

Verwalten der Cloud-Pod-Architektur in Horizon 7

MÄRZ 2020

VMware Horizon 7 7.12

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

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

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 © 2020 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

Verwalten von Cloud-Pod-Architektur in Horizon 7 6

1 Einführung in Cloud-Pod-Architektur 7

- Grundlegendes zu Cloud-Pod-Architektur 7
 - Gemeinsames Nutzen von Schlüsseldaten in der globalen Datenschicht 8
 - Senden von Nachrichten zwischen Pods 8
- Konfigurieren und Verwalten einer Cloud-Pod-Architektur-Umgebung 9
- Cloud-Pod-Architektur-Einschränkungen 9

2 Entwerfen einer Cloud-Pod-Architektur-Topologie 10

- Erstellen von Cloud-Pod-Architektur-Sites 11
- Berechtigung erteilen für Benutzer und Gruppen im Pod-Verbund 11
- Suchen und Zuweisen von Desktops und Anwendungen im Pod-Verbund 12
 - Grundlegendes zur Geltungsbereichsrichtlinie 13
 - Grundlegendes zur Richtlinie für mehrere Sitzungen pro Benutzer für globale Desktop-Berechtigungen 13
 - Verwenden von Start-Sites 13
- Überlegungen zu Benutzern für einen nicht authentifizierten Zugriff 14
- Beispiel für eine globale Berechtigung 15
- Implementieren von Verbindungsserver-Einschränkungen für globale Berechtigungen 16
 - Kennzeichenabgleich 17
 - Anforderungen und Beschränkungen für Verbindungsserver-Einschränkungen 17
 - Beispiel für Verbindungsserver-Einschränkungen 18
- Implementieren von Clienteneinschränkungen für globale Berechtigungen 19
- Implementieren der Funktion zum Vorabstart der Sitzung für globale Anwendungsberechtigungen 20
- Aktivieren des Mehrfach Sitzungsmodus für globale Anwendungsberechtigungen 20
- Aktivieren der Funktion „Session Collaboration“ für globale Desktopberechtigungen 21
- Implementieren von globalen Sicherheitsberechtigungen 22
- Überlegungen zu Umgebungen mit gemischten Versionen 23
- Grundlegendes zum Workspace ONE-Modus 23
- Überlegungen zu VMware Cloud on AWS 23
- Überlegungen für RDS-Clientzugriffslizenz auf Gerätebasis 23
- Einschränkungen für Cloud-Pod-Architektur-Topologie 24
- Anforderungen an den Cloud-Pod-Architektur-Port 24
- Sicherheitsüberlegungen für Cloud-Pod-Architektur-Topologien 25

3 Einrichten von Cloud-Pod-Architektur in Horizon Console 26

Initialisieren der Cloud-Pod-Architektur-Funktion in Horizon Console	27
Hinzufügen eines Pods zu einem Pod-Verbund in Horizon Console	27
Zuweisen eines Tags zu einer Verbindungsserver-Instanz in Horizon Console	29
Konfigurieren von Verknüpfungen für globale Berechtigungen	29
Arbeitsblatt zur Konfiguration einer globalen Berechtigung	30
Erstellen und Konfigurieren einer globalen Berechtigung in Horizon Console	36
Hinzufügen eines Pools zu einer globalen Berechtigung in Horizon Console	38
Erstellen und Konfigurieren einer Site in Horizon Console	39
Zuweisen einer Start-Site zu einem Benutzer oder einer Gruppe in Horizon Console	40
Erstellen einer Außerkraftsetzung der Start-Site in Horizon Console	41
Testen einer Cloud-Pod-Architektur-Konfiguration in Horizon Client	42
Beispiel: Einrichten einer Cloud-Pod-Architektur-Basiskonfiguration	43
Entwerfen der Beispieltopologie	44
Initialisieren der Beispielkonfiguration	45
Hinzufügen von Pods in der Beispielkonfiguration	45
Erstellen von Sites in der Beispielkonfiguration	45
Erstellen von globalen Desktop-Berechtigungen in der Beispielkonfiguration	46
Erstellen einer URL für die Beispielkonfiguration	47

4 Verwalten einer Cloud-Pod-Architektur-Umgebung in Horizon Console 48

Anzeigen einer Cloud-Pod-Architektur-Konfiguration in Horizon Console	48
Anzeigen des Zustands des Pod-Verbunds in Horizon Console	50
Anzeigen von Desktop- und Anwendungssitzungen in Horizon Console	51
Verwalten von Sites in Horizon Console	53
Hinzufügen eines Pods zu einer Site in Horizon Console	53
Löschen einer Site in Horizon Console	53
Ändern des Namens oder der Beschreibung einer Site in Horizon Console	54
Verwalten von globalen Berechtigungen in Horizon Console	54
Entfernen eines Pools aus einer globalen Berechtigung in Horizon Console	54
Hinzufügen eines Benutzers oder einer Gruppe zu einer globalen Berechtigung in Horizon Console	54
Entfernen eines Benutzers oder einer Gruppe aus einer globalen Berechtigung in Horizon Console	55
Ändern von Attributen oder Richtlinien für eine globale Berechtigung in Horizon Console	55
Löschen einer globalen Berechtigung in Horizon Console	56
Verwalten von Start-Sites in Horizon Console	57
Ändern einer Start-Site-Zuweisung in Horizon Console	57
Entfernen einer Start-Site-Zuweisung in Horizon Console	57
Festlegen der geltenden Start-Site für einen Benutzer in Horizon Console	57
Ändern einer Außerkraftsetzung der Start-Site in Horizon Console	58
Entfernen einer Außerkraftsetzung der Start-Site in Horizon Console	59

Entfernen eines Pods aus dem Pod-Verbund in Horizon Console	59
Aufheben der Initialisierung der Cloud-Pod-Architektur-Funktion in Horizon Console	60

5 Verwalten der Cloud-Pod-Architektur mit Imvutil 61

Verwenden des Befehls „Imvutil“	61
Authentifizierung für den Imvutil-Befehl	62
Ausgabe des Imvutil-Befehls	62
Optionen für den Imvutil-Befehl	63
Initialisieren der Funktion Cloud-Pod-Architektur	65
Deaktivieren der Funktion Cloud-Pod-Architektur	66
Verwalten eines Pod-Verbunds	66
Hinzufügen eines Pods zu einem Pod-Verbund	67
Entfernen eines Pods aus einem Pod-Verbund	67
Ändern des Namens oder der Beschreibung für einen Pod	68
Verwalten von Sites	69
Erstellen einer Site	69
Zuweisen eines Pods zu einer Site	70
Ändern des Namens oder der Beschreibung für eine Site	71
Löschen einer Site	71
Verwalten von globalen Berechtigungen	72
Erstellen einer globalen Berechtigung	73
Ändern einer globalen Berechtigung	77
Löschen einer globalen Berechtigung	82
Hinzufügen eines Pools zu einer globalen Berechtigung	82
Entfernen eines Pools aus einer globalen Berechtigung	83
Hinzufügen eines Benutzers oder einer Gruppe zu einer globalen Berechtigung	84
Entfernen eines Benutzers oder einer Gruppe aus einer globalen Berechtigung	85
Verwalten von Start-Sites	86
Konfigurieren einer Start-Site	86
Löschen einer Start-Site	88
Anzeigen einer Cloud-Pod-Architektur-Konfiguration	89
Auflisten von globalen Berechtigungen	89
Auflisten der Pools in einer globalen Berechtigung	90
Auflisten der Benutzer oder Gruppen in einer globalen Berechtigung	91
Auflisten der Start-Sites für einen Benutzer oder eine Gruppe	91
Auflisten der geltenden Start-Site für einen Benutzer	92
Auflisten von dedizierten Desktop-Pool-Zuweisungen	93
Auflisten der Pods oder Sites in einer Cloud-Pod-Architektur-Topologie	94
Verwalten von SSL-Zertifikaten	94
Erstellen eines ausstehenden Zertifikats	95
Aktivieren eines ausstehenden Zertifikats	95

Verwalten von Cloud-Pod-Architektur in Horizon 7

In *Verwalten der Cloud-Pod-Architektur in Horizon 7* wird beschrieben, wie Sie eine Cloud-Pod-Architektur-Umgebung in VMware Horizon® 7 konfigurieren und verwalten.

Zielgruppe

Dieses Dokument ist für erfahrene Systemadministratoren bestimmt, die mit der Windows- und Linux-VM-Technologie und Datencentervorgängen vertraut sind.

Einführung in Cloud-Pod-Architektur

1

Die Cloud-Pod-Architektur-Funktion verwendet standardmäßige Horizon-Komponenten für die Verwaltung mehrerer Datacenter, die globale und flexible Zuordnung zwischen Benutzern und Desktops, die Bereitstellung von Desktops mit hoher Verfügbarkeit sowie die Notfallwiederherstellung.

Dieses Kapitel enthält die folgenden Themen:

- [Grundlegendes zu Cloud-Pod-Architektur](#)
- [Konfigurieren und Verwalten einer Cloud-Pod-Architektur-Umgebung](#)
- [Cloud-Pod-Architektur-Einschränkungen](#)

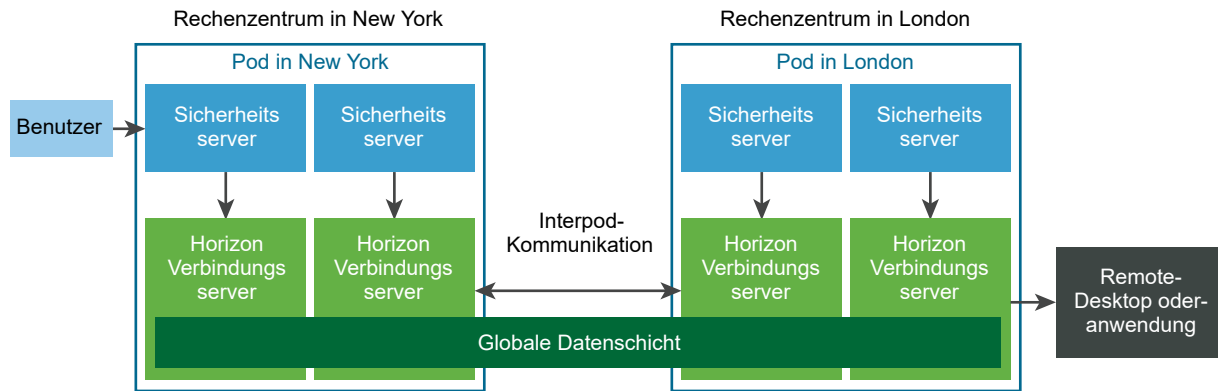
Grundlegendes zu Cloud-Pod-Architektur

Mit der Funktion Cloud-Pod-Architektur können Sie mehrere Pods verbinden, sodass eine einzelne große Umgebung für das Brokering und die Verwaltung von Desktops und Anwendungen entsteht.

Ein Pod besteht aus mehreren Verbindungsserver-Instanzen, einem gemeinsamen Speicher, einem Datenbankserver sowie den vSphere- und Netzwerkinfrastrukturen, die erforderlich sind, um Desktop- und Anwendungspools zu hosten. In einer herkömmlichen Horizon-Implementierung werden die einzelnen Pods unabhängig voneinander verwaltet. Mit der Funktion Cloud-Pod-Architektur können Sie mehrere Pods in einer einzelnen Horizon-Implementierung verbinden, die als Pod-Verbund bezeichnet wird.

Ein Pod-Verbund kann sich über mehrere Sites und Rechenzentren erstrecken und gleichzeitig die Verwaltung von großen Horizon-Bereitstellungen vereinfachen.

Das folgende Diagramm ist ein Beispiel einer einfachen Cloud-Pod-Architektur-Topologie.

Abbildung 1-1. Grundlegende Cloud-Pod-Architektur-Topologie

In der Beispieltopologie werden zwei zuvor eigenständige Pods in verschiedenen Rechenzentren zu einem Pod-Verbund kombiniert. Ein Endbenutzer kann in dieser Umgebung eine Verbindung mit einer Verbindungsserver-Instanz im Rechenzentrum in New York herstellen und einen Desktop oder eine Anwendung im Rechenzentrum in London erhalten.

Gemeinsames Nutzen von Schlüsseldaten in der globalen Datenschicht

Verbindungsserver-Instanzen in einem Pod-Verbund verwenden die globale Datenschicht, um Schlüsseldaten gemeinsam zu nutzen. Zu den gemeinsam genutzten Daten gehören Informationen zur Pod-Verbundtopologie, Benutzer- und Gruppenberechtigungen, Richtlinien und andere Cloud-Pod-Architektur-Konfigurationsinformationen.

In einer Cloud-Pod-Architektur-Umgebung werden gemeinsam genutzte Daten auf jeder Verbindungsserver-Instanz in einem Pod-Verbund repliziert. Die in der globalen Datenschicht gespeicherten Berechtigungs- und Topologiekonfigurationsinformationen bestimmen, wo und wie Desktops im Pod-Verbund zugeordnet werden.

Horizon richtet die globale Datenschicht auf jeder Verbindungsserver-Instanz ein, wenn Sie die Funktion Cloud-Pod-Architektur initialisieren.

Senden von Nachrichten zwischen Pods

Verbindungsserver-Instanzen kommunizieren in einer Cloud-Pod-Architektur-Umgebung mithilfe eines Kommunikationsprotokolls namens View InterPod API (VIPA).

Verbindungsserver-Instanzen verwenden den VIPA-Kommunikationskanal, um neue Desktops zu starten, vorhandene Desktops zu suchen und Integritätsstatusdaten und andere Informationen freizugeben. Horizon konfiguriert den VIPA-Kommunikationskanal, wenn Sie die Funktion Cloud-Pod-Architektur initialisieren.

Konfigurieren und Verwalten einer Cloud-Pod-Architektur-Umgebung

Sie verwenden Horizon Console oder die `lmvutil`-Befehlszeilenschnittstelle, um eine Cloud-Pod-Architektur-Umgebung einzurichten und zu verwalten. `lmvutil` wird im Rahmen der Horizon-Installation installiert. Sie können mit Horizon Console auch Informationen zum Pod-Zustand und zur Sitzung anzeigen.

Cloud-Pod-Architektur-Einschränkungen

Die Funktion Cloud-Pod-Architektur hat bestimmte Einschränkungen.

- Die Funktion Cloud-Pod-Architektur wird in einer IPv6-Umgebung nicht unterstützt.
- Clients im Kiosk-Modus werden in einer Cloud-Pod-Architektur-Implementierung nicht unterstützt, solange Sie keine Problemumgehung implementieren. Anweisungen dazu finden Sie im VMware-Knowledgebase-Artikel [2148888](#).

Entwerfen einer Cloud-Pod-Architektur-Topologie

2

Bevor Sie mit der Konfiguration der Funktion Cloud-Pod-Architektur beginnen, müssen Sie Entscheidungen in Bezug auf die Cloud-Pod-Architektur-Topologie treffen. Cloud-Pod-Architektur-Topologien können sich je nach Ihren Zielen, den Anforderungen der Benutzer und Ihrer vorhandenen Horizon-Implementierung unterscheiden. Wenn Sie vorhandene Horizon-Pods mit einem Pod-Verbund verbinden, basiert die Cloud-Pod-Architektur-Topologie üblicherweise auf der bestehenden Netzwerktopologie.

Dieses Kapitel enthält die folgenden Themen:

- Erstellen von Cloud-Pod-Architektur-Sites
- Berechtigung erteilen für Benutzer und Gruppen im Pod-Verbund
- Suchen und Zuweisen von Desktops und Anwendungen im Pod-Verbund
- Überlegungen zu Benutzern für einen nicht authentifizierten Zugriff
- Beispiel für eine globale Berechtigung
- Implementieren von Verbindungsserver-Einschränkungen für globale Berechtigungen
- Implementieren von Clienteinschränkungen für globale Berechtigungen
- Implementieren der Funktion zum Vorabstart der Sitzung für globale Anwendungsberechtigungen
- Aktivieren des Mehrfachsitzungsmodus für globale Anwendungsberechtigungen
- Aktivieren der Funktion „Session Collaboration“ für globale Desktopberechtigungen
- Implementieren von globalen Sicherheitsberechtigungen
- Überlegungen zu Umgebungen mit gemischten Versionen
- Grundlegendes zum Workspace ONE-Modus
- Überlegungen zu VMware Cloud on AWS
- Überlegungen für RDS-Clientzugriffslizenz auf Gerätebasis
- Einschränkungen für Cloud-Pod-Architektur-Topologie
- Anforderungen an den Cloud-Pod-Architektur-Port

■ Sicherheitsüberlegungen für Cloud-Pod-Architektur-Topologien

Erstellen von Cloud-Pod-Architektur-Sites

In einer Cloud-Pod-Architektur-Umgebung ist eine Site eine Sammlung von verbundenen Pods am gleichen physischen Standort, üblicherweise in einem einzelnen Datencenter. Die Funktion Cloud-Pod-Architektur behandelt Pods in der gleichen Site gleichmäßig.

Wenn Sie die Funktion Cloud-Pod-Architektur initialisieren, werden alle Pods in einer Standard-Site mit der Bezeichnung „Standardmäßige erste Site“ platziert. Bei größeren Implementierungen empfiehlt es sich möglicherweise, weitere Sites zu erstellen und ihnen Pods hinzuzufügen.

