Konfigurationsdatei importieren, um eine große Anzahl von Desktop-Pools zu erstellen.

Hinweis Sie können auch benutzerdefinierte LDIF-Konfigurationsdateien für andere Objekte erstellen, die im LDAP-Repository definiert werden, einschließlich globaler Konfigurationseinstellungen, Konfigurationseinstellungen für eine bestimmte Horizon Connection Server-Instanz oder für einen Sicherheitsserver sowie die Konfigurationseinstellungen für einen bestimmten Benutzer.

Um einen Desktop-Pool in einer LDIF-Konfigurationsdatei zu definieren, müssen Sie die im Folgenden aufgeführten Einträge der Datei hinzufügen.

- Einen virtuellen Desktop-VM-Eintrag für jeden virtuellen Desktop im Desktop-Pool
- Einen VM-Pool-Eintrag für jeden Desktop-Pool
- Einen Eintrag für die Desktop-Anwendung, der die Berechtigung des Desktop-Pools definiert

Ordnen Sie jedem VM-Pool-Eintrag einen Desktop-Anwendungseintrag in einer Eins-zu-Eins-Beziehung zu. Ein Eintrag für die Desktop-Anwendung kann nicht zwischen VM-Pool-Einträgen freigegeben werden, und ein VM-Pool-Eintrag kann nur einem Desktop-Anwendungseintrag zugeordnet sein.

Die folgende Tabelle beschreibt die Attribute, die Sie angeben müssen, wenn Sie eine Desktop-Pooldefinition in einer LDIF-Konfigurationsdatei ändern.

Tabelle 5-1. Wichtige Attribute für die Definition eines Desktop-Pools

Eintrag	Attribut	Beschreibung
Virtuelle Desktop-VM VM-Pool Desktop-Anwendung	cn	Allgemeiner Eintragsname. Wenn Namen automatisch generiert werden sollen, legen Sie GUID-Zeichenfolgen (Global Unique Identifiers) fest. Sie können jeden zuverlässigen GUID-Generator wie den Mechanismus von .NET verwenden (z. B. durch Aufruf von System.Guid.NewGuid().ToString() in Visual Basic).
Desktop-Anwendung	Mitglied	<p>Eine Liste der Active Directory-Benutzer und -Gruppen, die dazu berechtigt sind, auf den Desktop-Pool zuzugreifen. Das Attribut wird in der Form einer Windows-Sicherheits-ID (SID)-Referenz angegeben. Ein Mitgliedswert von <SID=S-1-2-3-4> steht für einen Active Directory-Benutzer oder eine Active Directory-Gruppe mit dem SID-Wert S-1-2-3-4.</p> <p>Im LDIF-Format ist das „Kleiner-als“-Zeichen (<) reserviert. Deshalb müssen Sie nach dem Attributnamen zwei Doppelpunkte (:) einfügen und den SID-Wert im Basis-64-Format eingeben (z. B. PFNJRD1TLTEtMi0zLTQ+IA==).</p> <p>Da dieses Attribut mehrwertig ist, können Sie es für mehrere Zeilen verwenden, sodass jeder Eintrag in einer Liste von SIDs repräsentiert ist.</p>

Beispiel für Desktop-Pooleinträge einer LDIF-Konfigurationsdatei

Beim folgenden Beispiel handelt es sich um einen Auszug aus einer LDIF-Konfigurationsdatei. Es zeigt Beispieleinträge für einen Desktop-Pool mit dem Namen „Pool1“, der zwei virtuelle Desktops namens „VM1“ und „VM2“ enthält. Der Desktop-Pooleintrag ist mit dem Desktop-Anwendungseintrag gekoppelt, der ebenfalls den Namen „Pool1“ hat.

```
#
# 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:: PFNJRDI1LTETMi0zLTQ+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

```

Importieren von LDAP-Konfigurationsdaten

Sie können mit dem Befehl `vdmimport` Konfigurationsdaten aus einer LDIF-Konfigurationsdatei in eine Standard- oder Replikatinstanz des Verbindungsservers importieren.

Voraussetzungen

- Exportieren Sie LDAP-Konfigurationsdaten in eine LDIF-Konfigurationsdatei. Weitere Informationen hierzu finden Sie unter [Exportieren von LDAP-Konfigurationsdaten](#).
- Wenn Sie eine globale LDIF-Konfigurationsdatei von Cloud-Pod-Architektur importieren, stellen Sie sicher, dass die Cloud-Pod-Architektur-Funktion auf der Verbindungsserver-Instanz initialisiert ist.

Verfahren

- 1 Melden Sie sich bei einer Verbindungsserver-Instanz als Benutzer mit der Rolle „Administratoren“ an.
Sie müssen als Benutzer mit der Rolle „Administratoren“ angemeldet sein, um Konfigurationsdaten in das Repository der Horizon-Konfiguration importieren zu können.

2 Geben Sie an der Eingabeaufforderung den Befehl `vdmimport` ein.

Standardmäßig wird das Befehlszeilendienstprogramm `vdmimport` im Verzeichnis `C:\Program Files\VMware\VMware View\Server\tools\bin` installiert.

Der Befehl `vdmimport` bietet die folgenden Optionen.

Option	Bezeichnung
-f	Name der Eingabedatei.
-i	Zeigt Dateiinformationen über die angegebene LDIF-Konfigurationsdatei an.
-d	Entschlüsselt die angegebene LDIF-Konfigurationsdatei.
-p	Gibt das Wiederherstellungskennwort für die Entschlüsselung einer verschlüsselten LDIF-Konfigurationsdatei an. Geben Sie "" ein, um das Kennwort im Rahmen der Eingabeaufforderung einzugeben.
-g	Gibt an, dass die Wiederherstellung für eine Cloud-Pod-Architektur-Umgebung erfolgt.