Die Funktion Cloud-Pod-Architektur nimmt an, dass sich Pods in der gleichen Site im gleichen LAN befinden und dass sich Pods in unterschiedlichen Sites in unterschiedlichen LANs befinden. Da mit WAN verbundene Pods eine langsamere Netzwerkleistung aufweisen, bevorzugt die Funktion Cloud-Pod-Architektur Desktops und Anwendungen, die sich im lokalen Pod oder in der lokalen Site befinden, wenn Desktops und Anwendungen an Benutzer zugewiesen werden.

Sites können bei einer Lösung für die Wiederherstellung nach einem Ausfall (Disaster Recovery) nützlich sein. Sie können beispielsweise Pods in unterschiedlichen Datencentern unterschiedlichen Sites zuweisen und Benutzern und Gruppen Berechtigungen für Pools erteilen, die diese Sites umfassen. Wenn das Datencenter in einer Site ausfällt, können Sie Desktops und Anwendungen aus der verfügbaren Site verwenden, wenn Benutzer einen Desktop oder eine Anwendung anfordern.

Berechtigung erteilen für Benutzer und Gruppen im Pod-Verbund

In einer herkömmlichen Horizon-Umgebung wird Horizon Console zum Erstellen von lokalen Berechtigungen verwendet. Diese lokalen Berechtigungen gewähren Benutzern und Gruppen den Zugriff auf einen bestimmten Desktop- oder Anwendungspool in einer Verbindungsserver-Instanz.

In einer Cloud-Pod-Architektur-Umgebung erstellen Sie globale Berechtigungen, um eine Berechtigung für Benutzer oder Gruppen für mehrere Desktops und Anwendungen über mehrere Pods im Pod-Verbund zu erteilen. Bei Verwendung von globalen Berechtigungen ist es nicht erforderlich, lokale Berechtigungen zu konfigurieren und zu verwalten. Globale Berechtigungen vereinfachen die Verwaltung, selbst in einem Pod-Verbund, der nur einen einzelnen Pod enthält.

Globale Berechtigungen werden in der globalen Datenschicht gespeichert. Da es sich bei globalen Berechtigungen um gemeinsame Daten handelt, stehen globale Berechtigungsinformationen in allen Verbindungsserver-Instanzen im Pod-Verbund zur Verfügung.

Sie können Benutzern und Gruppen Berechtigungen für Desktops durch Erstellung globaler Desktop-Berechtigungen erteilen. Jede globale Desktop-Berechtigung enthält eine Liste der Benutzer oder Gruppen, die Mitglieder sind, eine Liste der Desktop-Pools, die Desktops für berechtigte Benutzer bereitstellen können, und eine Geltungsbereichsrichtlinie. Die Desktop-Pools in einer globalen Berechtigung können entweder dynamisch oder dediziert sein. Bei der Erstellung einer globalen Berechtigung geben Sie an, ob diese dynamisch oder dediziert sein soll.

Sie können Benutzern und Gruppen Berechtigungen für Anwendungen durch Erstellung globaler Anwendungsberechtigungen erteilen. Jede globale Anwendungsberechtigung enthält eine Liste der Benutzer oder Gruppen, die Mitglieder sind, eine Liste der Anwendungspools, die Anwendungen für berechtigte Benutzer bereitstellen können, und eine Geltungsbereichsrichtlinie.

Die Geltungsbereichsrichtlinie einer globalen Berechtigung gibt an, wo Horizon nach Desktops oder Anwendungen sucht, wenn den Benutzern in der globalen Berechtigung Desktops oder Anwendungen zugeordnet werden. Weiterhin bestimmt diese Richtlinie, in welchen Pods Horizon nach Desktops oder Anwendungen sucht: in einem beliebigen Pod des Pod-Verbunds, in Pods in derselben Site oder nur in dem Pod, mit dem der Benutzer verbunden ist.

Lokale und globale Berechtigungen sollten nicht für denselben Desktop-Pool konfiguriert werden. Wenn Sie beispielsweise sowohl lokale als auch globale Berechtigungen für denselben Desktop-Pool verwenden, wird möglicherweise derselbe Desktop als eine lokale und eine globale Berechtigung in der Liste der Desktops und Anwendungen angezeigt, die in Horizon Client für einen berechtigten Benutzer dargestellt wird. Ebenso sollten Sie für Anwendungspools, die aus derselben Farm erstellt wurden, nicht beides, lokale und globale Berechtigungen, konfigurieren.

Suchen und Zuweisen von Desktops und Anwendungen im Pod-Verbund

Verbindungsserver-Instanzen in einer Cloud-Pod-Architektur-Umgebung verwenden freigegebene Konfigurationsinformationen für globale Berechtigungen und Topologien aus der globalen Datenebene, um festzulegen, in welchem Bereich nach Desktops gesucht wird und wie Desktops und Anwendungen über den Pod-Verbund zugeteilt werden.

Wenn ein Benutzer einen Desktop oder eine Anwendung aus einer globalen Berechtigung anfordert, sucht Horizon nach einem verfügbaren Desktop oder einer verfügbaren Anwendung in den Pools, die mit dieser globalen Berechtigung verknüpft sind. Standardmäßig bevorzugt Horizon den lokalen Pod, die lokale Site und Pods in anderen Sites (in der angegebenen Reihenfolge).

Für globale Desktop-Berechtigungen, die dedizierte Desktop-Pools enthalten, verwendet Horizon das Standardsuchverhalten nur, wenn ein Benutzer zum ersten Mal einen Desktop anfordert. Nachdem Horizon einen dedizierten Desktop zugewiesen hat, navigiert es den Benutzer direkt zum gleichen Desktop.

Sie können das Verhalten beim Suchen und Zuordnen für einzelne globale Berechtigungen ändern, indem Sie die Geltungsbereichsrichtlinie festlegen und Start-Sites konfigurieren.

Grundlegendes zur Geltungsbereichsrichtlinie

Wenn Sie eine globale Desktop- oder Anwendungsberechtigung erstellen, müssen Sie deren Geltungsbereichsrichtlinie festlegen. Die Geltungsbereichsrichtlinie legt den Geltungsbereich einer Suche fest, wenn Horizon Desktops oder Anwendungen sucht, um eine Anforderung von der globalen Berechtigung zu erfüllen.

Sie können die Geltungsbereichsrichtlinie so festlegen, dass Horizon nur in dem Pod sucht, zu dem der Benutzer eine Verbindung hergestellt hat, oder nur in Pods in der gleichen Site wie der Pod des Benutzers oder über alle Pods in dem Pod-Verbund sucht.

Für globale Desktop-Berechtigungen, die dedizierte Pools enthalten, beeinflusst die Geltungsbereichsrichtlinie, wo Horizon Desktops sucht, wenn ein Benutzer zum ersten Mal einen dedizierten Desktop anfordert. Nachdem Horizon einen dedizierten Desktop zugewiesen hat, navigiert es den Benutzer direkt zum gleichen Desktop.

Grundlegendes zur Richtlinie für mehrere Sitzungen pro Benutzer für globale Desktop-Berechtigungen

Wenn Sie eine globale Desktop-Berechtigung erstellen, können Sie festlegen, ob Benutzer die Möglichkeit haben sollen, separate Desktop-Sitzungen von unterschiedlichen Clientgeräten aus zu initiieren. Die Richtlinie für mehrere Sitzungen pro Benutzer gilt nur für globale Desktop-Berechtigungen mit dynamischen Desktop-Pools.

Wenn Sie die Richtlinie für mehrere Sitzungen pro Benutzer aktivieren, werden Benutzer, die eine Verbindung mit der globalen Desktop-Berechtigung von unterschiedlichen Clientgeräten aus herstellen, mit unterschiedlichen Desktop-Sitzungen verbunden. Um erneut eine Verbindung mit einer vorhandenen Desktop-Sitzung herzustellen, müssen Benutzer das Gerät verwenden, von dem aus die Sitzung initiiert wurde. Wenn Sie diese Richtlinie nicht aktivieren, werden Benutzer immer erneut mit ihren vorhandenen Desktop-Sitzungen verbunden, unabhängig vom verwendeten Clientgerät.

Wenn Sie die Richtlinie für mehrere Sitzungen pro Benutzer für eine globale Desktop-Berechtigung aktivieren, müssen alle Desktop-Pools, die mit der globalen Desktop-Berechtigung verknüpft sind, auch mehrere Benutzer pro Sitzung unterstützen.

Verwenden von Start-Sites

Eine Start-Site ist eine Beziehung zwischen einem Benutzer oder einer Gruppe und einer Cloud-Pod-Architektur-Site. Sie können mit Start-Sites sicherstellen, dass Horizon stets von einer bestimmten Site ausgehend nach Desktops und Anwendungen sucht und nicht auf der Grundlage des aktuellen Standorts des Benutzers.

Wenn die Start-Site nicht verfügbar ist oder nicht über ausreichend Ressourcen zur Durchführung der Benutzeranforderung verfügt, sucht Horizon nach anderen Sites gemäß der für diese globale Berechtigung gültigen Geltungsbereichsrichtlinie.

Für globale Desktop-Berechtigungen mit dedizierten Pools beeinflusst die Start-Site, wo Horizon Desktops sucht, wenn ein Benutzer zum ersten Mal einen dedizierten Desktop anfordert. Nachdem Horizon einen dedizierten Desktop zugewiesen hat, navigiert es den Benutzer direkt zum gleichen Desktop.

Die Funktion Cloud-Pod-Architektur beinhaltet die folgenden Typen von Start-Site-Zuweisungen.

Globale Start-Site

Eine einem Benutzer oder einer Gruppe zugewiesene Start-Site.

Wenn ein Benutzer, der eine Start-Site besitzt, zu einer Gruppe gehört, die mit einer anderen Start-Site verknüpft ist, hat die mit dem Benutzer verknüpfte Start-Site Vorrang vor der Zuweisung der Gruppen-Start-Site.

Globale Start-Sites sind nützlich, wenn kontrolliert werden soll, wo Roamingbenutzer Desktops und Anwendungen erhalten. Verfügt beispielsweise ein Benutzer über eine Start-Site in New York, besucht aber gerade London, beginnt Horizon mit einer Suche in der Site von New York, um die Desktop-Anforderung des Benutzers zu erfüllen, anstatt einen Desktop zuzuweisen, der sich näher am Benutzer befindet. Zuweisungen von globalen Start-Sites gelten für alle globalen Berechtigungen.

Wichtig Globale Berechtigungen erkennen Start-Sites nicht standardmäßig. Damit eine globale Berechtigung Start-Sites verwendet, müssen Sie die Option **Start-Site verwenden** auswählen, wenn Sie die globale Berechtigung erstellen oder ändern.

Start-Site mit globaler Berechtigung (Außerkraftsetzung der Start-Site)

Eine einer globalen Berechtigung zugewiesene Start-Site.

Start-Sites mit globaler Berechtigung setzen Zuweisungen für die globale Start-Site außer Kraft. Aus diesem Grund werden Start-Sites mit globaler Berechtigung auch als Außerkraftsetzungen der Start-Site bezeichnet.

Wenn beispielsweise ein Benutzer, der über eine Start-Site in New York verfügt, auf eine globale Berechtigung zugreift, die diesen Benutzer der Start-Site in London zuordnet, beginnt Horizon mit einer Suche in der Site in London, um die Anwendungsanforderung des Benutzers zu erfüllen, anstatt eine Anwendung aus der Site in New York zuzuweisen.

Das Konfigurieren von Start-Sites ist optional. Wenn ein Benutzer nicht über eine Start-Site verfügt, sucht Horizon nach Desktops bzw. Anwendungen und weist diese zu, wie in [Suchen und Zuweisen von Desktops und Anwendungen im Pod-Verbund](#) beschrieben.

Überlegungen zu Benutzern für einen nicht authentifizierten Zugriff

Ein Horizon-Administrator hat die Möglichkeit, Benutzer für einen nicht authentifizierten Zugriff auf veröffentlichte Anwendungen auf einer Verbindungsserver-Instanz zu erstellen. In einer Cloud-Pod-Architektur-Umgebung können Sie diesen Benutzern für einen nicht authentifizierten

Zugriff eine Berechtigung für Anwendungen im gesamten Pod-Verbund erteilen, indem Sie diese globalen Anwendungsberechtigungen hinzufügen.

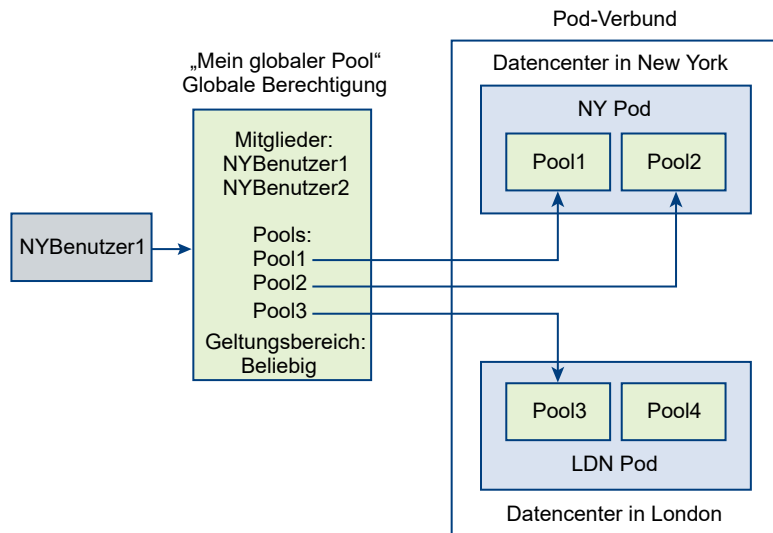
Im Folgenden finden Sie einige Überlegungen zu Benutzern für einen nicht authentifizierten Zugriff in einer Cloud-Pod-Architektur-Umgebung.

- Benutzer für einen nicht authentifizierten Zugriff können nur über globale Anwendungsberechtigungen verfügen. Wenn ein Benutzer für einen nicht authentifizierten Zugriff in einer globalen Desktop-Berechtigung enthalten ist, wird auf der Registerkarte **Benutzer und Gruppen** für die globale Desktop-Berechtigung in Horizon Console ein Warnsymbol neben dem Namen angezeigt.
- Wenn Sie einen Pod zum Pod-Verbund hinzufügen, werden die Daten von Benutzern für einen nicht authentifizierten Zugriff in die globale Datenschicht migriert. Wenn Sie einen Pod mit Benutzern für einen nicht authentifizierten Zugriff aus dem Pod-Verbund entfernen, werden die Daten von Benutzern für einen nicht authentifizierten Zugriff für diesen Pod aus der globalen Datenschicht entfernt.
- Für jeden Active Directory-Benutzer ist nur ein Benutzer für einen nicht authentifizierten Zugriff möglich. Wenn ein Benutzer-Aliasname mehr als einem Active Directory-Benutzer zugeordnet ist, wird im Bereich „Benutzer und Gruppen“ der Registerkarte **Nicht authentifizierter Zugriff** in Horizon Console eine Fehlermeldung angezeigt.
- Sie haben die Möglichkeit, Benutzern für einen nicht authentifizierten Zugriff Start-Sites zuzuweisen.
- Benutzer für einen nicht authentifizierten Zugriff können über mehrere Sitzungen verfügen.
- Benutzer mit nicht authentifiziertem Zugriff haben keine Berechtigung für globale Anwendungsberechtigungen, bei denen Anwendungen aus einem Desktop-Pool veröffentlicht werden.

Informationen zur Einrichtung von Benutzern für einen nicht authentifizierten Zugriff finden Sie im Dokument *Horizon 7-Verwaltung*.

Beispiel für eine globale Berechtigung

In diesem Beispiel ist „NYBenutzer1“ ein Mitglied der globalen Desktop-Berechtigung namens „Mein globaler Pool“. „Mein globaler Pool“ bietet eine Berechtigung für drei dynamische Desktop-Pools, die als Pool1, Pool2 und Pool3 bezeichnet werden. Pool1 und Pool2 befinden sich in einem Pod namens „NY Pod“ im New Yorker Datencenter. Pool3 und Pool4 befinden sich in einem Pod namens „LDN Pod“ im Londoner Datencenter.

Abbildung 2-1. Beispiel für eine globale Berechtigung

Da „Mein globaler Pool“ über eine Geltungsbereichsrichtlinie BELIEBIG verfügt, sucht die Funktion Cloud-Pod-Architektur nach Desktops über NY Pod und LDN Pod, wenn NYBenutzer1 einen Desktop anfordert. Die Funktion Cloud-Pod-Architektur versucht nicht, einen Desktop aus Pool4 zuzuteilen, da Pool4 nicht Teil von „Mein globaler Pool“ ist.

Wenn sich NYBenutzer1 bei NY Pod anmeldet, weist die Funktion Cloud-Pod-Architektur einen Desktop aus Pool1 oder Pool2 zu, wenn ein Desktop verfügbar ist. Wenn weder in Pool1 oder in Pool2 ein Desktop verfügbar ist, weist die Funktion Cloud-Pod-Architektur einen Desktop aus Pool3 zu.

Ein Beispiel für eingeschränkte globale Berechtigungen finden Sie unter [Beispiel für Verbindungsserver-Einschränkungen](#).

Implementieren von Verbindungsserver-Einschränkungen für globale Berechtigungen

Sie können den Zugriff auf globale Berechtigungen auf der Basis der Verbindungsserver-Instanz einschränken, mit der Benutzer anfänglich eine Verbindung herstellen, wenn sie globale Berechtigungen auswählen.

Bei der Funktion zur Einschränkung für Verbindungsserver weisen Sie einer Verbindungsserver-Instanz eine oder mehrere Kennzeichen zu. Wenn Sie anschließend eine globale Berechtigung konfigurieren, geben Sie die Kennzeichen der Verbindungsserver-Instanzen an, die auf die globale Berechtigung zugreifen sollen.

Sie haben die Möglichkeit, sowohl globalen Desktop-Berechtigungen wie globalen Anwendungsberechtigungen Kennzeichen zuzuweisen.

Kennzeichenabgleich

Die Verbindungsserver-Einschränkungsfunktion ermittelt anhand des Kennzeichenabgleichs, ob eine Verbindungsserver-Instanz auf eine bestimmte globale Berechtigung zugreifen kann.

Beim Kennzeichenabgleich wird im Wesentlichen festgestellt, ob eine Verbindungsserver-Instanz mit einem bestimmten Kennzeichen auf eine globale Berechtigung zugreifen kann, die das gleiche Kennzeichen aufweist.

Wenn keine Kennzeichen zugewiesen wurden, kann dies auch Einfluss darauf haben, ob Benutzer, die mit einer Verbindungsserver-Instanz verbunden sind, auf eine globale Berechtigung zugreifen können. Verbindungsserver-Instanzen ohne Kennzeichen können beispielsweise nur auf globale Berechtigungen zugreifen, die ebenfalls nicht über Kennzeichen verfügen.

[Tabelle 2-1. Regeln für den Kennzeichenabgleich](#) zeigt, wie der Kennzeichenabgleich festlegt, wann eine Verbindungsserver-Instanz auf eine globale Berechtigung zugreifen kann.

Tabelle 2-1. Regeln für den Kennzeichenabgleich

Verbindungsserver	Globale Berechtigung	Zugriff zulässig?
Keine Kennzeichen	Keine Kennzeichen	Ja
Keine Kennzeichen	Mindestens ein Kennzeichen	Nein
Mindestens ein Kennzeichen	Keine Kennzeichen	Ja
Mindestens ein Kennzeichen	Mindestens ein Kennzeichen	Nur bei übereinstimmenden Kennzeichen

Die Verbindungsserver-Einschränkungsfunktion erzwingt nur die Übereinstimmung mit Kennzeichen. Sie müssen Ihre Netzwerktopologie ändern, um bestimmte Clients zu zwingen, sich über eine bestimmte Verbindungsserver-Instanz anzumelden.

Anforderungen und Beschränkungen für Verbindungsserver-Einschränkungen

Vor der Implementierung von Verbindungsserver-Einschränkungen für globale Berechtigungen müssen Sie bestimmte Anforderungen und Beschränkungen beachten.

- Einzelne Verbindungsserver-Instanzen oder globale Berechtigungen können über mehrere Kennzeichen verfügen.
- Mehrere Verbindungsserver-Instanzen und globale Berechtigungen können über dasselbe Kennzeichen verfügen.
- Jede Verbindungsserver-Instanz kann auf eine globale Berechtigung ohne Kennzeichen zugreifen.
- Verbindungsserver-Instanzen ohne Kennzeichen können nur auf globale Berechtigungen zugreifen, die ebenfalls nicht über Kennzeichen verfügen.
- Bei Verwendung eines Sicherheitsservers müssen Sie Einschränkungen für die Verbindungsserver-Instanz konfigurieren, mit der der Sicherheitsserver gekoppelt ist. Einschränkungen können nicht auf einem Sicherheitsserver konfiguriert werden.

- Einschränkungen für Verbindungsserver haben Vorrang vor anderen Berechtigungen bzw. Zuweisungen. Wenn z. B. ein Benutzer einem bestimmten Computer zugewiesen wurde, kann dieser nicht auf diesen Computer zugreifen, wenn das der globalen Berechtigung zugewiesene Kennzeichen nicht mit dem Kennzeichen übereinstimmt, das der Verbindungsserver-Instanz zugewiesen wurde, mit der der Benutzer verbunden ist.
- Wenn Sie den Zugriff auf Ihre globalen Berechtigungen über VMware Identity Manager ermöglichen möchten und Einschränkungen für Verbindungsserver konfigurieren, werden in der VMware Identity Manager-Anwendung möglicherweise globale Berechtigungen angezeigt, obwohl für diese globalen Berechtigungen Einschränkungen gelten. Wenn ein VMware Identity Manager-Benutzer versucht, eine Verbindung mit einer globalen Berechtigung herzustellen, wird der Desktop oder die Anwendung nicht gestartet, wenn das Kennzeichen, das der globalen Berechtigung zugewiesen wurde, nicht mit dem Kennzeichen übereinstimmt, das der Verbindungsserver-Instanz zugewiesen wurde, mit der der Benutzer verbunden ist.

Beispiel für Verbindungsserver-Einschränkungen

In diesem Beispiel wird eine Cloud-Pod-Architektur-Umgebung mit zwei Pods verwendet. Beide Pods enthalten zwei Verbindungsserver-Instanzen. Die erste Verbindungsserver-Instanz unterstützt interne Benutzer. Die zweite Verbindungsserver-Instanz ist mit einem Sicherheitsserver gekoppelt und unterstützt externe Benutzer.

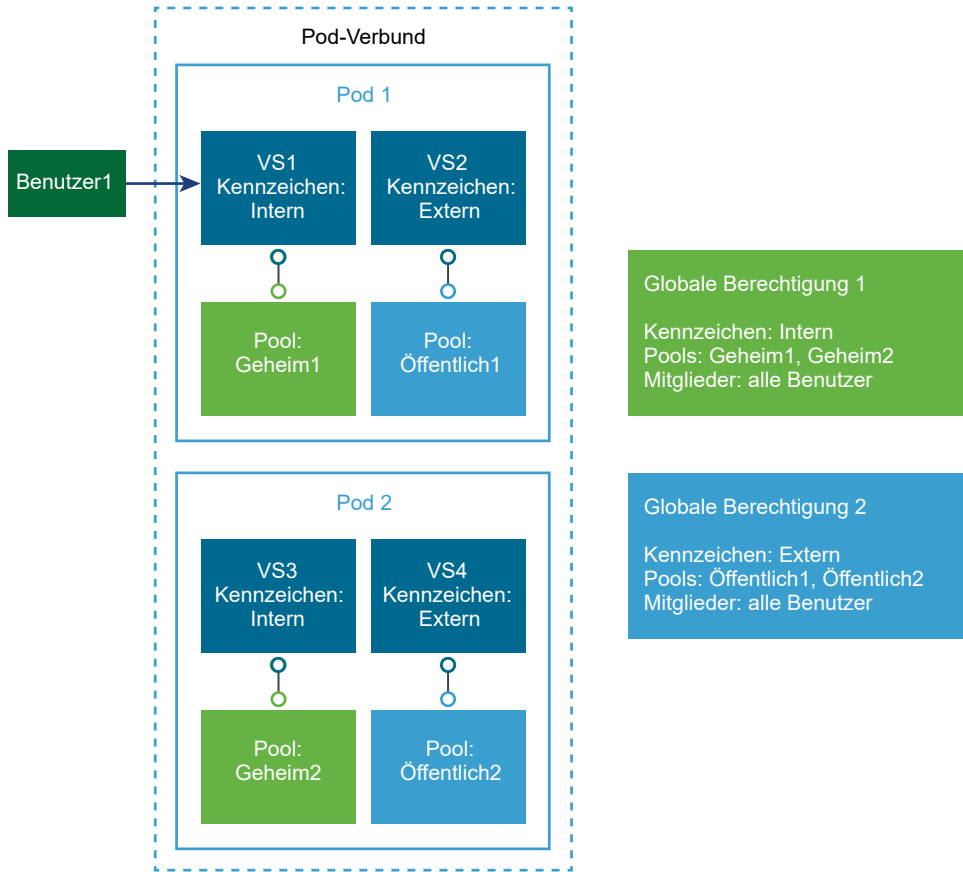
Damit externe Benutzer nicht auf bestimmte Desktop- und Anwendungspools zugreifen können, weisen Sie Kennzeichen wie folgt zu:

- Weisen Sie das Kennzeichen „Intern“ der Verbindungsserver-Instanz zu, die Ihre internen Benutzer unterstützt.
- Weisen Sie das Kennzeichen „Extern“ der Verbindungsserver-Instanz zu, die Ihre externen Benutzer unterstützt.
- Weisen Sie das Kennzeichen „Intern“ den globalen Berechtigungen zu, auf die nur interne Benutzer zugreifen dürfen.
- Weisen Sie das Kennzeichen „Extern“ den globalen Berechtigungen zu, auf die nur externe Benutzer zugreifen dürfen.

Externen Benutzern werden als „Intern“ gekennzeichnete globale Berechtigungen nicht angezeigt, da sie sich über Verbindungsserver-Instanzen anmelden, die als „Extern“ gekennzeichnet sind. Interne Benutzer haben keinen Zugang zu als „Extern“ gekennzeichneten globalen Berechtigungen, da sie sich über Verbindungsserver-Instanzen anmelden, die als „Intern“ gekennzeichnet sind.

Im nachfolgend dargestellten Diagramm stellt „Benutzer1“ eine Verbindung mit der Verbindungsserver-Instanz „VS1“ her. Da „VS1“ und auch „Globale Berechtigung 1“ als „Intern“ gekennzeichnet sind, wird für „Benutzer1“ nur „Globale Berechtigung 1“ angezeigt. Da „Globale Berechtigung 1“ die Pools „Geheim1“ und „Geheim2“ enthält, erhält „Benutzer1“ nur Desktops und Anwendungen aus den Pools „Geheim1“ und „Geheim2“.

Abbildung 2-2. Beispiel für Verbindungsserver-Einschränkungen



Implementieren von Clienteinschränkungen für globale Berechtigungen

Sie können den Zugriff auf globale Berechtigungen auf bestimmte Clientcomputer einschränken. Um den Zugriff einzuschränken, fügen Sie die Namen der Clientcomputer, die berechtigt sind, auf eine globale Berechtigung zuzugreifen, einer Active Directory-Sicherheitsgruppe und diese Gruppe dann den Benutzern und Gruppen der globalen Berechtigung hinzu.

Für die Funktion zur Clienteinschränkung gelten bestimmte Anforderungen und Beschränkungen.

- Sie müssen die Client-Einschränkungsrichtlinie aktivieren, wenn Sie die globale Berechtigung erstellen oder ändern. Standardmäßig ist die Client-Einschränkungsrichtlinie deaktiviert. Sie können diese Richtlinie nur für dynamische Desktop-Berechtigungen und globale Anwendungsberechtigungen aktivieren.
- Die Richtlinieeinstellung zur Einschränkung der globalen Berechtigung auf bestimmte Clients hat Vorrang vor der Richtlinieeinstellung zur Clienteinschränkung auf Poolebene. Als Best Practice wird empfohlen, bei der Aktivierung der Clienteinschränkungsrichtlinie für eine globale Berechtigung nicht die Clienteinschränkungsrichtlinie für die Pools zu aktivieren, die die globale Berechtigung enthalten.

- Sie müssen die Active Directory-Sicherheitsgruppe mit den Namen der Clientcomputer hinzufügen, die Zugriff auf die globale Berechtigung haben, wenn Sie die globale Berechtigung erstellen oder ändern.
- Die Clienteinschränkungsfunktion gestattet nur bestimmten Clientcomputern den Zugriff auf globale Berechtigungen. Sie gewährt keinen Benutzern den Zugriff auf globale Berechtigungen. Wenn beispielsweise ein Benutzer nicht in einer globalen Berechtigung (entweder als Benutzer oder als Mitglied einer Benutzergruppe) enthalten ist, kann der Benutzer nicht auf die globale Berechtigung zugreifen, auch wenn dem Clientcomputer des Benutzers der Zugriff auf die globale Berechtigung gestattet ist.
- Die Funktion zur Clienteinschränkung wird nur von Windows-Clientcomputern in dieser Version unterstützt. Horizon Client 4.6 für Windows oder höher muss auf den Clientcomputern installiert sein.
- Wenn die Client-Einschränkungsrichtlinie für eine globale Berechtigung aktiviert ist, können Nicht-Windows-Clients, Windows-Clients, auf denen Versionen von Horizon Client für Windows vor 4.6 ausgeführt werden, und HTML Access-Clients die globale Berechtigung nicht starten.

Implementieren der Funktion zum Vorabstart der Sitzung für globale Anwendungsberechtigungen

Mit der Funktion zum Vorabstart der Sitzung kann ein Horizon-Administrator eine veröffentlichte Anwendung so konfigurieren, dass die Sitzung gestartet wird, bevor ein Benutzer die Anwendung in Horizon Client öffnet. Die Funktion zum Vorabstart der Sitzung ermöglicht schnellere Startzeiten für häufig verwendete veröffentlichte Anwendungen.

Sie können die Funktion zum Vorabstart der Sitzung für eine globale Anwendungsberechtigung aktivieren, indem Sie die Richtlinie für den Vorabstart aktivieren, wenn Sie die globale Anwendungsberechtigung erstellen oder ändern. Alle Anwendungspools in der globalen Anwendungsberechtigung müssen die Funktion für den Vorabstart der Sitzung unterstützen, und die Zeitüberschreitung für die vorab gestartete Sitzung muss für alle Farmen identisch sein.

Informationen zum Konfigurieren von Anwendungspools und Farmen für die Nutzung der Funktion zum Vorabstart der Sitzung finden Sie im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

Die Funktion zum Vorabstart der Sitzung wird für Remotedesktops nicht unterstützt.

Aktivieren des Mehrfachsitzungsmodus für globale Anwendungsberechtigungen

Wenn Sie eine globale Anwendungsberechtigung erstellen, können Sie angeben, ob Benutzer mehrere Sitzungen derselben veröffentlichten Anwendung auf unterschiedlichen Clientgeräten ausführen können. Diese Funktion wird „Mehrfachsitzungsmodus“ genannt.

Wenn beispielsweise ein Benutzer eine veröffentlichte Anwendung im Mehrfach Sitzungsmodus auf Client A öffnet und dann dieselbe veröffentlichte Anwendung auf Client B öffnet, bleibt die veröffentlichte Anwendung auf Client A geöffnet und eine neue Sitzung der veröffentlichten Anwendung wird auf Client B geöffnet. Wenn der Benutzer hingegen die veröffentlichte Anwendung auf Client A im Einzelsitzungsmodus öffnet, wird die Sitzung auf Client A unterbrochen und auf Client B neu eingerichtet.

Wenn Sie den Mehrfach Sitzungsmodus aktivieren, können Sie angeben, ob er standardmäßig aktiviert, standardmäßig deaktiviert ist oder erzwungen ist.

- Wenn der Mehrfach Sitzungsmodus standardmäßig aktiviert oder deaktiviert ist, können Benutzer, die Horizon Client 4.10 oder höher besitzen, den Mehrfach Sitzungsmodus deaktivieren oder aktivieren, indem Sie die Einstellung **Mehrfachstart** auf dem Client ändern. Benutzer, die frühere Versionen von Horizon Client besitzen, können die Standardeinstellung nicht ändern.
- Wenn der Mehrfach Sitzungsmodus erzwungen wird, ist er immer aktiviert und Benutzer können ihn in Horizon Client nicht deaktivieren.

Weitere Informationen zur Verwendung der Einstellung **Mehrfachstart** finden Sie in der Dokumentation zu Horizon Client 4.10 oder höher.

Für die Funktion des Mehrfach Sitzungsmodus gelten die folgenden Anforderungen und Einschränkungen für globale Anwendungsberechtigungen.

- Die Einstellung des Mehrfach Sitzungsmodus, die Sie für die globale Anwendungsberechtigung konfigurieren, muss mit der Einstellung übereinstimmen, die für die Anwendungspools, die mit der globalen Anwendungsberechtigung verknüpft sind, konfiguriert ist. Informationen zum Aktivieren des Mehrfach Sitzungsmodus für Anwendungspools finden Sie im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.
- Sie können die Funktion für den Vorabstart der Sitzung für die globale Anwendungsberechtigung oder die Anwendungspools, die mit der globalen Anwendungsberechtigung verknüpft sind, bei aktiviertem Mehrfach Sitzungsmodus nicht aktivieren. Die Funktion für den Vorabstart der Sitzung wird nicht unterstützt, wenn der Mehrfach Sitzungsmodus aktiviert ist.

Aktivieren der Funktion „Session Collaboration“ für globale Desktopberechtigungen

Mit der Funktion „Session Collaboration“ können Endbenutzer andere Benutzer zur Teilnahme an einer vorhandenen Remote-Desktop-Sitzung einladen.

Um Remote-Desktop-Benutzern die Teilnahme an einer gemeinsamen Sitzung zu ermöglichen, muss der Horizon-Administrator die Funktion „Session Collaboration“ für den Desktop-Pool aktivieren, der den Remote-Desktop bereitstellt. Für RDS-Desktop-Pools muss ein Horizon-Administrator die Funktion „Session Collaboration“ für die Farm aktivieren, auf der der RDS-Desktop-Pool basiert.

Um eingeladenen Benutzern die Teilnahme an Sitzungen aus anderen Pods als dem Pod des Sitzungsbesitzers zu ermöglichen, müssen Sie die Richtlinie „Session Collaboration“ für die globale Desktopberechtigung aktivieren, die den Desktop-Pool enthält, wenn Sie die globale Desktopberechtigung erstellen oder ändern.

Eine vollständige Darstellung der Anforderungen und Einschränkungen einschließlich der Lizenzanforderungen für die Funktion „Session Collaboration“ finden Sie unter „Konfigurieren der Funktion „Session Collaboration““ im Dokument *Konfigurieren von Remote-Desktop-Funktionen in Horizon 7*.