Mit den folgenden Befehlen lässt sich beispielsweise eine lokale LDIF-Konfigurationsdatei entschlüsseln und importieren.

```
vdmimport -d -p mypassword -f MyEncryptedxport.LDF > MyDecryptedexport.LDF
```

```
vdmimport -f MyDecryptedexport.LDF
```

Mit den folgenden Befehlen lässt sich eine globale Cloud-Pod-Architektur-LDIF_Konfigurationsdatei entschlüsseln und importieren.

```
vdmimport -d -p mypassword -f MyEncryptedCPAexport.LDF > MyDecryptedCPAexport.LDF
```

```
vdmimport -g -f MyDecryptedCPAexport.LDF
```

Nach der Ausführung des Befehls `vdmimport` wird die Konfiguration Ihrer Verbindungsserver-Instanz mit den Daten aus der Datei aktualisiert, und die Anzahl der Einträge, die erfolgreich aktualisiert wurden, wird angezeigt. Es werden Fehlermeldungen angezeigt, wenn Datensätze nicht aktualisiert werden konnten, weil Ihre Rolle nicht über die dafür notwendigen Berechtigungen verfügt.

Untersuchen von PColP-Sitzungsstatistiken mit WMI

6

Mit der Windows-Verwaltungsinstrumentation (Windows Management Instrumentation, WMI) können Sie die Leistungsstatistiken für eine PColP-Sitzung unter Verwendung einer unterstützten Programmierungsschnittstelle, einschließlich C#, C++, PowerShell, VBScript, VB .NET und Windows WMI-Befehlszeile (WMIC), untersuchen.

Sie können auch mit dem Microsoft WMI Code Creator VBScript-, C#- und VB .NET-Code generieren, der auf die PColP-Leistungsindikatoren zugreift. Weitere Informationen zu WMI, WMIC und dem WMI Code Creator-Tool finden Sie unter <http://technet.microsoft.com/de-de/library/bb742610.aspx>.

Dieses Kapitel enthält die folgenden Themen:

- [Verwenden von PColP-Sitzungsstatistiken](#)
- [Allgemeine PColP-Sitzungsstatistiken](#)
- [PCoIP-Audiostatistiken](#)
- [PCoIP-Bildverarbeitungsstatistiken](#)
- [PCoIP-Netzwerkstatistiken](#)
- [PCoIP-USB-Statistiken](#)
- [Beispiele für die Verwendung von PowerShell-Cmdlets für die Untersuchung von PColP-Statistiken](#)

Verwenden von PColP-Sitzungsstatistiken

Der WMI-Namespace für die PColP-Sitzungsstatistiken lautet root\CIMV2. Die Namen der Statistiken enthalten als Suffix (Server) oder (Client), je nachdem, ob die Statistiken auf dem PColP Server oder auf dem PColP Client aufgezeichnet wurden.

Sie können mit dem Windows-Systemmonitor und mit den Leistungsindikatoren die durchschnittlichen Werte für einen angegebenen Abfragezeitraum berechnen. Für einen Remotezugriff auf die Leistungsindikatoren benötigen Sie Administratorrechte.

Alle Statistiken werden auf 0 zurückgesetzt, wenn eine PCoIP-Sitzung geschlossen wird. Wenn die WMI-Eigenschaft `SessionDurationSeconds` konstant über einen Wert ungleich null verfügt, wurde der PCoIP-Server zwangsweise beendet, oder er ist abgestürzt ist. Wenn sich die Eigenschaft `SessionDurationSeconds` von einem Wert ungleich null auf 0 ändert, wird die PCoIP-Sitzung geschlossen.

Um einen Fehler durch eine Division durch null zu vermeiden, müssen Sie überprüfen, ob der Nenner in den Ausdrücken zum Berechnen der Bandbreite oder des prozentualen Paketverlustes null ergibt.

USB-Statistiken werden für Zero Clients, aber nicht für Thin Clients und Softwareclients aufgezeichnet.

Allgemeine PCoIP-Sitzungsstatistiken

Der Name der WMI-Klasse für allgemeine PCoIP-Sitzungsstatistiken lautet `Win32_PerfRawData_TeradiciPerf_PCoIPSessionGeneralStatistics`.

Tabelle 6-1. Allgemeine Sitzungsstatistiken

Name der WMI-Eigenschaft	Beschreibung
<code>BytesReceived</code>	Gesamte Byte-Anzahl an PCoIP-Daten, die seit dem Start der PCoIP-Sitzung empfangen wurden.
<code>BytesSent</code>	Gesamte Byte-Anzahl an PCoIP-Daten, die seit dem Start der PCoIP-Sitzung übertragen wurden.
<code>PacketsReceived</code>	Gesamte Anzahl der Pakete, die seit dem Start der PCoIP-Sitzung erfolgreich empfangen wurden. Nicht alle Pakete sind gleich groß.
<code>PacketsSent</code>	Gesamte Anzahl der Pakete, die seit dem Start der PCoIP-Sitzung übertragen wurden. Nicht alle Pakete sind gleich groß.
<code>RXPacketsLost</code>	Gesamte Anzahl der empfangenen Pakete, die seit dem Start der PCoIP-Sitzung verloren gegangen sind.
<code>SessionDurationSeconds</code>	Gesamte Anzahl an Sekunden, in denen die PCoIP-Sitzung geöffnet war.
<code>TXPacketsLost</code>	Gesamte Anzahl der übertragenen Pakete, die seit dem Start der PCoIP-Sitzung verloren gegangen sind.