Die Funktion „Session Collaboration“ wird für veröffentlichte Anwendungen nicht unterstützt.

Implementieren von globalen Sicherungsberechtigungen

Wenn Sie eine globale Desktop-Berechtigung oder globale Anwendungsberechtigung bearbeiten, können Sie eine globale Sicherungsberechtigung auswählen. Eine globale Sicherungsberechtigung stellt Remote-Desktops oder veröffentlichte Anwendungen bereit, wenn die primäre globale Berechtigung eine Sitzung aufgrund von Problemen wie unzureichender Poolkapazität oder nicht verfügbarer Pods nicht starten kann. Eine globale Sicherungsberechtigung kann Pools aus jedem Pod im Pod-Verbund enthalten.

Die folgenden Einstellungen einer globalen Sicherungsberechtigung müssen mit den Einstellungen der entsprechenden primären globalen Berechtigung übereinstimmen.

- Benutzerzuweisungstyp
- Standardanzeigeprotokoll (nur, wenn Benutzer das Anzeigeprotokoll nicht auswählen dürfen)
- Unterstützte Anzeigeprotokolle
- HTML Access
- Benutzern das Zurücksetzen/den Neustart ihrer Computer gestatten
- Benutzer dürfen separate Sitzungen von unterschiedlichen Clientgeräten aus starten
- Session Collaboration zulassen

Für globale Sicherungsberechtigungen gelten die folgenden Anforderungen und Einschränkungen.

- Für globale Desktop-Berechtigungen können Sie eine globale Sicherungsberechtigung nur dann konfigurieren, wenn für die Benutzerzuweisungsrichtlinie „Dynamisch“ festgelegt ist.
- Nachdem Sie eine globale Sicherungsberechtigung konfiguriert haben, sind die Bearbeitungsfunktion, Benutzerberechtigungen und die Einstellung für das Außerkraftsetzen der Start-Site der globalen Sicherungsberechtigung deaktiviert.
- Sie können keine vorhandene primäre oder globale Sicherungsberechtigung auswählen, wenn Sie eine globale Sicherungsberechtigung auswählen.
- Eine globale Sicherungsberechtigung kann nicht über die Cloud verwaltet werden.

- Eine globale Sicherungsberechtigung kann nicht mit Benutzer- oder Gruppenberechtigungen verknüpft werden.

Informationen zum Bearbeiten einer globalen Berechtigung finden Sie unter [Ändern von Attributen oder Richtlinien für eine globale Berechtigung in Horizon Console](#).

Überlegungen zu Umgebungen mit gemischten Versionen

Cloud-Pod-Architektur-Umgebungen mit gemischten Versionen werden ab Horizon 7 Version 7.4 unterstützt. Beispielsweise können in einem Pod-Verbund sowohl Pods enthalten sein, die Horizon 7 Version 7.4 ausführen, als auch Pods, die Horizon 6 Version 6.x ausführen.

Neue Funktionen können in einer gemischten Umgebung nicht verwendet werden. Beispielsweise ist eine neue Funktion, die in Horizon Administrator für eine Verbindungsserver-Instanz von Horizon 7 Version 7.4 sichtbar ist, in Horizon Administrator für eine Horizon 6 Version 6.x-Verbindungsserver-Instanz nicht sichtbar. Es wird von VMware empfohlen, alle Pods auf die gleiche Horizon 7-Version zu aktualisieren.

Grundlegendes zum Workspace ONE-Modus

Wenn ein Horizon-Administrator den Workspace ONE-Modus für eine Verbindungsserver-Instanz aktiviert, können Horizon Client-Benutzer zu einem Workspace ONE-Server weitergeleitet werden, um ihre Berechtigungen zu starten.

Bei der Konfiguration des Workspace ONE-Modus legt ein Horizon-Administrator den Hostnamen des Workspace ONE-Servers fest. In einer Cloud-Pod-Architektur-Umgebung muss jeder Pod im Pod-Verbund mit einem Verweis auf denselben Workspace ONE-Server konfiguriert werden.

Weitere Informationen zur Konfiguration des Workspace ONE-Modus finden Sie im Dokument *Horizon 7-Verwaltung*.

Überlegungen zu VMware Cloud on AWS

Sie können Horizon 7 in einer hybriden Cloudumgebung bereitstellen, wenn Sie Cloud-Pod-Architektur verwenden, um Horizon 7 lokal und Horizon 7-Pods auf VMware Cloud on AWS miteinander zu verbinden. Sie können Benutzern Berechtigungen für virtuelle Desktops und veröffentlichte Anwendungen lokal und auf VMware Cloud on AWS erteilen.

Weitere Informationen finden Sie unter „Planung der Horizon 7-Cloud-Pod-Architektur (CPA) für VMware Cloud on AWS“ im Dokument *Bereitstellungshandbuch für Horizon 7 auf VMware Cloud on AWS* unter <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vmw-deploy-horizon-seven-on-vmware-cloud-on-aws.pdf>.

Überlegungen für RDS-Clientzugriffslizenz auf Gerätebasis

Wenn ein Windows-Clientgerät eine Verbindung mit einem veröffentlichten Desktop oder einer veröffentlichten Anwendung auf einem RDS-Host herstellt, erhält es eine RDS-Clientzugriffslizenz

(Client Access License, CAL) auf Gerätebasis, wenn der gerätebasierte Lizenzierungsmodus auf dem RDS-Host konfiguriert ist. Standardmäßig wird die CAL nur auf dem Clientgerät gespeichert.

Ab Horizon Client für Windows 4.9 präsentiert das Clientgerät immer seine Lizenz, wenn es über eine Lizenz verfügt. Windows-Clients, die Horizon Client 4.8 oder früher verwenden, präsentieren eine Lizenz nur dann, wenn sie über eine Lizenz für den jeweiligen Pod verfügen. Wenn das Clientgerät keine Lizenz präsentiert, wird die aktuellste Lizenz verwendet, die in jedem Pod gefunden wird, der am Start eines veröffentlichten Desktops oder einer veröffentlichten Anwendung beteiligt ist. Wenn in keinem am Start beteiligten Pod eine Lizenz gefunden wird, wird die ID des Clientgeräts dem Lizenzserver präsentiert, und eine Lizenz wird ausgestellt.

Wichtig VMware empfiehlt ein Upgrade auf den neuesten Windows-Client und die neueste Serversoftware für die optimale Handhabung der RDS-Lizenzierung.

Weitere Informationen finden Sie unter „Informationen zu RDS-Clientzugriffslizenz auf Gerätebasis in Horizon 7“ im Dokument *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

Einschränkungen für Cloud-Pod-Architektur-Topologie

Eine typische Cloud-Pod-Architektur-Topologie besteht aus zwei oder mehr Pods, die in einem Pod-Verbund miteinander verknüpft sind.

In der folgenden Tabelle wird die Gesamtanzahl der Sitzungen gezeigt, die in der vorliegenden Version unterstützt werden.

Tabelle 2-2. Einschränkungen für einen Pod-Verbund

Objekt	Einschränkung
Sitzungen insgesamt	250.000
Pods	50
Sitzungen pro Pod	12.000
Sites	15
Verbindungsserver-Instanzen pro Pod	7
Verbindungsserver-Instanzen gesamt	350

Die Grenzwerte für Pods, Sites und Gesamtzahl der Verbindungsserver-Instanzen geben die maximal unterstützte Anzahl für die jeweilige Komponente im Pod-Verbund an. Solange die Konfiguration innerhalb der angegebenen Grenzwerte verbleibt, können Sie eine geeignete Topologie entwerfen, um die Gesamtanzahl der Sitzungen zu erreichen.

Anforderungen an den Cloud-Pod-Architektur-Port

Bestimmte Netzwerkports müssen in der Windows-Firewall geöffnet sein, damit die Funktion Cloud-Pod-Architektur verwendet werden kann. Wenn Sie den Verbindungsserver installieren, kann das Installationsprogramm optional die erforderlichen Firewallregeln für Sie konfigurieren.

Mit diesen Regeln werden die standardmäßig verwendeten Ports geöffnet. Wenn Sie die Standardports nach der Installation ändern oder das Netzwerk andere Firewalls verwendet, müssen Sie die Windows-Firewall manuell konfigurieren.

Tabelle 2-3. Ports, die während der Verbindungsserver-Installation geöffnet werden

Protokoll	TCP-Port	Beschreibung
HTTP	22389	Wird für die Replizierung der LDAP-Instanz der globalen Datenschicht verwendet. Gemeinsame Daten werden auf jeder Verbindungsserver-Instanz in einem Pod-Verbund repliziert. Jede Verbindungsserver-Instanz in einem Pod-Verbund führt eine zweite LDAP-Instanz zum Speichern von gemeinsamen Daten aus.
HTTPS	22636	Wird für die sichere Replizierung der LDAP-Instanz der globalen Datenschicht verwendet.
HTTPS	8472	Wird für die View Interpod API (VIPA-)Kommunikation verwendet. Verbindungsserver-Instanzen verwenden den VIPA-Kommunikationskanal, um neue Desktops und Anwendungen zu starten, vorhandene Desktops zu suchen und Integritätsstatusdaten sowie andere Informationen freizugeben.

Hinweis Für Microsoft Windows Server ist es erforderlich, dass ein dynamischer Portbereich zwischen allen Verbindungsserver-Instanzen geöffnet sein muss. Microsoft Windows benötigt diese Ports für die herkömmliche Ausführung des Remoteprozeduraufrufs (Remote Procedure Call, RPC) und der Active Directory-Replizierung. Weitere Informationen zum dynamischen Portbereich finden Sie in der Microsoft Windows Server-Dokumentation.

Sicherheitsüberlegungen für Cloud-Pod-Architektur-Topologien

Um Horizon Console oder den `lmvutil`-Befehl zum Konfigurieren und Verwalten einer Cloud-Pod-Architektur-Umgebung verwenden zu können, müssen Sie über die Administratorrolle verfügen. Administratoren mit der Administratorenrolle für die Stammzugriffsgruppe sind übergeordnete Benutzer.

Wenn eine Verbindungsserver-Instanz Teil einer replizierten Gruppe von Verbindungsserver-Instanzen ist, werden die Rechte von übergeordneten Benutzern auf andere Verbindungsserver-Instanzen im Pod ausgeweitet. Gleichermaßen werden, wenn ein Pod einem Pod-Verbund beitrifft, die Rechte von übergeordneten Benutzern auf alle Verbindungsserver-Instanzen in allen Pods im Pod-Verbund ausgeweitet. Diese Rechte sind notwendig, um globale Berechtigungen zu ändern und andere Vorgänge auf der globalen Datenschicht durchzuführen.

Wenn Sie nicht möchten, dass bestimmte übergeordnete Benutzer Vorgänge auf der globalen Datenschicht ausführen können, können Sie die Administratorenrollenzuweisung aufheben und stattdessen die lokale Administratorenrolle zuweisen. Benutzer mit der lokalen Administratorrolle haben die Rechte von übergeordneten Benutzern nur für ihre lokale Verbindungsserver-Instanz und für alle Instanzen in einer replizierten Gruppe.

Informationen zum Zuweisen von Rollen finden Sie im Dokument *Horizon 7-Verwaltung*.

Einrichten von Cloud-Pod-Architektur in Horizon Console

3

Die Einrichtung einer Cloud-Pod-Architektur-Umgebung umfasst das Initialisieren der Funktion Cloud-Pod-Architektur, das Hinzufügen von Pods zum Pod-Verbund und das Erstellen globaler Berechtigungen.

Sie müssen mindestens eine globale Berechtigung erstellen und konfigurieren, um die Funktion Cloud-Pod-Architektur zu verwenden. Optional können Sie Sites erstellen und Start-Sites zuweisen.

In diesem Kapitel wird erläutert, wie Sie eine Horizon Console-Umgebung in Cloud-Pod-Architektur einrichten. Weitere Informationen zur Verwendung der `lmvutil`-Befehlszeilenschnittstelle finden Sie unter [Kapitel 5 Verwalten der Cloud-Pod-Architektur mit `lmvutil`](#).

Dieses Kapitel enthält die folgenden Themen:

- [Initialisieren der Cloud-Pod-Architektur-Funktion in Horizon Console](#)
- [Hinzufügen eines Pods zu einem Pod-Verbund in Horizon Console](#)
- [Zuweisen eines Tags zu einer Verbindungsserver-Instanz in Horizon Console](#)
- [Konfigurieren von Verknüpfungen für globale Berechtigungen](#)
- [Arbeitsblatt zur Konfiguration einer globalen Berechtigung](#)
- [Erstellen und Konfigurieren einer globalen Berechtigung in Horizon Console](#)
- [Hinzufügen eines Pools zu einer globalen Berechtigung in Horizon Console](#)
- [Erstellen und Konfigurieren einer Site in Horizon Console](#)
- [Zuweisen einer Start-Site zu einem Benutzer oder einer Gruppe in Horizon Console](#)
- [Erstellen einer Außerkraftsetzung der Start-Site in Horizon Console](#)
- [Testen einer Cloud-Pod-Architektur-Konfiguration in Horizon Client](#)
- [Beispiel: Einrichten einer Cloud-Pod-Architektur-Basiskonfiguration](#)

Initialisieren der Cloud-Pod-Architektur-Funktion in Horizon Console

Bevor Sie eine Cloud-Pod-Architektur-Umgebung konfigurieren, müssen Sie die Funktion Cloud-Pod-Architektur initialisieren.

Sie brauchen die Funktion Cloud-Pod-Architektur nur einmal zu initialisieren, und zwar im ersten Pod in einem Pod-Verbund. Um dem Pod-Verbund weitere Pods hinzuzufügen, fügen Sie die neuen Pods zum initialisierten Pod hinzu.

Während der Initialisierung richtet Horizon die globale Datenschicht auf jeder Verbindungsserver-Instanz im Pod ein, konfiguriert den VIPA-Kommunikationskanal und stellt eine Replikationsvereinbarung zwischen jeder Verbindungsserver-Instanz her.

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod an.
- 2 Wählen Sie **Einstellungen > Cloud-Pod-Architektur**, klicken Sie auf **Cloud-Pod-Architektur-Funktion initialisieren** und klicken Sie auf **OK**, um den Initialisierungsvorgang zu starten.

In Horizon Console wird der Fortschritt des Initialisierungsvorgangs angezeigt. Nach der Initialisierung der Funktion Cloud-Pod-Architektur enthält der Pod-Verbund den initialisierten Pod und eine einzelne Site. Der Standardname für den Pod-Verbund ist „Horizon-Cloud-Pod-Verbund“. Der Standard-Pod-Name basiert auf dem Hostnamen der Verbindungsserver-Instanz. Wenn der Hostname beispielsweise „CS1“ lautet, erhält der Pod den Namen „Cluster-CS1“. Der Standard-Site-Name ist „Erste Standard-Site“.
- 3 (Optional) Um den Standardnamen des Pod-Verbunds zu ändern, klicken Sie auf **Bearbeiten**, geben Sie den neuen Namen in das Textfeld **Name** ein und klicken Sie auf **OK**.
- 4 (Optional) Um den Standardnamen des Pods zu ändern, wählen Sie **Einstellungen > Sites** aus, wählen Sie den Pod aus, klicken Sie auf **Bearbeiten**, geben Sie den neuen Namen in das Textfeld **Name** ein und klicken Sie auf **OK**.
- 5 (Optional) Um den Standardnamen der Site zu ändern, wählen Sie **Einstellungen > Sites** aus, wählen Sie die Site aus, klicken Sie auf **Bearbeiten**, geben Sie den neuen Namen in das Textfeld **Name** ein und klicken Sie auf **OK**.

Nächste Schritte

Unter [Hinzufügen eines Pods zu einem Pod-Verbund in Horizon Console](#) wird beschrieben, wie Sie dem Pod-Verbund weitere Pods hinzufügen.

Hinzufügen eines Pods zu einem Pod-Verbund in Horizon Console

Während des Cloud-Pod-Architektur-Initialisierungsvorgangs erstellt die Funktion Cloud-Pod-Architektur einen Pod-Verbund, der einen einzelnen Pod enthält. Sie können dem Pod-Verbund

mithilfe von Horizon Console weitere Pods hinzufügen. Das Hinzufügen zusätzlicher Pods ist optional.

Wichtig Stoppen oder starten Sie keine Verbindungsserver-Instanz, während Sie sie einem Pod-Verbund hinzufügen. Andernfalls kann der Verbindungsserver-Dienst möglicherweise nicht richtig neu gestartet werden. Sie können den Verbindungsserver stoppen und starten, nachdem er erfolgreich dem Pod-Verbund hinzugefügt wurde.

Voraussetzungen

- Stellen Sie sicher, dass die Verbindungsserver-Instanzen, die Sie hinzufügen möchten, unterschiedliche Hostnamen aufweisen. Sie können Server mit demselben Namen nicht hinzufügen, selbst wenn sie sich in verschiedenen Domänen befinden.
- Initialisieren Sie die Funktion Cloud-Pod-Architektur. Siehe [Initialisieren der Cloud-Pod-Architektur-Funktion in Horizon Console](#).