Berechnen der Bandbreite für empfangene PCoIP-Daten

Mit der folgenden Formel können Sie die Bandbreite in Kilobit pro Sekunde für die im Zeitintervall von `t1` bis `t2` empfangenen PCoIP-Daten berechnen.

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

Berechnen der Bandbreite für übertragene PCoIP-Daten

Mit der folgenden Formel können Sie die Bandbreite in Kilobit pro Sekunde für die im Zeitintervall von `t1` bis `t2` übertragenen PCoIP-Daten berechnen.

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

Berechnen des Paketverlustes für empfangene PCoIP-Daten

Mit der folgenden Formel können Sie den Prozentsatz der verloren gegangenen empfangenen Pakete berechnen.

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

Berechnen des Paketverlustes für übertragene PCoIP-Daten

Mit der folgenden Formel können Sie den Prozentsatz der verloren gegangenen übertragenen Pakete berechnen.

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

PCoIP-Audiostatistiken

Der Name der WMI-Klasse für PCoIP-Audiostatistiken lautet `Win32_PerfRawData_TeradiciPerf_PCoIPSessionAudioStatistics`.

Hinweis Audiostatistiken enthalten keine Audiodaten, die mit USB-Daten übertragen werden.

Tabelle 6-2. PCoIP-Audiostatistiken

Name der WMI-Eigenschaft	Beschreibung
AudioBytesReceived	Gesamte Byte-Anzahl der Audiodaten, die seit dem Start der PCoIP-Sitzung empfangen wurden.
AudioBytesSent	Gesamte Byte-Anzahl der Audiodaten, die seit dem Start der PCoIP-Sitzung gesendet wurden.
AudioRXBkbitPersec	Durchschnittliche Bandbreite im Abfragezeitraum für eingehende Audiopakete in Sekunden.
AudioTXBkbitPersec	Durchschnittliche Bandbreite im Abfragezeitraum für ausgehende Audiopakete in Sekunden.
AudioTXBWLimitkbitPersec	Maximale Übertragungsbandbreite für ausgehende Audiopakete in Kilobit pro Sekunde. Dieser Grenzwert wird durch eine GPO-Einstellung definiert.

Berechnen der Bandbreite für empfangene Audiodaten

Verwenden Sie zum Berechnen der Bandbreite für empfangene Audiodaten (in Kilobit pro Sekunde) im Zeitintervall von t1 bis t2 die folgende Formel:

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

Verwenden Sie für diese Berechnung nicht `AudioRXBkbitPersec`.

Berechnen der Bandbreite für übertragene Audiodaten

Verwenden Sie zum Berechnen der Bandbreite für übertragene Audiodaten (in Kilobit pro Sekunde) im Zeitintervall von t1 bis t2 die folgende Formel:

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

Verwenden Sie für diese Berechnung nicht AudioTXBkbitPersec.

PCoIP-Bildverarbeitungsstatistiken

Der Name der WMI-Klasse für PCoIP-Bildverarbeitungsstatistiken lautet Win32_PerfRawData_TeradiciPerf_PCoIPSessionImagingStatistics.

Tabelle 6-3. PCoIP-Bildverarbeitungsstatistiken

Name der WMI-Eigenschaft	Beschreibung
ImagingBytesReceived	Gesamte Byte-Anzahl der Bildverarbeitungsdaten, die seit dem Start der PCoIP-Sitzung empfangen wurden.
ImagingBytesSent	Gesamte Byte-Anzahl der Bildverarbeitungsdaten, die seit dem Start der PCoIP-Sitzung übertragen wurden.
ImagingDecoderCapabilitykbitPersec	Geschätzte Verarbeitungskapazität des Bildverarbeitungs-Decoders in Kilobit pro Sekunde. Diese Statistik wird einmal pro Sekunde aktualisiert.
ImagingEncodedFramesPersec	Anzahl der Bildverarbeitungs-Frames, die in einem Abfragezeitraum von einer Sekunde codiert wurden.
ImagingActiveMinimumQuality	Niedrigster Wert der Kodierungsqualität von 0 bis 100. Diese Statistik wird einmal pro Sekunde aktualisiert. Dieser Indikator entspricht nicht der GPO-Einstellung für die Mindestqualität.
ImagingRXBkbitPersec	Durchschnittliche Bandbreite im Abfragezeitraum für eingehende Bildverarbeitungspakete in Sekunden.
ImagingTXBkbitPersec	Durchschnittliche Bandbreite im Abfragezeitraum für ausgehende Bildverarbeitungspakete in Sekunden.

Berechnen der Bandbreite für empfangene Bildverarbeitungsdaten

Verwenden Sie zum Berechnen der Bandbreite für empfangene Bildverarbeitungsdaten (in Kilobit pro Sekunde) im Zeitintervall von t1 bis t2 die folgende Formel:

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

Verwenden Sie für die Berechnung nicht ImagingRXBkbitPersec.

Berechnen der Bandbreite für übertragene Bildverarbeitungsdaten

Verwenden Sie zum Berechnen der Bandbreite für übertragene Bildverarbeitungsdaten (in Kilobit pro Sekunde) im Zeitintervall von t1 bis t2 die folgende Formel:

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

Verwenden Sie für die Berechnung nicht ImagingTXBwKbitPersec.

PCoIP-Netzwerkstatistiken

Der Name der WMI-Klasse für PCoIP-Netzwerkstatistiken lautet Win32_PerfRawData_TeradiciPerf_PCoIPSessionNetworkStatistics.