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für einen Verbindungsserver in dem Pod an, den Sie dem Pod-Verbund hinzufügen.
- 2 Wählen Sie **Einstellungen > Cloud-Pod-Architektur** aus und klicken Sie auf **Pod-Verbund beitreten**.
- 3 Geben Sie in das Textfeld **Verbindungsserver (Hostname oder IP-Adresse)** den Hostnamen oder die IP-Adresse einer beliebigen Verbindungsserver-Instanz in einem beliebigen initialisierten oder bereits zum Pod-Verbund hinzugefügten Pod ein.
- 4 Geben Sie in das Textfeld **Benutzername (Domäne/Benutzername)** den Namen eines Horizon-Administratorbenutzers im bereits initialisierten Pod ein.
Verwenden Sie das Format *Domäne\Benutzername*.
- 5 Geben Sie in das Feld **Kennwort** das Kennwort für den Horizon-Administratorbenutzer ein.
- 6 Um den Pod zum Pod-Verbund hinzuzufügen, klicken Sie auf **OK**.

In Horizon Console wird der Fortschritt des Vorgangs angezeigt. Der Standard-Pod-Name basiert auf dem Hostnamen der Verbindungsserver-Instanz. Wenn der Hostname beispielsweise „CS1“ lautet, erhält der Pod den Namen „Cluster-CS1“.

Ergebnisse

Sobald der Pod zum Pod-Verbund hinzugefügt wurde, beginnt er, Daten zum Systemzustand freizugeben. Sie können diese Zustandsdaten auf dem Dashboard in Horizon Console anzeigen. Siehe [Anzeigen des Zustands des Pod-Verbunds in Horizon Console](#).

Hinweis Die Zustandsdaten sind möglicherweise erst nach einer kurzen Verzögerung in Horizon Console verfügbar.

Nächste Schritte

Wiederholen Sie diese Schritte, um dem Pod-Verbund weitere Pods hinzuzufügen.

Zuweisen eines Tags zu einer Verbindungsserver-Instanz in Horizon Console

Wenn Sie den Zugriff auf eine globale Berechtigung basierend auf der Verbindungsserver-Instanz, mit der Benutzer bei der Auswahl der globalen Berechtigung anfänglich eine Verbindung hergestellt haben, beschränken möchten, müssen Sie der Verbindungsserver-Instanz zuerst ein oder mehrere Kennzeichen zuweisen.

Voraussetzungen

Machen Sie sich mit der Verbindungsserver-Einschränkungsfunktion vertraut. Siehe [Implementieren von Clienteinschränkungen für globale Berechtigungen](#).

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für die Verbindungsserver-Instanz an.
- 2 Wählen Sie **Einstellungen > Server** aus.
- 3 Klicken Sie auf die Registerkarte **Verbindungsserver**, wählen Sie die Verbindungsserver-Instanz aus und klicken Sie auf **Bearbeiten**.
- 4 Geben Sie im Textfeld **Kennzeichen** mindestens ein Kennzeichen ein.
Trennen Sie mehrere Kennzeichen durch ein Komma oder Semikolon.
- 5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.
- 6 Wiederholen Sie diese Schritte für jede Verbindungsserver-Instanz, der Sie Kennzeichen zuweisen möchten.

Nächste Schritte

Beim Erstellen oder Bearbeiten einer globalen Berechtigung wählen Sie die Kennzeichen aus, die mit den Verbindungsserver-Instanzen verknüpft sind, die auf die globale Berechtigung zugreifen sollen. Siehe [Erstellen und Konfigurieren einer globalen Berechtigung in Horizon Console](#) oder [Ändern von Attributen oder Richtlinien für eine globale Berechtigung in Horizon Console](#).

Konfigurieren von Verknüpfungen für globale Berechtigungen

Sie können Verknüpfungen für globale Berechtigungen konfigurieren. Wenn ein berechtigter Benutzer eine Verbindung zu einer Verbindungsserver-Instanz im Pod-Verbund von einem Windows-Client herstellt, platziert Horizon Client für Windows diese Verknüpfungen im Windows-Startmenü bzw. auf dem Desktop des Clientgeräts des Benutzers oder an beiden Positionen. Sie

können eine Verknüpfung konfigurieren, wenn Sie eine globale Berechtigung erstellen oder ändern.

Während der Konfiguration einer Verknüpfung müssen Sie einen Kategorienordner oder den Stammordner (/) auswählen. Sie können eigene Kategorienordner hinzufügen und benennen. Sie können bis zu vier Ordnebenen konfigurieren. Sie können z. B. einen Kategorienordner mit dem Namen Office hinzufügen und diesen Ordner für alle geschäftlichen Anwendungen wie z. B. Microsoft Office und Microsoft PowerPoint auswählen.

Für Startmenüverknüpfungen: Auf Windows 7-Clientgeräten platziert Horizon Client Kategorienordner und Verknüpfungen im Ordner „VMware-Anwendungen“ des Startmenüs. Wenn Sie den Stammordner (/) für eine Verknüpfung auswählen, platziert Horizon Client die Verknüpfung direkt im Ordner „VMware-Anwendungen“. Auf Windows 8- und Windows 10-Clientgeräten platziert Horizon Client Kategorienordner und Verknüpfungen in der Liste der Anwendungen. Wenn Sie den Stammordner (/) für eine Verknüpfung auswählen, platziert Horizon Client die Verknüpfung direkt in der Liste der Anwendungen.

Wenn auf Mac-Clients Horizon Client für Mac konfiguriert ist, um veröffentlichte Anwendungen aus dem Ordner Anwendungen auszuführen und automatische Verknüpfungen vom Server aus zuzulassen, werden Kategorienordner für globale Anwendungsberechtigungen im Ordner Anwendungen auf dem Mac-Client angezeigt.

Nachdem Sie eine Verknüpfung erstellt haben, wird ein Häkchen in der Spalte „App-Verknüpfung“ für die globale Berechtigung auf der Seite „Globale Berechtigungen“ in Horizon Console angezeigt.

Standardmäßig fordert Horizon Client für Windows berechtigte Benutzer zur Installation von Verknüpfungen auf, wenn diese das erste Mal eine Verbindung zu einem Server herstellen. Sie können Horizon Client für Windows so konfigurieren, dass Verknüpfungen automatisch oder niemals erstellt werden, indem Sie die Gruppenrichtlinieneinstellung **Verknüpfungen automatisch installieren, wenn diese auf Horizon Server konfiguriert wurden** ändern. Weitere Informationen finden Sie im Dokument *VMware Horizon Client für Windows Installations- und Einrichtungshandbuch*.

Standardmäßig werden Änderungen, die Sie an den Verknüpfungen vornehmen, jedes Mal auf dem Windows-Clientgerät eines Benutzers synchronisiert, wenn der Benutzer eine Verbindung zum Server herstellt. Benutzer können die Funktion zur Synchronisierung von Verknüpfungen in Horizon Client für Windows deaktivieren. Weitere Informationen finden Sie im Dokument *VMware Horizon Client für Windows Installations- und Einrichtungshandbuch*.

Bei Windows-Benutzern muss für diese Funktion auf dem Clientsystem Horizon Client 4.6 für Windows oder höher installiert sein. Bei Mac-Benutzern muss für diese Funktion auf dem Clientsystem Horizon Client für Mac 4.10 oder höher installiert sein.

Arbeitsblatt zur Konfiguration einer globalen Berechtigung

Bei der Erstellung einer globalen Berechtigung in Horizon Console werden Sie von der Benutzeroberfläche aufgefordert, bestimmte Optionen zu konfigurieren. Mithilfe dieses

Arbeitsblatts können Sie Ihre Konfigurationsoptionen vorbereiten, bevor Sie die globale Berechtigung erstellen.

Sie können dieses Arbeitsblatt drucken und die Werte notieren, die Sie beim Hinzufügen einer globalen Berechtigung angeben möchten.

Tabelle 3-1. Arbeitsblatt: Optionen zum Konfigurieren einer globalen Berechtigung

Option	Beschreibung	Wert
Name	Der Name der globalen Berechtigung. Der Name erscheint in der Liste der verfügbaren Desktops und Anwendungen in Horizon Client. Der Name kann zwischen 1 und 64 Zeichen enthalten.	
Beschreibung	(Optional) Eine Beschreibung der globalen Berechtigung. Die Beschreibung kann 1 bis 1024 Zeichen enthalten.	
Einschränkungen für Verbindungsserver	(Optional) Ordnet Verbindungsserver-Tags die globale Berechtigung zu, um den Zugriff auf die globale Berechtigung von bestimmten Verbindungsserver-Instanzen aus zu beschränken. Hinweis Sie können nur Tags auswählen, die Verbindungsserver-Instanzen im lokalen Pod zugewiesen sind. Um Tags auszuwählen, die Verbindungsserver-Instanzen in einem anderen Pod zugewiesen wurden, müssen Sie sich bei einer Verbindungsserver-Instanz in dem anderen Pod anmelden und die globale Berechtigung ändern. Weitere Informationen finden Sie unter Implementieren von Verbindungsserver-Einschränkungen für globale Berechtigungen .	
Kategorienordner	(Optional) Erstellt eine Verknüpfung für die globale Berechtigung. Sie haben die Möglichkeit, einen vorhandenen Kategorienordner auszuwählen oder einen Kategorienordner zu erstellen. Sie können bis zu vier Unterordner konfigurieren. Sie können eine Verknüpfung mit dem Windows-Startmenü, eine Desktop-Verknüpfung oder beides konfigurieren. Ein Ordnername darf bis zu 64 Zeichen enthalten. Geben Sie einen umgekehrten Schrägstrich (\) ein, z. B. dir1\dir2\dir3\dir4, um einen Unterordner anzugeben. Sie können bis zu vier Ordnerstufen eingeben. Sie können einen Ordnernamen nicht mit einem umgekehrten Schrägstrich beginnen oder beenden und auch nicht zwei oder mehr umgekehrte Schrägstriche kombinieren. Beispielsweise sind \dir1, dir1\dir2\, dir1\dir2 und dir1\\dir2 ungültig. Sie können keine für Windows reservierten Schlüsselwörter eingeben. Weitere Informationen finden Sie unter Konfigurieren von Verknüpfungen für globale Berechtigungen .	

Tabelle 3-1. Arbeitsblatt: Optionen zum Konfigurieren einer globalen Berechtigung (Fortsetzung)

Option	Beschreibung	Wert
Globale Sicherungsberechtigung	<p>(Nur verfügbar, wenn Sie eine globale Berechtigung bearbeiten) Eine globale Sicherungsberechtigung stellt Remote-Desktops oder veröffentlichte Anwendungen bereit, wenn mit der primären globalen Berechtigung keine Sitzung gestartet werden kann. Informationen zu den Anforderungen und Einschränkungen finden Sie unter Implementieren von globalen Sicherungsberechtigungen.</p>	
Benutzerzuweisung	<p>(Nur globale Desktop-Berechtigung) Gibt den Desktop-Pool-Typ an, den die globale Berechtigung enthalten kann. Sie können eine der folgenden Benutzerzuweisungsrichtlinien konfigurieren:</p> <ul style="list-style-type: none"> ■ Dynamisch – die globale Berechtigung enthält nur dynamische Desktop-Pools. ■ Dediziert – die globale Berechtigung enthält nur dedizierte Desktop-Pools. 	
Geltungsbereich	<p>Gibt an, wo nach Desktops oder Anwendungen gesucht werden soll, um eine Anfrage von der globalen Berechtigung zu erfüllen. Sie können eine der folgenden Bereichsrichtlinien konfigurieren:</p> <ul style="list-style-type: none"> ■ Alle Sites – Sucht nach Desktops oder Anwendungen in beliebigen Pods im Pod-Verbund. ■ Innerhalb der Site – Sucht nach Desktops oder Anwendungen nur in Pods innerhalb der Site des Pods, mit dem der Benutzer verbunden ist. ■ Innerhalb des Pods – Sucht nach Desktops oder Anwendungen nur in dem Pod, mit dem der Benutzer verbunden ist. <p>Weitere Informationen finden Sie unter Grundlegendes zur Geltungsbereichsrichtlinie.</p>	
Start-Site verwenden und Berechtigter Benutzer benötigt Start-Site	<p>(Optional) Wenn Benutzer über Start-Sites verfügen, konfigurieren Sie eine Richtlinie für die Start-Site für die globale Berechtigung. Sie können die folgenden Richtlinien für die Start-Site konfigurieren:</p> <ul style="list-style-type: none"> ■ Start-Site verwenden – es wird eine Suche nach Desktops oder Anwendungen in der Start-Site des Benutzers gestartet. Wenn der Benutzer nicht über eine Start-Site verfügt und die Option Berechtigter Benutzer benötigt Start-Site nicht ausgewählt ist, wird angenommen, dass die Site, zu der der Benutzer die Verbindung hergestellt hat, die Start-Site ist. ■ Berechtigter Benutzer benötigt Start-Site – die globale Berechtigung wird nur dann zur Verfügung gestellt, wenn der Benutzer eine Start-Site hat. Diese Option ist nur verfügbar, wenn die Option Start-Site verwenden ausgewählt ist. <p>Weitere Informationen finden Sie unter Verwenden von Start-Sites.</p>	

Tabelle 3-1. Arbeitsblatt: Optionen zum Konfigurieren einer globalen Berechtigung (Fortsetzung)

Option	Beschreibung	Wert
Redundante Sitzungen automatisch bereinigen	<p>(Optional) Gibt an, ob redundante Sitzungen bereinigt werden sollen.</p> <p>Mehrere Sitzungen sind möglich, wenn ein Pod, der eine Sitzung enthält, offline geschaltet wird, der Benutzer sich erneut anmeldet und eine andere Sitzung startet und der problematische Pod wieder mit der ursprünglichen Sitzung online geschaltet wird. Wenn mehrere Sitzungen vorhanden sind, fordert Horizon Client den Benutzer auf, eine Sitzung auszuwählen. Diese Option legt fest, was mit Sitzungen passiert, die der Benutzer nicht auswählt. Wenn Sie diese Option nicht auswählen, müssen Benutzer ihre eigenen zusätzlichen Sitzungen manuell beenden, indem sie sich entweder in Horizon Client abmelden oder indem sie die Sitzungen starten und diese abmelden.</p>	
Standardanzeigeprotokoll	Gibt ein Standardanzeigeprotokoll für Desktops oder Anwendungen in der globalen Berechtigung an. Sie können PCoIP oder VMware Blast konfigurieren.	
Benutzern die Wahl des Protokolls erlauben	Wenn Sie diese Richtlinie aktivieren, können Benutzer das Standardanzeigeprotokoll außer Kraft setzen.	
Benutzern das Zurücksetzen/den Neustart ihrer Computer gestatten	(Nur globale Desktop-Berechtigung) Wenn Sie diese Richtlinie aktivieren, können Benutzer Desktops in der globalen Desktop-Berechtigung zurücksetzen und neu starten.	
HTML Access	<p>Wenn Sie diese Richtlinie aktivieren, können Endbenutzer mithilfe eines Webbrowsers eine Verbindung mit Remote-Desktops und -Anwendungen herstellen und müssen keine Clientsoftware auf ihren lokalen Systemen installieren.</p> <p>Weitere Informationen finden Sie im Dokument <i>VMware Horizon HTML Access Benutzerhandbuch</i>.</p>	
Vorabstart	<p>(Nur globale Anwendungsberechtigung) Wenn Sie diese Richtlinie aktivieren, können Benutzer die globale Anwendungsberechtigung schneller starten.</p> <p>Hinweis Wenn Sie diese Richtlinie aktivieren, müssen alle Anwendungspools in der globalen Anwendungsberechtigung die Funktion für den Vorabstart der Sitzung unterstützen, und die Zeitüberschreitung für die vorab gestartete Sitzung muss für alle Farmen identisch sein.</p>	

Tabelle 3-1. Arbeitsblatt: Optionen zum Konfigurieren einer globalen Berechtigung (Fortsetzung)

Option	Beschreibung	Wert
Session Collaboration zulassen	<p>Wenn Sie diese Richtlinie aktivieren, können Benutzer andere Benutzer zur Teilnahme an ihren Remote-Desktop-Sitzungen einladen.</p> <hr/> <p>Hinweis Wenn Sie diese Richtlinie aktivieren, müssen alle Desktop-Pools in der globalen Desktop-Berechtigung ebenfalls die Funktion „Session Collaboration“ unterstützen. Für RDS-Desktop-Pools wird die Funktion „Session Collaboration“ auf Farmebene aktiviert.</p> <hr/> <p>Weitere Informationen finden Sie unter Aktivieren der Funktion „Session Collaboration“ für globale Desktopberechtigungen.</p>	
Benutzer darf separate Sitzungen von unterschiedlichen Client-Geräten aus starten	<p>(Nur globale Desktop-Berechtigung) Wenn Sie diese Richtlinie aktivieren, werden Benutzer, die eine Verbindung mit der globalen Berechtigung von unterschiedlichen Clientgeräten aus herstellen, mit unterschiedlichen Desktop-Sitzungen verbunden. Um erneut eine Verbindung mit einer vorhandenen Desktop-Sitzung herzustellen, müssen Benutzer das Gerät verwenden, von dem aus die Sitzung initiiert wurde. Wenn Sie diese Richtlinie nicht aktivieren, werden Benutzer immer erneut mit ihren vorhandenen Desktop-Sitzungen verbunden, unabhängig vom verwendeten Clientgerät. Sie können diese Richtlinie nur für dynamische Desktop-Berechtigungen aktivieren.</p> <hr/> <p>Hinweis Wenn Sie diese Richtlinie aktivieren, müssen alle Desktop-Pools in der globalen Berechtigung auch mehrere Sitzungen pro Benutzer unterstützen.</p> <hr/> <p>Weitere Informationen finden Sie unter Grundlegendes zur Richtlinie für mehrere Sitzungen pro Benutzer für globale Desktop-Berechtigungen.</p>	
Clienteinschränkungen	<p>Wenn Sie diese Richtlinie aktivieren, ist der Zugriff auf die globale Berechtigung auf bestimmte Clientcomputer beschränkt. Sie können diese Richtlinie nur für dynamische Desktop-Berechtigungen und globale Anwendungsberechtigungen aktivieren.</p> <p>Sie müssen die Namen der Computer, die berechtigt sind, auf die globale Berechtigung zuzugreifen, einer Active Directory-Sicherheitsgruppe hinzufügen. Sie können diese Sicherheitsgruppe auswählen, wenn Sie Benutzer oder Gruppen zur globalen Berechtigung hinzufügen.</p> <p>Weitere Informationen finden Sie unter Implementieren von Clienteinschränkungen für globale Berechtigungen.</p>	