Tabelle 6-4. PCoIP-Netzwerkstatistiken

Name der WMI-Eigenschaft	Beschreibung
RoundTripLatencymsec	Round-Trip-Latenz (in Millisekunden) zwischen PCoIP Server und PCoIP Client.
RXBWkbitPersec	Gesamte durchschnittliche Bandbreite im Abfragezeitraum für eingehende PCoIP-Pakete in Sekunden.
RXBWPeakkbitPersec	Maximale Bandbreite für eingehende PCoIP-Pakete in Kilobit pro Sekunde in einem Abfragezeitraum von einer Sekunde.
RXPacketLossPercent	Prozentsatz der empfangenen Pakete, die in einem Abfragezeitraum verloren gehen.
TXBWkbitPersec	Gesamte durchschnittliche Bandbreite im Abfragezeitraum für ausgehende PCoIP-Pakete in Sekunden.
TXBWActiveLimitkbitPersec	Geschätzte verfügbare Netzwerkbandbreite in Kilobit pro Sekunde. Diese Statistik wird einmal pro Sekunde aktualisiert.
TXBWLimitskbitPersec	Maximale Übertragungsbandbreite für ausgehende Pakete in Kilobit pro Sekunde. Der gültige Grenzwert wird aus dem Mindestwert der im Folgenden aufgeführten Werte ermittelt. <ul style="list-style-type: none"> ■ Maximale GPO-Bandbreite für den PCoIP Client ■ Maximale GPO-Bandbreite für den PCoIP Server ■ Maximale Bandbreite für die lokale Netzwerkverbindung ■ Ausgehandelte maximale Bandbreite für die Zero Client-Firmware, basierend auf den Verschlüsselungsgrenzwerten.
TXPacketLossPercent	Prozentsatz der übertragenen Pakete, die in einem Abfragezeitraum verloren gehen.

Berechnen der Bandbreite für empfangene Netzwerkdaten

Verwenden Sie zum Berechnen der Bandbreite für empfangene Daten (in Kilobit pro Sekunde) im Zeitintervall von t1 bis t2 die folgende Formel:

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

Verwenden Sie für die Berechnung nicht RXBWkbitPersec.

Berechnen der Bandbreite für übertragene Netzwerkdaten

Verwenden Sie zum Berechnen der Bandbreite für übertragene Netzwerkdaten (in Kilobit pro Sekunde) im Zeitintervall von t1 bis t2 die folgende Formel:

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

Verwenden Sie für die Berechnung nicht TXBWkbitPersec.

Berechnen des Paketverlustes für empfangene Netzwerkdaten

Verwenden Sie zum Berechnen des Paketverlustes für empfangene Daten (in Prozent) im Zeitintervall von t1 bis t2 die folgende Formel:

$$\text{PacketsReceived during interval} = (\text{PacketsReceived}[t2] - \text{PacketsReceived}[t1])$$

$$\text{RXPacketsLost during interval} = (\text{RXPacketsLost}[t2] - \text{RXPacketsLost}[t1])$$

$$\text{RXPacketsLost \%} = \text{RXPacketsLost during interval} / (\text{RXPacketsLost during interval} + \text{PacketsReceived during interval}) * 100$$

Verwenden Sie für die Berechnung nicht RXPacketLostPercent oder RXPacketLostPercent_Base.

Berechnen des Paketverlustes für übertragene Netzwerkdaten

Verwenden Sie zum Berechnen des Paketverlustes für übertragene Daten (in Prozent) im Zeitintervall von t1 bis t2 die folgende Formel:

$$\text{PacketsSent during interval} = (\text{PacketsSent}[t2] - \text{PacketsSent}[t1])$$

$$\text{TXPacketsLost during interval} = (\text{TXPacketsLost}[t2] - \text{TXPacketsLost}[t1])$$

$$\text{TXPacketsLost \%} = \text{TXPacketsLost during interval} / (\text{TXPacketsLost during interval} + \text{PacketsSent during interval}) * 100$$

Verwenden Sie für die Berechnung nicht TXPacketLostPercent oder TXPacketLostPercent_Base.

Verwenden Sie diese Formel, um zu verhindern, dass der prozentuale Paketverlust größer als 100 Prozent wird. Diese Berechnung ist erforderlich, da PacketsLost und PacketsSent asynchron sind.

PCoIP-USB-Statistiken

Der Name der WMI-Klasse für PCoIP-USB-Statistiken lautet Win32_PerfRawData_TeradiciPerf_PCoIPSessionUSBStatistics.

Tabelle 6-5. PCoIP-USB-Statistiken

Name der WMI-Eigenschaft	Beschreibung
USBBytesReceived	Gesamte Byte-Anzahl der USB-Daten, die seit dem Start der PCoIP-Sitzung empfangen wurden.
USBBytesSent	Gesamte Byte-Anzahl der USB-Daten, die seit dem Start der PCoIP-Sitzung übertragen wurden.
USBRXBWkbitPersec	Durchschnittliche Bandbreite im Abfragezeitraum für eingehende USB-Pakete in Sekunden.
USBTXBWkbitPersec	Durchschnittliche Bandbreite im Abfragezeitraum für ausgehende USB-Pakete in Sekunden.

Berechnen der Bandbreite für empfangene USB-Daten

Verwenden Sie zum Berechnen der Bandbreite für empfangene USB-Daten (in Kilobit pro Sekunde) im Zeitintervall von t1 bis t2 die folgende Formel:

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

Verwenden Sie für die Berechnung nicht USBRXBWkbitPersec.

Berechnen der Bandbreite für übertragene USB-Daten

Verwenden Sie zum Berechnen der Bandbreite für übertragene USB-Daten (in Kilobit pro Sekunde) im Zeitintervall von t1 bis t2 die folgende Formel:

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

Verwenden Sie für die Berechnung nicht USBTXBWkbitPersec.

Beispiele für die Verwendung von PowerShell-Cmdlets für die Untersuchung von PCoIP-Statistiken

Sie können mithilfe von PowerShell-Cmdlets PCoIP-Statistiken untersuchen.

Im folgenden Beispiel ruft das Cmdlet `Get-WmiObject` PCoIP-Netzwerkstatistiken für den Client „cm-02“ ab.

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

Im folgenden Beispiel ruft das Cmdlet `Get-WmiObject` die allgemeinen PCoIP-Sitzungsstatistiken für den Desktop „dt-03“ ab, wenn ein übertragenes Paket verloren gegangen ist.

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


Festlegen von Desktop-Richtlinien mit Sitzungsstartskripts

7

Mit Sitzungsstartskripts können Sie bestimmte Horizon 7-Desktop-Einstellungen konfigurieren, bevor eine Desktop-Sitzung basierend auf Daten aus Horizon Client und vom Horizon Connection Server gestartet wird.

Beispielsweise können Sie mit einem Sitzungsstartskript Desktop-Richtlinien basierend auf dem Clientgerät und dem Benutzerstandort konfigurieren, statt mehrere Desktop-Pools mit unterschiedlichen Desktop-Richtlinien einzurichten. Ein Sitzungsstartskript kann auch zugeordnete Laufwerke, die Umleitung der Zwischenablage und andere Desktop-Funktionen für einen Benutzer mit einer IP-Adresse in der internen Domäne Ihrer Organisation aktivieren, diese Funktionen aber für einen Benutzer mit einer IP-Adresse in einer externen Domäne sperren.

Dieses Kapitel enthält die folgenden Themen:

- [Abrufen von Eingabedaten für ein Sitzungsstartskript](#)
- [Best Practices für die Verwendung von Sitzungsstartskripts](#)
- [Vorbereiten eines Horizon 7-Desktops für die Verwendung eines Sitzungsstartskripts](#)
- [Beispiele für Sitzungsstartskripts](#)

Abrufen von Eingabedaten für ein Sitzungsstartskript

Sitzungsstartskripts können nicht interaktiv ausgeführt werden. Ein Sitzungsstartskript wird in einer von Horizon 7 erstellten Umgebung ausgeführt und muss seine Eingabedaten aus dieser Umgebung abrufen.

Sitzungsstartskripts erfassen Eingabedaten aus Umgebungsvariablen auf dem Clientcomputer. Umgebungsvariablen für den Sitzungsstart haben das Präfix `VDM_StartSession_`. Beispielsweise lautet die Umgebungsvariable für den Sitzungsstart, die die IP-Adresse des Clientsystems enthält, `VDM_StartSession_IP_Address`. Sie müssen sicherstellen, dass ein Sitzungsstartskript das Vorhandensein einer Umgebungsvariable überprüft, die es verwenden kann.

Eine Liste von mit den Umgebungsvariablen für den Sitzungsstart vergleichbaren Variablen finden Sie unter „An Remote-Desktops gesendete Clientsysteminformationen“ im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Best Practices für die Verwendung von Sitzungsstartskripts

Befolgen Sie die im Folgenden aufgeführten Best Practices, wenn Sie Sitzungsstartskripts verwenden.

Wann Sitzungsstartskripts verwendet werden

Verwenden Sie Sitzungsstartskripts nur dann, wenn Sie Desktop-Richtlinien konfigurieren müssen, bevor eine Sitzung gestartet wird.

Als Best Practice wird empfohlen, die Gruppenrichtlinieneinstellungen Horizon Agent `CommandsToRunOnConnect` und `CommandsToRunOnReconnect` für die Ausführung der Befehlsskripts zu verwenden, wenn eine Desktop-Sitzung verbunden bzw. erneut verbunden wird. Das Ausführen von Skripten in einer Desktop-Sitzung anstelle der Verwendung eines Sitzungsstartskripts ist für die meisten Anwendungsfälle ausreichend.

Weitere Informationen finden Sie im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7* im Abschnitt „Ausführen von Befehlen auf Horizon-Desktops“.

Verwalten von Zeitüberschreitungen bei Sitzungsstarts

Stellen Sie sicher, dass Ihre Sitzungsstartskripts schnell ausgeführt werden.

Wenn Sie in der Windows-Registrierung den Wert `WaitScriptsOnStartSession` festlegen, muss Ihr Sitzungsstartskript ausgeführt worden sein, damit Horizon Agent auf die Sitzungsstartmeldung antworten kann, die der Horizon Connection Server sendet. Ein Skript mit langer Ausführungszeit führt wahrscheinlich zu einer Zeitüberschreitung der `StartSession`-Anforderung.

Wenn eine Zeitüberschreitung auftritt und der Pool dynamische Zuweisungen verwendet, versucht der Verbindungsserver, den Benutzer mit einer anderen virtuellen Maschine zu verbinden. Wenn eine Zeitüberschreitung auftritt und keine virtuelle Maschine verfügbar ist, lehnt der Verbindungsserver die Verbindungsanforderung des Benutzers ab.

Als Best Practice legen Sie eine feste Zeitüberschreitung für den Skriphostvorgang fest, sodass ein aufgetretener Fehler zurückgegeben werden kann, wenn ein Skript zu lange ausgeführt wird.