Tabelle 3-1. Arbeitsblatt: Optionen zum Konfigurieren einer globalen Berechtigung (Fortsetzung)

Option	Beschreibung	Wert
Mehrfachsitzungsmodus	<p>(Nur globale Anwendungsberechtigung) Verwenden Sie diese Richtlinie, um die Funktion für den Mehrfachsitzungsmodus für eine globale Anwendungsberechtigung zu konfigurieren. Folgende Werte sind gültig.</p> <ul style="list-style-type: none"> ■ Deaktiviert – Mehrfachsitzungsmodus wird nicht unterstützt. ■ Aktiviert (standardmäßig deaktiviert) – Mehrfachsitzungsmodus wird unterstützt, ist jedoch standardmäßig deaktiviert. Um den Mehrfachsitzungsmodus zu verwenden, müssen Benutzer die Einstellung Mehrfachstart in Horizon Client 4.10 oder höher aktivieren. Bei Benutzern mit einer früheren Version von Horizon Client wird die Anwendung immer im Einzelsitzungsmodus gestartet. ■ Aktiviert (standardmäßig aktiviert) – Mehrfachsitzungsmodus wird unterstützt und ist standardmäßig aktiviert. Benutzer können den Mehrfachsitzungsmodus deaktivieren, indem sie die Einstellung Mehrfachstart in Horizon Client 4.10 oder höher deaktivieren. Bei Benutzern mit einer früheren Version von Horizon Client wird die Anwendung immer im Einzelsitzungsmodus gestartet. ■ Aktiviert (erzwungen) – Mehrfachsitzungsmodus wird unterstützt, und die Anwendung wird immer im Mehrfachsitzungsmodus gestartet. Benutzer können den Mehrfachsitzungsmodus nicht deaktivieren, indem sie die Einstellung Mehrfachstart in Horizon Client 4.10 oder höher deaktivieren. Benutzer mit einer früheren Version von Horizon Client erhalten eine Fehlermeldung, die besagt, dass der angeforderte Startmodus nicht unterstützt wird. <p>Weitere Informationen finden Sie unter Aktivieren des Mehrfachsitzungsmodus für globale Anwendungsberechtigungen.</p>	
Name des zugewiesenen Computers anzeigen	<p>(Nur globale Desktop-Berechtigung) Zeigt den Hostnamen des zugewiesenen Computers anstelle des Namen der globalen Berechtigung an, wenn sich ein Benutzer bei Horizon Client anmeldet.</p>	

Tabelle 3-1. Arbeitsblatt: Optionen zum Konfigurieren einer globalen Berechtigung (Fortsetzung)

Option	Beschreibung	Wert
	Wenn dem Benutzer kein Computer zugewiesen ist, wird für die globale Berechtigung „Berechtigungsname (kein Computer zugewiesen)“ angezeigt, wenn sich der Benutzer bei Horizon Client anmeldet.	
	Hinweis Wenn der Pod, der den Computer enthält, nicht verfügbar ist oder nicht rechtzeitig antwortet, kann der Verbindungsserver den Namen des zugewiesenen Computers nicht abrufen. In solchen Fällen wird anstelle des Namens der globalen Berechtigung „Berechtigungsname (Name des Computers konnte nicht abgerufen werden)“ angezeigt, wenn sich der Benutzer bei Horizon Client anmeldet.	
	Diese Option ist nur verfügbar, wenn Sie unter Benutzerzuweisung Dediziert ausgewählt haben.	

Erstellen und Konfigurieren einer globalen Berechtigung in Horizon Console

Sie können mit Horizon Console globale Berechtigungen erstellen und konfigurieren. Globale Berechtigungen erteilen Benutzern und Gruppen Berechtigungen für Desktops und Anwendungen in einer Cloud-Pod-Architektur-Umgebung. Globale Berechtigungen ermöglichen die Verbindung zwischen Benutzern und ihren Desktops bzw. Anwendungen, unabhängig davon, wo sich diese Desktops und Anwendungen im Pod-Verbund befinden.

Eine globale Berechtigung enthält eine Liste der dazugehörigen Benutzer oder Gruppen, eine Reihe von Richtlinien und eine Liste der Pools, die Desktops oder Anwendungen für berechtigte Benutzer bereitstellen können. Sie können einer globalen Berechtigung Benutzer und Gruppen, nur Benutzer oder nur Gruppen hinzufügen.

Voraussetzungen

- Initialisieren Sie die Funktion Cloud-Pod-Architektur. Siehe [Initialisieren der Cloud-Pod-Architektur-Funktion in Horizon Console](#).
- Legen Sie fest, welche Art von globaler Desktop-Berechtigung Sie erstellen möchten und welche Benutzer und Gruppen in der globalen Berechtigung enthalten sein sollen. Siehe [Berechtigung erteilen für Benutzer und Gruppen im Pod-Verbund](#).
- Legen Sie fest, welche Optionen Sie für die globale Berechtigung konfigurieren möchten. Siehe [Arbeitsblatt zur Konfiguration einer globalen Berechtigung](#).

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Wählen Sie **Bestandsliste > Globale Berechtigungen** aus und klicken Sie auf **Hinzufügen**.

- 3 Wählen Sie die Art der globalen Berechtigung aus, die Sie hinzufügen möchten.

Option	Beschreibung
Desktop Entitlement (Desktop-Berechtigung)	Fügt eine globale Desktop-Berechtigung hinzu.
Application Entitlement (Anwendungsberechtigung)	Fügt eine globale Anwendungsberechtigung hinzu.

- 4 Klicken Sie auf **Weiter** und folgen Sie den Eingabeaufforderungen, um die globale Berechtigung zu konfigurieren.

Verwenden Sie die Konfigurationsinformationen, die Sie im Arbeitsblatt für die Konfiguration der globalen Berechtigung zusammengestellt haben.

- 5 Klicken Sie auf **Weiter** und fügen Sie Benutzer oder Gruppen zur globalen Berechtigung hinzu.

- Um Benutzer oder Gruppen basierend auf Ihren Suchkriterien zu filtern, klicken Sie auf **Hinzufügen**, wählen Sie mindestens ein Suchkriterium aus und klicken Sie auf **Suchen**.
- Wählen Sie den Benutzer oder die Gruppe aus, der bzw. die zu der globalen Berechtigung hinzugefügt werden soll, und klicken Sie auf **OK**.

Mithilfe der Strg- und Umschalt-Taste können Sie mehrere Benutzer und Gruppen auswählen.

Wählen Sie zum Einschränken des Zugriffs auf die globale Berechtigung auf bestimmte Clientcomputer die Active Directory-Sicherheitsgruppe aus, die die Namen der Computer enthält, die auf die globale Berechtigung zugreifen dürfen.

Durch Aktivierung des Kontrollkästchens **Nicht authentifizierte Benutzer** können Sie Benutzer für einen nicht authentifizierten Zugriff ermitteln und globalen Anwendungsberechtigungen hinzufügen. Benutzer für einen nicht authentifizierten Zugriff lassen sich globalen Desktop-Berechtigungen nicht hinzufügen.

- 6 Um die globale Berechtigung zu erstellen, klicken Sie auf **Weiter**, überprüfen Sie die Konfiguration für die globale Berechtigung und klicken Sie auf **Fertig stellen**.

Die globale Berechtigung wird auf der Seite „Globale Berechtigungen“ angezeigt.

Ergebnisse

Die Cloud-Pod-Architektur-Funktion speichert die globale Berechtigung in der globalen Datenschicht, die die globale Berechtigung auf jedem Pod im Pod-Verbund repliziert.

Nächste Schritte

Wählen Sie die Desktop-Pools aus, die Desktops oder Anwendungen für die Benutzer in der globalen Berechtigung bereitstellen können, die Sie erstellt haben. Siehe [Hinzufügen eines Pools zu einer globalen Berechtigung in Horizon Console](#).

Hinzufügen eines Pools zu einer globalen Berechtigung in Horizon Console

Sie können mit Horizon Console einen Desktop-Pool einer vorhandenen globalen Desktop-Berechtigung oder einen Anwendungspool einer vorhandenen globalen Anwendungsberechtigung hinzufügen.

Sie können zu einer globalen Berechtigung mehrere Pools hinzufügen. Zu einem bestimmten Pool lässt sich jedoch nur eine globale Berechtigung hinzufügen.

Wenn Sie mehrere Anwendungspools einer globalen Anwendungsberechtigung hinzufügen, müssen Sie jeweils dieselbe Anwendung hinzufügen. Beispielsweise sollten Sie nicht den Rechner und Microsoft Office PowerPoint derselben globalen Anwendungsberechtigung hinzufügen. Wenn Sie unterschiedliche Anwendungen derselben globalen Anwendungsberechtigung hinzufügen, erhalten berechtigte Benutzer eventuell unterschiedliche Anwendungen zu unterschiedlichen Zeitpunkten.

Hinweis Wenn ein Horizon-Administrator das Poolebenen-Anzeigeprotokoll oder die Richtlinie für das Überschreiben von Protokollen ändert, nachdem ein Desktop-Pool mit einer globalen Desktop-Berechtigung verknüpft wurde, können Benutzer, wenn sie die globale Berechtigung auswählen, eine Fehlermeldung erhalten, dass der Desktop nicht gestartet wird. Wenn ein Horizon-Administrator die Richtlinie zum Zurücksetzen von virtuellen Maschinen ändert, nachdem ein Desktop-Pool mit einer globalen Desktop-Berechtigung verknüpft wurde, können Benutzer eine Fehlermeldung erhalten, wenn sie versuchen, den Desktop zurückzusetzen.

Voraussetzungen

- Erstellen und konfigurieren Sie eine globale Berechtigung. Siehe [Erstellen und Konfigurieren einer globalen Berechtigung in Horizon Console](#).
- Erstellen Sie den Desktop- oder Anwendungspool, den Sie der globalen Berechtigung hinzufügen möchten. Weitere Erläuterungen finden Sie im Dokument *Einrichten von virtuellen Desktops in Horizon 7* oder *Einrichten von veröffentlichten Desktops und Anwendungen in Horizon 7*.

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz in dem Pod an, der den Pool enthält, der zu der globalen Berechtigung hinzugefügt werden soll.
- 2 Wählen Sie **Bestandsliste > Globale Berechtigungen**.
- 3 Klicken Sie auf den Namen der globalen Berechtigung.

- 4 Klicken Sie auf der Registerkarte **Lokale Pools** auf **Hinzufügen**, wählen Sie den hinzuzufügenden Desktop- oder Anwendungspool aus und klicken Sie auf **Hinzufügen**.

Sie können die Strg- und Umschalttaste drücken, um mehrere Pools auszuwählen.

Hinweis Pools, die bereits mit einer globalen Berechtigung verknüpft sind oder die nicht die Kriterien für die Richtlinien für die globale Berechtigung erfüllen, die Sie ausgewählt haben, werden nicht angezeigt. Wenn Sie beispielsweise die HTML Access-Richtlinie aktiviert haben, können Sie keine Pools auswählen, für die HTML Access nicht zulässig ist.

- 5 Wiederholen Sie diese Schritte auf einer Verbindungsserver-Instanz in jedem Pod mit einem Pool, der der globalen Berechtigung hinzugefügt werden soll.

Ergebnisse

Wenn ein berechtigter Benutzer mithilfe von Horizon Client eine Verbindung zu einer Verbindungsserver-Instanz im Pod-Verbund herstellt, wird der Name der globalen Berechtigung in der Liste verfügbarer Desktops und Anwendungen angezeigt.

Erstellen und Konfigurieren einer Site in Horizon Console

Wenn die Cloud-Pod-Architektur-Topologie mehrere Pods enthält, können Sie bei Bedarf diese Pods in unterschiedliche Sites gruppieren. Die Funktion Cloud-Pod-Architektur behandelt Pods in der gleichen Site gleichmäßig.

Voraussetzungen

- Entscheiden Sie, ob die Cloud-Pod-Architektur-Topologie Sites enthalten sollte. Siehe [Erstellen von Cloud-Pod-Architektur-Sites](#).
- Initialisieren Sie die Funktion Cloud-Pod-Architektur. Siehe [Initialisieren der Cloud-Pod-Architektur-Funktion in Horizon Console](#).

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Erstellen Sie die Site.
 - a Wählen Sie in Horizon Console **Einstellungen > Sites** aus und klicken Sie auf **Hinzufügen**.
 - b Geben Sie einen Namen für die Site in das Textfeld **Name** ein.
Der Name einer Site kann 1 bis 64 Zeichen enthalten.
 - c (Optional) Geben Sie eine Beschreibung für die Site in das Textfeld **Beschreibung** ein.
Der Site-Name darf zwischen 1 und 1.024 Zeichen lang sein.
 - d Um die Site zu erstellen, klicken Sie auf **OK**.

3 Fügen Sie einen Pod der Site hinzu.

Wiederholen Sie diesen Schritt für jeden Pod, der der Site hinzugefügt werden soll.

- a Wählen Sie in Horizon Console **Einstellungen > Sites** aus.
- b Wählen Sie die Site aus, die momentan den Pod enthält, der zu der Site hinzugefügt werden soll.
- c Wählen Sie den Pod aus, der zu der Site hinzugefügt werden soll, und klicken Sie auf **Bearbeiten**.
- d Wählen Sie die Site aus dem Dropdown-Menü **Site** aus und klicken Sie auf **OK**.

Zuweisen einer Start-Site zu einem Benutzer oder einer Gruppe in Horizon Console

Eine Start-Site ist eine Beziehung zwischen einem Benutzer oder einer Gruppe und einer Cloud-Pod-Architektur-Site. Sie können mit Start-Sites sicherstellen, dass Horizon 7 stets von einer bestimmten Site ausgehend nach Desktops und Anwendungen sucht und nicht auf der Grundlage des aktuellen Standorts des Benutzers. Die Zuweisung von Start-Sites ist optional.

Sie können eine Start-Site auch mit einer globalen Berechtigung verknüpfen, sodass die Start-Site der globalen Berechtigung die eigene Start-Site eines Benutzers überschreibt, wenn der Benutzer die globale Berechtigung auswählt. Weitere Informationen finden Sie unter [Erstellen einer Außerkraftsetzung der Start-Site in Horizon Console](#).

Voraussetzungen

- Entscheiden Sie, ob Sie Start-Sites Benutzern oder Gruppen in der Cloud-Pod-Architektur-Umgebung zuweisen. Siehe [Verwenden von Start-Sites](#).
- Gruppieren Sie die Pods in Ihrem Pod-Verbund in Sites. Siehe [Erstellen und Konfigurieren einer Site in Horizon Console](#).
- Globale Berechtigungen verwenden standardmäßig keine Start-Sites. Beim Erstellen einer globalen Berechtigung müssen Sie die Option **Start-Site verwenden** auswählen, damit Horizon 7 eine Start-Site des Benutzers beim Zuweisen von Desktops aus dieser globalen Berechtigung verwendet. Siehe [Erstellen und Konfigurieren einer globalen Berechtigung in Horizon Console](#).
- Initialisieren Sie die Funktion Cloud-Pod-Architektur. Siehe [Initialisieren der Cloud-Pod-Architektur-Funktion in Horizon Console](#).

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Wählen Sie **Benutzer und Gruppen** aus, klicken Sie auf die Registerkarte **Start-Site-Zuweisung** und klicken Sie auf **Hinzufügen**.

- 3 Um die Benutzer oder Gruppen basierend auf Ihren Suchkriterien zu filtern, wählen Sie mindestens ein Suchkriterium aus und klicken Sie auf **Suchen**.

Durch Aktivierung des Kontrollkästchens **Nicht authentifizierte Benutzer** können Sie Benutzer für einen nicht authentifizierten Zugriff im Pod-Verbund ermitteln.

- 4 Wählen Sie einen Benutzer oder eine Gruppe aus und klicken Sie auf **Weiter**.
- 5 Wählen Sie im Dropdown-Menü **Start-Site** die Start-Site aus, die Sie dem Benutzer bzw. der Gruppe zuweisen möchten, und klicken Sie dann auf **Senden**.

Erstellen einer Außerkraftsetzung der Start-Site in Horizon Console

Sie können eine Start-Site mit einer globalen Berechtigung verknüpfen und so die Start-Site eines Benutzers mit der Start-Site der globalen Berechtigung überschreiben, wenn der Benutzer die globale Berechtigung auswählt.

Sie setzen eine Start-Site außer Kraft, indem Sie diese mit einer globalen Berechtigung und mit einem bestimmten Benutzer oder einer bestimmten Gruppe verknüpfen. Wenn der Benutzer (oder ein Benutzer in einer ausgewählten Gruppe) dann auf die globale Berechtigung zugreift, überschreibt die Start-Site der globalen Berechtigung die Start-Site des Benutzers.