Verfügbarkeit von Sitzungsstartskripts

Der Pfad, unter dem Sie Ihre Sitzungsstartskripts konfigurieren, darf nur für das SYSTEM-Konto und die lokalen Administratoren zugänglich sein. Legen Sie die Zugriffssteuerungsliste für die Basisschlüssel so fest, dass er nur für diese Konten zugänglich ist.

Als Best Practice platzieren Sie die Sitzungsstartskripts im Verzeichnis `View_Agent_install_path\scripts` z. B.:

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

Standardmäßig ist dieses Verzeichnis nur für das SYSTEM-Konto und die Administratorkonten zugänglich.

Vorbereiten eines Horizon 7-Desktops für die Verwendung eines Sitzungsstartskripts

Um einen Horizon 7-Desktop für die Verwendung eines Sitzungsstartskripts vorzubereiten, müssen Sie den VMware View-Skriphostdienst aktivieren und der Windows-Registrierung Einträge hinzufügen.

Sie müssen alle Horizon 7-Desktops konfigurieren, die zur Ausführung von Sitzungsstartskripten benötigt werden. Horizon 7 bietet keine Möglichkeit zur Weitergabe von Registrierungsänderungen, von Änderungen der VMware View-Skriphostdienstkonfiguration und von Sitzungsstartskripten an mehrere virtuelle Horizon 7-Desktop-Maschinen.

Aktivieren des Skriphostdienstes von VMware View

Sie müssen den Skriphostdienst von VMware View auf jeder virtuellen Horizon 7-Desktop-Maschine aktivieren, auf der Horizon 7 ein Sitzungsstartskript ausführen soll. Der VMware View-Skriphostdienst ist standardmäßig deaktiviert.

Wenn Sie den VMware View-Skriphostdienst konfigurieren, können Sie optional das Benutzerkonto angeben, unter dem das Sitzungsstartskript ausgeführt wird. Sitzungsstartskripts werden im Rahmen des VMware View-Skriphostdienstes ausgeführt. Standardmäßig wird der VMware View-Skriphostdienst für die Ausführung als SYSTEM-Benutzer konfiguriert.

Wichtig Sitzungsstartskripts werden außerhalb einer Desktop-Benutzersitzung und nicht vom Desktop-Benutzerkonto ausgeführt. Die Informationen werden direkt vom Clientcomputer in einem Skript gesendet, das als SYSTEM-Benutzer ausgeführt wird.

Verfahren

- 1 Melden Sie sich bei der virtuellen Horizon 7-Desktop-Maschine an.
- 2 Geben Sie an der Eingabeaufforderung `services.msc` ein, um das Windows-Dienste-Tool zu starten.
- 3 Klicken Sie im Bereich „Details“ mit der rechten Maustaste auf den Eintrag des VMware View-Skriphostdienstes und wählen Sie **Eigenschaften**.
- 4 Wählen Sie auf der Registerkarte **Allgemein** die Option **Automatisch** aus dem Dropdown-Menü **Starttyp**.
- 5 (Optional) Wenn das Sitzungsstartskript nicht vom lokalen Systemkonto ausgeführt werden soll, wählen Sie die Registerkarte **Anmelden** und dann **Dieses Konto** aus und geben Sie den Benutzernamen sowie das Kennwort des Kontos ein, um das Sitzungsstartskript auszuführen.
- 6 Klicken Sie auf **OK** und beenden Sie das Tool „Windows-Dienste“.

Hinzufügen von Windows-Registrierungseinträgen für ein Sitzungsstartskript

Sie müssen Windows-Registrierungseinträge auf jeder virtuellen Horizon-Desktop-Maschine hinzufügen, auf der Horizon ein Sitzungsstartskript ausführen soll.

Voraussetzungen

- Stellen Sie sicher, dass der Pfad, in dem Ihre Sitzungsstartskripts konfiguriert sind, nur für das SYSTEM-Konto und für lokale Administratoren zugänglich ist. Weitere Informationen finden Sie unter [Verfügbarkeit von Sitzungsstartskripten](#).
- Stellen Sie sicher, dass Ihre Sitzungsstartskripts schnell ausgeführt werden. Wenn Sie in der Windows-Registrierung den Wert `WaitScriptsOnStartSession` festlegen, muss Ihr Sitzungsstartskript ausgeführt worden sein, damit Horizon Agent auf die Sitzungsstartmeldung antworten kann, die der Horizon Connection Server sendet. Weitere Informationen finden Sie unter [Verwalten von Zeitüberschreitungen bei Sitzungsstarts](#).

Verfahren

- 1 Melden Sie sich bei der virtuellen Horizon-Desktop-Maschine an.
- 2 Geben Sie an der Eingabeaufforderung `regedit` ein, um den Windows-Registrierungs-Editor zu starten.
- 3 Wechseln Sie in der Registrierung zu `HKLM\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents`.
- 4 Fügen Sie der Registrierung den Pfad zum Sitzungsstartskript hinzu.
 - a Klicken Sie im Navigationsbereich mit der rechten Maustaste auf `ScriptEvents`, wählen Sie **Neu > Schlüssel** und erstellen Sie einen Schlüssel namens `StartSession`.
 - b Klicken Sie im Navigationsbereich mit der rechten Maustaste auf `StartSession`, wählen Sie **Neu > Zeichenfolge** aus und erstellen Sie einen Zeichenfolgenwert, der das auszuführende Sitzungsstartskript identifiziert, z. B. `Beispielskript`.