Wenn beispielsweise ein Benutzer, der über eine Start-Site in New York verfügt, auf eine globale Berechtigung zugreift, die diesen Benutzer der Start-Site in London zuordnet, beginnt Horizon mit einer Suche in der Site in London, um die Anwendungsanforderung des Benutzers zu erfüllen, anstatt eine Anwendung aus der Site in New York zuzuweisen.

Voraussetzungen

- Stellen Sie sicher, dass in der globalen Berechtigung die Richtlinie **Start-Site verwenden** aktiviert ist. Weitere Informationen finden Sie unter [Ändern von Attributen oder Richtlinien für eine globale Berechtigung in Horizon Console](#).
- Stellen Sie sicher, dass der Benutzer oder die Gruppe in die globale Berechtigung aufgenommen wurde. Weitere Informationen finden Sie unter [Hinzufügen eines Benutzers oder einer Gruppe zu einer globalen Berechtigung in Horizon Console](#).

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Wählen Sie **Bestandsliste > Globale Berechtigungen**.
- 3 Wählen Sie den Namen der globalen Berechtigung aus, die mit einer Start-Site verknüpft werden soll, und klicken Sie auf die Registerkarte **Start-Site außer Kraft setzen**.
- 4 Klicken Sie auf **Hinzufügen**.

Die Schaltfläche **Hinzufügen** ist nicht verfügbar, wenn die Richtlinie **Start-Site verwenden** für die globale Berechtigung nicht aktiviert ist.

- 5 Wählen Sie mindestens ein Suchkriterium aus und klicken Sie auf **Suchen**, um Active Directory-Benutzer und -Gruppen basierend auf Ihren Suchkriterien zu filtern.
- 6 Wählen Sie den Active Directory-Benutzer oder die Active Directory-Gruppe aus, deren Start-Site Sie außer Kraft setzen möchten, und klicken Sie auf **Weiter**.

Der Benutzer oder die Gruppe muss bereits der globalen Berechtigung zugeordnet sein, die Sie ausgewählt haben.
- 7 Wählen Sie aus dem Dropdown-Menü **Start-Site außer Kraft setzen** die Start-Site aus, die Sie mit der globalen Berechtigung verknüpfen möchten, und klicken Sie auf **Absenden**.

Testen einer Cloud-Pod-Architektur-Konfiguration in Horizon Client

Nachdem Sie eine Cloud-Pod-Architektur-Umgebung initialisiert und konfiguriert haben, führen Sie bestimmte Schritte aus, um zu prüfen, ob die Umgebung ordnungsgemäß konfiguriert ist.

Voraussetzungen

- Installieren Sie die neueste Version von Horizon Client auf einem unterstützten Computer oder mobilen Endgerät.
- Überprüfen Sie, ob Sie über Anmeldeinformationen für einen Benutzer in einer Ihrer neu erstellten globalen Berechtigungen verfügen.

Verfahren

- 1 Starten Sie Horizon Client.
- 2 Stellen Sie unter Verwendung der Anmeldeinformationen eines Benutzers in einer Ihrer neuen globalen Berechtigungen eine Verbindung mit einer beliebigen Verbindungsserver-Instanz im Pod-Verbund her.

Der Name der globalen Berechtigung wird nach dem Herstellen der Verbindung mit der Verbindungsserver-Instanz in der Liste der verfügbaren Desktops und Anwendungen angezeigt.

- 3 Wählen Sie die globale Berechtigung aus und stellen Sie eine Verbindung mit einem Remote-Desktop oder einer veröffentlichten Anwendung her.

Ergebnisse

Der Remote-Desktop oder die veröffentlichte Anwendung wird erfolgreich gestartet. Welcher Remote-Desktop oder welche veröffentlichte Anwendung gestartet wird, richtet sich nach der individuellen Konfiguration der globalen Berechtigung, der Pods und der Desktop- bzw. Anwendungspools. Die Funktion Cloud-Pod-Architektur versucht, einen Remote-Desktop oder eine veröffentlichte Anwendung aus dem Pod zuzuordnen, mit dem Sie verbunden sind.

Nächste Schritte

Wenn die globale Berechtigung beim Herstellen der Verbindung mit der Verbindungsserver-Instanz nicht angezeigt wird, überprüfen Sie mit Horizon Console, ob die Berechtigung richtig konfiguriert ist. Wenn die globale Berechtigung angezeigt, aber ein Remote-Desktop oder eine veröffentlichte Anwendung nicht gestartet wird, sind alle Desktop- und Anwendungspools möglicherweise bereits vollständig anderen Benutzern zugeordnet.

Beispiel: Einrichten einer Cloud-Pod-Architektur-Basiskonfiguration

Dieses Beispiel zeigt, wie Sie die Funktion Cloud-Pod-Architektur verwenden können, um eine Cloud-Pod-Architektur-Konfiguration abzuschließen.

In diesem Beispiel hat eine Krankenversicherung einen mobilen Vertriebsmitarbeiter, der in zwei Regionen tätig ist (die Zentralregion und die Ostregion). Die Vertriebsmitarbeiter präsentieren den Kunden unter Verwendung von mobilen Endgeräten Angebote für Versicherungsverträge, und die Kunden zeigen digitale Dokumente an und unterzeichnen sie.

Die Vertriebsmitarbeiter speichern die Kundendaten nicht auf ihren mobilen Endgeräten, sondern verwenden standardisierte dynamische Desktops. Der Zugriff auf die Kundendaten wird in den Datacentern der Krankenversicherung geschützt.

Die Krankenversicherung verfügt über ein Rechenzentrum in jeder Region. Aufgrund von gelegentlichen Kapazitätsproblemen müssen Vertriebsmitarbeiter nach verfügbaren Desktops in einem nicht lokalen Rechenzentrum suchen und es treten manchmal WAN-Latenz-Probleme auf. Wenn Vertriebsmitarbeiter die Verbindung mit Desktops trennen, aber ihre Sitzungen weiterhin angemeldet sind, müssen sie sich das Datacenter merken, das ihre Sitzungen gehostet hat, damit sie die Verbindung mit ihren Desktops wiederherstellen können.

Um diese Probleme zu beheben, entwirft die Krankenversicherung eine Cloud-Pod-Architektur-Topologie, initialisiert die Cloud-Pod-Architektur-Funktion, verbindet ihre bestehenden Pods mit dem Pod-Verbund, erstellt Sites für alle ihre Rechenzentren, berechtigt ihre Vertriebsmitarbeiter für alle ihre Desktop-Pools und implementiert eine einzelne URL.

Verfahren

1 Entwerfen der Beispieltopologie

Die Versicherung entwirft eine Cloud-Pod-Architektur-Topologie, die eine Site für jede Region enthält.

2 Initialisieren der Beispielkonfiguration

Zum Initialisieren der Cloud-Pod-Architektur-Funktion meldet sich der Horizon-Administrator bei der Horizon Console-Benutzeroberfläche für eine Verbindungsserver-Instanz in „Pod 1 Ost“ an, wählt **Einstellungen > Cloud-Pod-Architektur** aus und klickt auf **Cloud-Pod-Architektur-Funktion initialisieren**.

3 Hinzufügen von Pods in der Beispielkonfiguration

Der Horizon-Administrator verwendet Horizon Console, um „Pod 1 Mitte“ und „Pod 2 Mitte“ zum Pod-Verbund hinzuzufügen.

4 Erstellen von Sites in der Beispielkonfiguration

Der Horizon-Administrator verwendet Horizon Console, um eine Site für die Datencenter Ost und Mitte zu erstellen, und fügt Pods diesen Sites hinzu.

5 Erstellen von globalen Desktop-Berechtigungen in der Beispielkonfiguration

Der Horizon-Administrator verwendet Horizon Console, um eine einzelne globale Desktop-Berechtigung zu erstellen, die allen Vertriebsmitarbeitern eine Berechtigung für alle Desktops in den Desktop-Pools für Vertriebsmitarbeiter über alle Pods im Pod-Verbund erteilt.

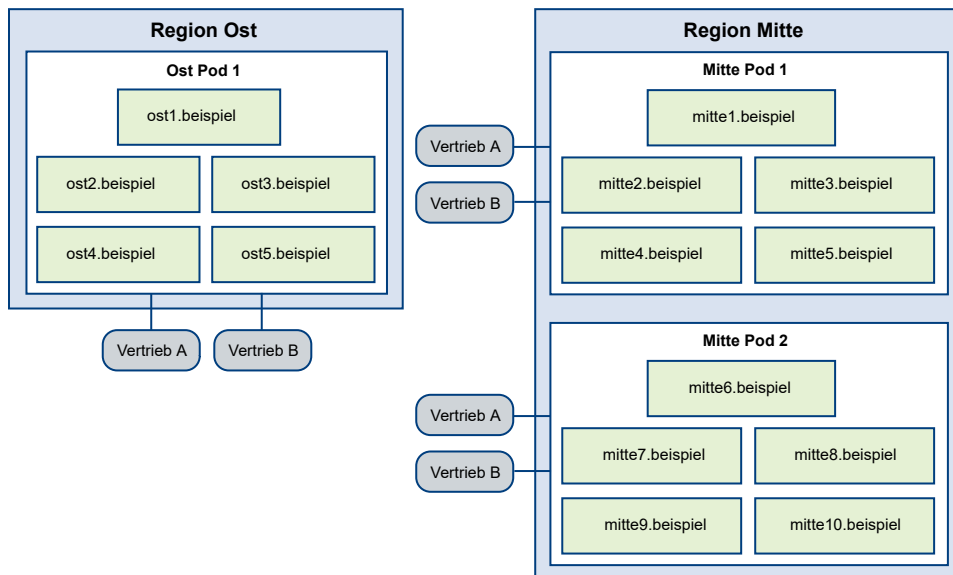
6 Erstellen einer URL für die Beispielkonfiguration

Die Versicherung verwendet eine einzelne URL und einen DNS-Dienst, um Vertrieb.Beispiel an den nächsten Pod im nächsten Rechenzentrum aufzulösen. Mit dieser Anordnung müssen sich Vertriebsmitarbeiter nicht verschiedene URLs für jeden Pod merken und werden immer zum nächsten Rechenzentrum geleitet, unabhängig von ihrem Standort.

Entwerfen der Beispieltopologie

Die Versicherung entwirft eine Cloud-Pod-Architektur-Topologie, die eine Site für jede Region enthält.

Abbildung 3-1. Beispiel Cloud-Pod-Architektur-Topologie



In dieser Topologie enthält die Site der Region Ost einen einzelnen Pod, „Pod 1 Ost“, der aus fünf Verbindungsserver-Instanzen besteht, mit der Bezeichnung „Ost1.Beispiel bis Ost5.Beispiel“.

Die Site der Region Mitte enthält zwei Pods, Pod 1 Mitte und Pod 2 Mitte. Jeder Pod enthält fünf Verbindungsserver-Instanzen. Die Verbindungsserver im ersten Pod werden als „Mitte1.Beispiel“ bis „Mitte5.Beispiel“ bezeichnet. Die Verbindungsserver im zweiten Pod werden als „Mitte6.Beispiel“ bis „Mitte10.Beispiel“ bezeichnet.

Jeder Pod in der Topologie enthält zwei Desktop-Pools von Vertriebsmitarbeiter-Desktops mit der Bezeichnung „Vertrieb A“ und „Vertrieb B“.

Initialisieren der Beispielkonfiguration

Zum Initialisieren der Cloud-Pod-Architektur-Funktion meldet sich der Horizon-Administrator bei der Horizon Console-Benutzeroberfläche für eine Verbindungsserver-Instanz in „Pod 1 Ost“ an, wählt **Einstellungen > Cloud-Pod-Architektur** aus und klickt auf **Cloud-Pod-Architektur-Funktion initialisieren**.

Da der Horizon-Administrator die Horizon Console-Benutzeroberfläche für eine Verbindungsserver-Instanz in „Pod 1 Ost“ verwendet, enthält der Pod-Verbund anfänglich „Pod 1 Ost“. Der Pod-Verbund enthält zudem eine einzelne Site namens „Erste Standard-Site“, die „Pod 1 Ost“ enthält.

Hinzufügen von Pods in der Beispielkonfiguration

Der Horizon-Administrator verwendet Horizon Console, um „Pod 1 Mitte“ und „Pod 2 Mitte“ zum Pod-Verbund hinzuzufügen.

- 1 Um „Pod 1 Mitte“ hinzuzufügen, meldet sich der Horizon-Administrator bei der Horizon Console-Benutzeroberfläche für eine Verbindungsserver-Instanz in „Pod 1 Mitte“ an, wählt **Einstellungen > Cloud-Pod-Architektur** aus, klickt auf **Pod-Verbund beitreten** und gibt den Hostnamen oder die IP-Adresse einer Verbindungsserver-Instanz in „Pod 1 Ost“ ein.

„Pod 1 Mitte“ wurde dem Pod-Verbund hinzugefügt.

- 2 Um „Pod 2 Mitte“ hinzuzufügen, meldet sich der Horizon-Administrator bei der Horizon Console-Benutzeroberfläche für eine Verbindungsserver-Instanz in „Pod 2 Mitte“ an, wählt **Einstellungen > Cloud-Pod-Architektur** aus, klickt auf **Pod-Verbund beitreten** und gibt den Hostnamen oder die IP-Adresse einer Verbindungsserver-Instanz in „Pod 1 Ost“ oder „Pod 1 Mitte“ ein.

„Pod 2 Mitte“ wurde dem Pod-Verbund hinzugefügt.

Nachdem „Pod 1 Mitte“ und „Pod 2 Mitte“ zum Pod-Verbund hinzugefügt wurden, sind alle zehn Verbindungsserver-Instanzen in beiden Pods in der Region Mitte Teil des Pod-Verbunds.

Erstellen von Sites in der Beispielkonfiguration

Der Horizon-Administrator verwendet Horizon Console, um eine Site für die Datacenter Ost und Mitte zu erstellen, und fügt Pods diesen Sites hinzu.

- 1 Der Horizon-Administrator meldet sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.

- 2 Um eine Site für das Datacenter Ost zu erstellen, wählt der Horizon-Administrator **Einstellungen > Sites** aus und klickt auf **Hinzufügen**.
- 3 Um eine Site für das Datacenter Mitte zu erstellen, wählt der Horizon-Administrator **Einstellungen > Sites** aus und klickt auf **Hinzufügen**.
- 4 Um „Pod 1 Ost“ auf die Site für das Datacenter Ost zu verschieben, wählt der Horizon-Administrator **Einstellungen > Sites** aus, wählt die Site aus, die momentan „Pod 1 Ost“ enthält, wählt „Pod 1 Ost“ aus, klickt auf **Bearbeiten** und wählt die Site für das Datacenter Ost aus dem Dropdown-Menü **Site** aus.
- 5 Um „Pod 1 Mitte“ auf die Site für das Datacenter Mitte zu verschieben, wählt der Horizon-Administrator **Einstellungen > Sites** aus, wählt die Site aus, die momentan „Pod 1 Mitte“ enthält, wählt „Pod 1 Mitte“ aus, klickt auf **Bearbeiten** und wählt die Site für das Datacenter Mitte aus dem Dropdown-Menü **Site** aus.
- 6 Um „Pod 2 Mitte“ auf die Site für das Datacenter Mitte zu verschieben, wählt der Horizon-Administrator **Einstellungen > Sites** aus, wählt die Site aus, die momentan „Pod 2 Mitte“ enthält, wählt „Pod 2 Mitte“ aus, klickt auf **Bearbeiten** und wählt die Site für das Datacenter Mitte aus dem Dropdown-Menü **Site** aus.

Die Sitetopologie des Pod-Verbunds entspricht nun der geografischen Verteilung von Pods im Netzwerk der Versicherungsgesellschaft.

Erstellen von globalen Desktop-Berechtigungen in der Beispielkonfiguration

Der Horizon-Administrator verwendet Horizon Console, um eine einzelne globale Desktop-Berechtigung zu erstellen, die allen Vertriebsmitarbeitern eine Berechtigung für alle Desktops in den Desktop-Pools für Vertriebsmitarbeiter über alle Pods im Pod-Verbund erteilt.

- 1 Um Benutzer zur globalen Desktop-Berechtigung hinzuzufügen, meldet sich der Horizon-Administrator bei der Horizon Console-Benutzeroberfläche für einen Verbindungsserver im Pod-Verbund an, wählt **Bestandsliste > Globale Berechtigungen** aus, klickt auf die Registerkarte **Benutzer und Gruppen** und dann auf **Berechtigungen hinzufügen**.

Der Horizon-Administrator fügt die Gruppe „Vertriebsmitarbeiter“ zu der globalen Desktop-Berechtigung hinzu. Die Gruppe „Vertriebsmitarbeiter“ ist in Active Directory definiert und enthält alle Benutzer, die Vertriebsmitarbeiter sind. Nachdem die Gruppe „Vertriebsmitarbeiter“ der globalen Desktop-Berechtigung „Agent-Vertrieb“ hinzugefügt wurde, können Vertriebsmitarbeiter auf die Desktop-Pools „Vertrieb A“ und „Vertrieb B“ in den Pods der Regionen Ost und Mitte zugreifen.

- 2 Um die Desktop-Pools in „Pod 1 Ost“ der globalen Berechtigung hinzuzufügen, meldet sich der Horizon-Administrator bei der Horizon Console-Benutzeroberfläche für eine Verbindungsserver-Instanz in „Pod 1 Ost“ an, wählt **Bestandsliste > Globale Berechtigungen** aus, klickt auf den Namen der globalen Berechtigung, klickt auf **Hinzufügen** auf der Registerkarte **Lokale Pools**, wählt die hinzuzufügenden Desktop-Pools aus und klickt auf **Hinzufügen**.