Um weitere Sitzungsstartskripts auszuführen, erstellen Sie zusätzliche Zeichenfolgenwerte für jedes Skript unter dem Schlüssel `StartSession`. Sie können die Reihenfolge, in der diese Skripts ausgeführt werden, nicht festlegen. Wenn die Skripts in einer bestimmten Reihenfolge ausgeführt werden müssen, rufen Sie diese über ein einzelnes Steuerelementskript auf.

- c Klicken Sie im Themenbereich mit der rechten Maustaste auf den neu erstellten Zeichenfolgenwert und wählen Sie im eingeblendeten Kontextmenü **Ändern** aus.
 - d Geben Sie in das Textfeld **Wert** den Befehl zum Laden Ihres Sitzungsstartskripts ein und klicken Sie auf **OK**.

Geben Sie den vollständigen Pfad des Sitzungsstartskripts und aller Dateien ein, die es erfordert.
- 5 Fügen Sie der Registrierung einen Sitzungsstartwert hinzu und aktivieren Sie diesen.
 - a Wechseln Sie zu `HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Configuration`.
 - b (Optional) Wenn der Schlüssel `Configuration` nicht vorhanden ist, klicken Sie mit der rechten Maustaste auf **Agent** und wählen Sie **Neu > Schlüssel** aus. Erstellen Sie dann den Schlüssel.
 - c Klicken Sie im Navigationsbereich mit der rechten Maustaste auf `Configuration`, wählen Sie **Neu > DWORD-Wert (32 Bit)** aus und geben Sie `RunScriptsOnStartSession` ein.

- d Klicken Sie im Themenbereich mit der rechten Maustaste auf den neu erstellten DWORD-Wert und wählen Sie **Ändern** aus.

- e Geben Sie in das Textfeld **Wert** 1 ein, um das Sitzungsstartskript zu aktivieren. Klicken Sie auf **OK**.

Geben Sie 0 ein, um diese Funktion zu deaktivieren. Der Standardwert ist 0.

- f (Optional) Zum Verzögern der StartSession-Antwort durch Horizon Agent fügen Sie einen zweiten DWORD-Wert in den Schlüssel Configuration ein. Dieser muss den Namen WaitScriptsOnStartSession erhalten.

Der Wert 1 für WaitScriptsOnStartSession bewirkt eine Verzögerung, bevor von Horizon Agent eine StartSession-Antwort gesendet wird, und ein Fehlschlagen, falls die Skripts nicht ausgeführt werden. Der Wert 0 bedeutet, dass Horizon Agent nicht wartet, bis die Skripts ausgeführt sind, oder die Beendigungscodes der Skripts prüft, bevor die StartSession-Antwort gesendet wird. Der Standardwert ist 0.

- 6 Legen Sie einen Registrierungswert fest, um Zeitüberschreitungswerte in Sekunden anstelle von Minuten anzugeben und so zu verhindern, dass Skripts einer Zeitüberschreitung unterliegen.

Das Festlegen dieses Zeitüberschreitungswerts in Sekunden ermöglicht Ihnen, den Zeitüberschreitungswert für den VMware View-Skriphostdienst in Sekunden zu konfigurieren. Beispiel: Wenn Sie die Zeitüberschreitung für den VMware View-Skriphostdienst auf 30 Sekunden festlegen, können Sie z. B. sicherstellen, dass die Ausführung eines Sitzungsstartskripts entweder abgeschlossen ist oder eine Zeitüberschreitung erfolgt, bevor eine Zeitüberschreitung des Verbindungsservers auftritt.

- a Wechseln Sie zu HKLM\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents.
- b Fügen Sie einen DWORD-Wert namens TimeoutsInMinutes hinzu.
- c Legen Sie den Wert 0 fest.

- 7 (Optional) Damit der VMware View-Skriphostdienst eine Zeitüberschreitung des Sitzungsstartskripts auslösen kann, müssen Sie einen Wert für die Zeitüberschreitung festlegen.

- a Wechseln Sie zu HKLM\SOFTWARE\VMware, Inc.\VMware VDM\ScriptEvents\StartSession.
- b Klicken Sie mit der rechten Maustaste auf den Schlüssel Default (@) und wählen Sie **Ändern** aus.
- c Klicken Sie in das Textfeld **Wert**, geben Sie den Wert der Zeitüberschreitung ein und klicken Sie auf **OK**.

Der Wert 0 bedeutet, dass keine Zeitüberschreitung festgelegt ist.

- 8 Beenden Sie den Registrierungs-Editor und starten Sie das System neu.

Beispiele für Sitzungsstartskripts

Diese Beispielskripts für Sitzungsstarts veranschaulichen das Schreiben von Umgebungsvariablen in eine Datei, das Testen der Zeitüberschreitungsfunctionalität und das Testen eines Beendigungscodees ungleich Null.

Das folgende Visual Basic-Beispielskript schreibt alle bereitgestellten Umgebungsvariablen in eine Datei. Sie können mit diesem Beispielskript Beispieldaten in Ihrer eigenen Umgebung anzeigen. Dieses Skript lässt sich beispielsweise als `C:\sample.vbs` speichern.

```
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
```

Das folgende Beispielskript testet die Zeitüberschreitungsfunctionalität.

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

Das folgende Beispielskript testet einen Beendigungscode ungleich Null.

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

Verwenden des Horizon PowerCLI-Moduls

8

Das Horizon PowerCLI-Modul enthält Horizon PowerCLI-Cmdlets, die Sie zum Ausführen verschiedener Administrationsaufgaben auf Horizon-Komponenten verwenden können. Sie können Horizon PowerCLI mit API-Spezifikationen verwenden, um Community-basierte Open-Source-Skripte zu erstellen.

Sie können das Horizon PowerCLI-Modul bei der Installation von VMware PowerCLI installieren.

Weitere Informationen zu Horizon PowerCLI-Cmdlets finden Sie im Dokument *Referenz zu VMware PowerCLI-Cmdlets* unter <https://code.vmware.com/docs/6978/cmdlet-reference>.

Informationen zu den API-Spezifikationen für das Erstellen erweiterter Funktionen und Skripten zur Verwendung mit Horizon PowerCLI finden Sie in der View API-Referenz unter <https://code.vmware.com/apis/405/view>.

Weitere Informationen zu Beispielskripten, mit denen Sie Ihre eigenen Horizon PowerCLI-Skripte erstellen können, erhalten Sie in der PowerCLI-Community unter <https://github.com/vmware/PowerCLI-Example-Scripts>.

Dieses Kapitel enthält die folgenden Themen:

- [Einrichten des Horizon PowerCLI-Moduls](#)
- [Ausführen von Horizon PowerCLI-Beispielskripten](#)

Einrichten des Horizon PowerCLI-Moduls

Sie können das Horizon PowerCLI-Modul mit VMware PowerCLI einrichten und die Horizon PowerCLI-Cmdlets zum Verbinden mit dem oder Trennen vom Verbindungsserver verwenden. Nachdem Sie eine Verbindung zum Verbindungsserver hergestellt haben, können Sie PowerShell-Skripte schreiben, die die Horizon-APIs aufrufen.

Verfahren

1 Installieren Sie VMware PowerCLI.

Installieren Sie VMware PowerCLI aus der PowerShell-Galerie. Um VMware PowerCLI zu installieren, führen Sie den folgenden Befehl in der Windows PowerShell-Eingabeaufforderung aus:

```
Install-Module -Name VMware.PowerCLI
```

Dieser Befehl installiert alle VMware PowerCLI-Module in Windows PowerShell. Das Modul `VMware.VimAutomation.HorizonView` ist das Horizon PowerCLI-Modul.

Sie können VMware PowerCLI auch von <https://code.vmware.com/web/dp/tool/vmware-powercli> herunterladen und installieren.

Weitere Informationen zur Installation von VMware PowerCLI finden Sie im *Benutzerhandbuch zu VMware PowerCLI* unter <https://code.vmware.com/web/dp/tool/vmware-powercli>.

2 Importieren Sie das Horizon PowerCLI-Modul mit dem Namen `VMware.VimAutomation.HorizonView` in die Windows PowerShell-Sitzung.

Verwenden Sie den folgenden Befehl, um `VMware.VimAutomation.HorizonView` in die Windows PowerShell-Sitzung zu importieren:

```
Import-Module -Name VMware.VimAutomation.HorizonView
```

`VMware.VimAutomation.HorizonView` enthält die `Connect-HVServer`- und `Disconnect-HVServer`-Cmdlets, die Sie zum Verbinden mit einem Verbindungsserver oder Trennen von einem Verbindungsserver verwenden können.

3 Rufen Sie Beispielskripte aus dem Github-Repository ab.

Nachdem Sie das `Connect-HVServer`-Cmdlet für die Verbindung mit dem Horizon-API-Dienst des Verbindungsservers verwendet haben, können Sie PowerShell-Skripte ausführen, die die Horizon-APIs aufrufen. Weitere Informationen zu Horizon-APIs finden Sie in der Dokumentation *View-API-Referenz* unter <https://code.vmware.com/apis/405/view>.

Beispielskripte für das Horizon PowerCLI-Modul stehen als Modul `VMware.Hv.Helper` im Abschnitt „Modules“ unter <https://github.com/vmware/PowerCLI-Example-Scripts> zur Verfügung.

Nächste Schritte

Verwenden Sie die Beispielskripte direkt oder ändern Sie die Skripte entsprechend Ihren Automatisierungsanforderungen. Zusätzlich zu den Beispielskripten können Sie auch neue Skripte entwickeln, die Horizon-APIs gemäß Ihren Anforderungen aufrufen. Siehe [Ausführen von Horizon PowerCLI-Beispielskripten](#).

Ausführen von Horizon PowerCLI-Beispielskripten

Sie können Beispielskripte verwenden, die Horizon-APIs aufrufen, und mit diesen Skripten Horizon 7-Administratortasks durchführen. Sie können diese Skripte auch ändern, um administrative Aufgaben je nach Ihren Anforderungen auszuführen.

Voraussetzungen

- Führen Sie die Schritte zum Installieren von VMware PowerCLI und Einrichten des Horizon PowerCLI-Moduls aus. Siehe [Einrichten des Horizon PowerCLI-Moduls](#).

Verfahren

- 1 Laden Sie das Modul `VMware.Hv.Helper` vom Abschnitt „Modules“ unter <https://github.com/vmware/PowerCLI-Example-Scripts> herunter.
- 2 Verwenden Sie den Befehl `$env:PSModulePath`, um den Modulpfad in Ihrer Windows PowerShell-Sitzung zu ermitteln, und kopieren Sie das Modul `VMware.Hv.Helper` in diesen Speicherort.
- 3 Verwenden Sie den folgenden Befehl zum Laden des Moduls `VMware.Hv.Helper` in Ihrer Windows PowerShell-Sitzung und beginnen Sie mit der Verwendung der Skripte.

```
Get-Module -ListAvailable 'VMware.Hv.Helper' | Import-Module Get-Command -Module  
'VMware.Hv.Helper'
```