- 3 Um die Desktop-Pools in „Pod 1 Mitte“ der globalen Desktop-Berechtigung hinzuzufügen, meldet sich der Horizon-Administrator bei der Horizon Console-Benutzeroberfläche für eine Verbindungsserver-Instanz in „Pod 1 Mitte“ an, wählt **Bestandsliste > Globale Berechtigungen** aus, klickt auf den Namen der globalen Desktop-Berechtigung, klickt auf **Hinzufügen** auf der Registerkarte **Lokale Pools**, wählt die hinzuzufügenden Desktop-Pools aus und klickt auf **Hinzufügen**.
- 4 Um die Desktop-Pools in „Pod 2 Mitte“ der globalen Desktop-Berechtigung hinzuzufügen, meldet sich der Horizon-Administrator bei der Horizon Console-Benutzeroberfläche für eine Verbindungsserver-Instanz in „Pod 2 Mitte“ an, wählt **Bestandsliste > Globale Berechtigungen** aus, klickt auf den Namen der globalen Desktop-Berechtigung, klickt auf **Hinzufügen** auf der Registerkarte **Lokale Pools**, wählt die hinzuzufügenden Desktop-Pools aus und klickt auf **Hinzufügen**.

Erstellen einer URL für die Beispielkonfiguration

Die Versicherung verwendet eine einzelne URL und einen DNS-Dienst, um Vertrieb.Beispiel an den nächsten Pod im nächsten Rechenzentrum aufzulösen. Mit dieser Anordnung müssen sich Vertriebsmitarbeiter nicht verschiedene URLs für jeden Pod merken und werden immer zum nächsten Rechenzentrum geleitet, unabhängig von ihrem Standort.

Wenn ein Vertriebsmitarbeiter eine Verbindung mit der URL in Horizon Client herstellt, wird die globale Berechtigung „Agent-Vertrieb“ in der Liste der verfügbaren Desktop-Pools angezeigt. Wenn ein Vertriebsmitarbeiter die globale Desktop-Berechtigung auswählt, stellt die Funktion Cloud-Pod-Architektur den nächsten verfügbaren Desktop im Pod-Verbund bereit. Wenn alle Desktops im lokalen Rechenzentrum verwendet werden, wählt die Funktion Cloud-Pod-Architektur einen Desktop aus einem anderen Rechenzentrum aus. Wenn ein Vertriebsmitarbeiter eine Desktop-Sitzung verlässt, dort aber noch angemeldet ist, navigiert die Funktion Cloud-Pod-Architektur den Vertriebsmitarbeiter zu einem späteren Zeitpunkt zu diesem Desktop, selbst wenn sich der Vertriebsmitarbeiter dann in einer anderen Region befindet.

Verwalten einer Cloud-Pod-Architektur-Umgebung in Horizon Console

4

Sie können Horizon Console verwenden, um Ihre Cloud-Pod-Architektur-Umgebung anzuzeigen, zu ändern und zu verwalten.

Allgemeine Informationen zum Verwenden von Horizon Console finden Sie unter „Verwenden von VMware Horizon Console“ im Dokument *Verwaltung der VMware Horizon Console*. Weitere Informationen zur Verwendung der `lmvutil`-Befehlszeilenschnittstelle finden Sie unter [Kapitel 5 Verwalten der Cloud-Pod-Architektur mit lmvutil](#).

Dieses Kapitel enthält die folgenden Themen:

- [Anzeigen einer Cloud-Pod-Architektur-Konfiguration in Horizon Console](#)
- [Anzeigen des Zustands des Pod-Verbunds in Horizon Console](#)
- [Anzeigen von Desktop- und Anwendungssitzungen in Horizon Console](#)
- [Verwalten von Sites in Horizon Console](#)
- [Verwalten von globalen Berechtigungen in Horizon Console](#)
- [Verwalten von Start-Sites in Horizon Console](#)
- [Entfernen eines Pods aus dem Pod-Verbund in Horizon Console](#)
- [Aufheben der Initialisierung der Cloud-Pod-Architektur-Funktion in Horizon Console](#)

Anzeigen einer Cloud-Pod-Architektur-Konfiguration in Horizon Console

Sie können Horizon Console verwenden, um Informationen zu globalen Berechtigungen, Pods, Sites und Start-Sites anzuzeigen.

Verfahren

- ◆ Zum Auflisten aller globalen Berechtigungen in Ihrer Konfiguration wählen Sie **Bestandsliste > Globale Berechtigungen** aus.

Sie können die Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund verwenden.

- ◆ Wählen Sie zum Auflisten der Desktop- oder Anwendungspools in einer globalen Berechtigung **Bestandsliste > Globale Berechtigungen** aus, klicken Sie auf den Namen der globalen Berechtigung und klicken Sie dann auf die Registerkarte **Lokale Pools**.

Auf der Registerkarte **Lokale Pools** werden nur die Pools im lokalen Pod angezeigt. Enthält eine globale Berechtigung Desktop- oder Anwendungspools in einem Remote-Pod, müssen Sie sich zum Anzeigen dieser Pools bei der Horizon Console-Benutzeroberfläche für eine Verbindungsserver-Instanz im Remote-Pod anmelden.

- ◆ Um die globale Desktop-Berechtigung anzuzeigen, die einen bestimmten Desktop-Pool enthält, wählen Sie **Bestandsliste > Desktops** aus.

Der Name der globalen Desktop-Berechtigung, die den Desktop-Pool enthält, wird in der Spalte „Globale Berechtigung“ für diesen Desktop-Pool auf der Seite „Desktop-Pools“ angezeigt. Sie können auch auf der Seite „Desktop-Pools“ auf den Namen eines Desktop-Pools klicken und den Namen der globalen Desktop-Berechtigung auf der Registerkarte **Übersicht** anzeigen.

- ◆ Wählen Sie zum Auflisten der einer globalen Berechtigung zugeordneten Benutzer oder Gruppen **Bestandsliste > Globale Berechtigungen** aus, klicken Sie auf den Namen der globalen Berechtigung und klicken Sie dann auf die Registerkarte **Benutzer und Gruppen**.

Sie können die Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund verwenden.

- ◆ Um den Pod, bei dem Sie in Horizon Console angemeldet sind, schnell zu identifizieren, suchen Sie in der Kopfzeile im oberen Bereich des Horizon Console-Fensters nach dem Pod-Namen.

Diese Funktion ist besonders nützlich, wenn Sie bei mehreren Pods angemeldet sind.

- ◆ Zum Auflisten der Pods im Pod-Verbund wählen Sie **Einstellung > Cloud-Pod-Architektur** aus.

Sie können die Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund verwenden.

- ◆ Zum Auflisten der Sites im Pod-Verbund, einschließlich der Pods in einer Site, wählen Sie **Einstellungen > Sites** aus.

Sie können die Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund verwenden.

- ◆ Zum Auflisten der Start-Site-Zuweisungen für Benutzer und Gruppen wählen Sie **Benutzer und Gruppen** aus und klicken Sie auf die Registerkarte **Start-Site-Zuweisung**.

- ◆ Mit den nachfolgend aufgeführten Schritten können Sie die Start-Sites für einen Benutzer oder eine Gruppe gemäß der globalen Berechtigung darstellen.

- a Wählen Sie **Benutzer und Gruppen** aus und klicken Sie auf die Registerkarte **Auflösung der Start-Site**.

- b Klicken Sie auf **Benutzer suchen**.

- c Wählen Sie mindestens ein Suchkriterium aus, und klicken Sie auf **Suchen**, um die Active Directory-Benutzer basierend auf Ihren Suchkriterien zu filtern.
- d Wählen Sie den Active Directory-Benutzer aus, und klicken Sie auf **OK**.

Der Name der globalen Berechtigung wird in der Spalte „Berechtigungen“ und die geltende Start-Site für die globale Berechtigung wird in der Spalte „Auflösung der Start-Site“ angezeigt. Der Ursprung einer Start-Site-Zuweisung wird nach dem Namen der Start-Site in Klammern dargestellt. Wenn ein Benutzer mehrere Start-Sites verwendet, erscheint neben dem Namen der globalen Berechtigung ein Ordnersymbol. Sie können diesen Ordner erweitern, um alle Start-Site-Zuweisungen anzuzeigen, die nicht für die globale Berechtigung gelten.

- ◆ Um die mit einer globalen Berechtigung verknüpften Kennzeichen aufzulisten, wählen Sie **Bestandsliste > Globale Berechtigungen** aus, klicken Sie auf den Namen der globalen Berechtigung und klicken Sie auf die Registerkarte **Übersicht**.

Die Tags, die mit der globalen Berechtigung verknüpft sind, werden im Feld „Einschränkungen für Verbindungsserver“ angezeigt.

Anzeigen des Zustands des Pod-Verbunds in Horizon Console

Horizon überwacht den Zustand des Pod-Verbunds fortlaufend durch Prüfung des Zustands der einzelnen Pods und der in ihnen enthaltenen Verbindungsserver-Instanzen. Sie können den Zustand eines Pod-Verbunds in Horizon Console anzeigen.

Sie können den Zustand eines Pod-Verbunds auch unter Verwendung des Befehls `vdmadmin` mit der Option `-H` über die Befehlszeile anzeigen. Weitere Informationen zur `vdmadmin`-Syntax finden Sie im Dokument *Horizon 7-Verwaltung*.

Wichtig Horizon-Ereignisdatenbanken werden nicht von allen Pods in einem Pod-Verbund gemeinsam verwendet.

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Wählen Sie in Horizon Console die Optionen **Überwachen > Dashboard** aus.
- 3 Klicken Sie im Bereich **Systemzustand** auf **Ansicht** und klicken Sie dann auf **Remote-Pods**.

Ergebnisse

Auf der Seite „Remote-Pods“ sind alle Pods, ihre Verbindungsserver-Instanzen und der bekannte Zustandsstatus jeder Verbindungsserver-Instanz aufgelistet.

Ein grünes Zustandssymbol gibt an, dass die Verbindungsserver-Instanz online und für die Funktion Cloud-Pod-Architektur verfügbar ist. Ein rotes Zustandssymbol gibt an, dass die Verbindungsserver-Instanz offline ist oder die Funktion Cloud-Pod-Architektur keine Verbindung mit der Verbindungsserver-Instanz herstellen kann, um ihre Verfügbarkeit zu bestätigen.

Anzeigen von Desktop- und Anwendungssitzungen in Horizon Console

Mithilfe von Horizon Console können Sie Desktop- und Anwendungssitzungen im gesamten Pod-Verbund anzeigen.

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.

2 Führen Sie die folgenden Schritte aus, um nach Sitzungen zu suchen.

- a Wählen Sie in Horizon Console **Sitzungen suchen** aus.
- b Wählen Sie Suchkriterien aus und beginnen Sie die Suche.

Sie können Desktop- und Anwendungssitzungen nach Benutzer, Pod oder Brokering-Pod suchen. Der Benutzer ist der Endbenutzer, der mit dem Desktop oder der Anwendung verbunden ist; der Pod ist der Pod, auf dem der Desktop oder die Anwendung gehostet wird; der Brokering-Pod ist der Pod, mit dem der Benutzer verbunden wurde, als der Desktop erstmalig zugeordnet wurde.

Option	Aktion
Suchen nach Benutzer	<ol style="list-style-type: none"> 1 Wählen Sie Benutzer aus dem Dropdown-Menü aus und klicken Sie auf Benutzer suchen. 2 Wählen Sie Suchkriterien im Dialogfeld „Benutzer suchen“ aus und klicken Sie auf Suchen.
Suchen nach Pod	<ol style="list-style-type: none"> 1 Wählen Sie im Dropdown-Menü Pod aus. 2 Wählen Sie einen Pod aus der Liste der Pods aus und klicken Sie auf Suchen.
Suchen nach Brokering-Pod	<ol style="list-style-type: none"> 1 Wählen Sie Brokering-Pod aus dem Dropdown-Menü aus. 2 Wählen Sie einen Pod aus der Liste der Pods aus und klicken Sie auf Suchen.

Die Suchergebnisse beinhalten den Benutzer, den Sitzungstyp (Desktop oder Anwendung), die Maschine, den Pool oder die Farm, den Pod, die Brokering-Pod-ID, die Site und die jeder Sitzung zugewiesenen globalen Berechtigungen. Weiterhin werden die Startzeit, die Dauer und der Status der Sitzung in den Suchergebnissen angezeigt. Auf der Seite der Suchergebnisse können Sie möglicherweise eine Sitzung trennen oder abmelden, einen Desktop neu starten, eine virtuelle Maschine zurücksetzen oder eine Nachricht an einen Desktop-Benutzer senden.

Hinweis Die Brokering-Pod-ID wird für neue Sitzungen nicht sofort in den Suchergebnissen angezeigt. Diese ID wird normalerweise zwei bis drei Minuten nach Sitzungsbeginn in Horizon Console angezeigt.

- 3 Führen Sie die folgenden Schritte aus, um Informationen zu allen Cloud-Pod-Architektur-Sitzungen anzuzeigen.

- a Wählen Sie **Überwachen > Dashboard** aus.
- b Wählen Sie im Bereich **Cloud-Pod-Architektur-Sitzung** im Dropdown-Menü einen Pod aus.

Das Ringdiagramm zeigt die Gesamtzahl der gehosteten und vermittelten Sitzungen für den ausgewählten Pod.

- c Klicken Sie für weitere Sitzungsinformationen auf **Anzeigen**.

Eine Tabelle zeigt die Gesamtzahl der für die einzelnen Pods vermittelten und gehosteten Sitzungen sowie den Pod-Status. Wenn der Pod-Status rot ist, ist der Pod entweder ausgefallen oder er wird nicht in Horizon 7 Version 7.12 oder höher ausgeführt. Sitzungen in Pods, auf denen frühere Versionen von Horizon 7 ausgeführt werden, werden nicht berücksichtigt.

Verwalten von Sites in Horizon Console

Mit Horizon Console können Sie Cloud-Pod-Architektur-Sites erstellen, ändern und löschen. Eine Site ist eine Gruppe von Pods.

Hinzufügen eines Pods zu einer Site in Horizon Console

Sie können mit Horizon Console einen Pod zu einer vorhandenen Site hinzufügen.

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Wählen Sie **Einstellungen > Sites**.
- 3 Wählen Sie die Site aus, die momentan den Pod enthält, der zu der Site hinzugefügt werden soll.
- 4 Wählen Sie den Pod aus, der zu der Site hinzugefügt werden soll, und klicken Sie auf **Bearbeiten**.
- 5 Wählen Sie die Site aus dem Dropdown-Menü **Site** aus und klicken Sie auf **OK**.

Löschen einer Site in Horizon Console

Sie können eine Site mithilfe von Horizon Console aus dem Pod-Verbund löschen.

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Wählen Sie **Einstellungen > Sites**.

- 3 Wählen Sie die zu löschende Site aus und klicken Sie auf **Löschen** und dann auf **OK**.

Ändern des Namens oder der Beschreibung einer Site in Horizon Console

Sie können mit Horizon Console den Namen oder die Beschreibung einer Site bearbeiten.

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Wählen Sie **Einstellungen > Sites**.
- 3 Wählen Sie die zu bearbeitende Site aus, klicken Sie auf **Bearbeiten**, nehmen Sie Ihre Änderungen vor und klicken Sie auf **OK**.

Verwalten von globalen Berechtigungen in Horizon Console

Sie können mit Horizon Console Pools, Benutzer und Gruppen in globalen Berechtigungen hinzufügen und daraus entfernen. Weiterhin können Sie globale Berechtigungen löschen und die Attribute und Richtlinien von globalen Berechtigungen ändern.

Entfernen eines Pools aus einer globalen Berechtigung in Horizon Console

Mit Horizon Console können Sie einen Pool aus einer globalen Berechtigung entfernen.

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz in dem Pod an, der den zu entfernenden Pool enthält.
- 2 Wählen Sie **Bestandsliste > Globale Berechtigungen**.
- 3 Klicken Sie auf den Namen der globalen Berechtigung.
- 4 Klicken Sie auf der Registerkarte **Lokale Pools** auf die Zeile, die den Pool enthält, klicken Sie auf **Löschen** und klicken Sie auf **OK**.

Hinzufügen eines Benutzers oder einer Gruppe zu einer globalen Berechtigung in Horizon Console

Sie können Horizon Console verwenden, um einer vorhandenen globalen Berechtigung einen Benutzer oder eine Gruppe hinzuzufügen.

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.

- 2 Wählen Sie **Bestandsliste > Globale Berechtigungen** aus und klicken Sie auf den Namen der globalen Berechtigung.
- 3 Klicken Sie auf der Registerkarte **Benutzer und Gruppen** auf **Berechtigungen hinzufügen**.
- 4 Um nach Active Directory-Benutzern oder -Gruppen zu suchen, klicken Sie auf **Hinzufügen**, wählen Sie mindestens ein Suchkriterium aus und klicken Sie auf **Suchen**.

Durch Aktivierung des Kontrollkästchens **Nicht authentifizierte Benutzer** können Sie Benutzer für einen nicht authentifizierten Zugriff ermitteln und globalen Anwendungsberechtigungen hinzufügen. Benutzer für einen nicht authentifizierten Zugriff lassen sich globalen Desktop-Berechtigungen nicht hinzufügen.

- 5 Wählen Sie den Active Directory-Benutzer oder die Active Directory-Gruppe aus, die zu der globalen Berechtigung hinzugefügt werden soll, und klicken Sie auf **OK**.

Mithilfe der Strg- und Umschalt-Taste können Sie mehrere Benutzer und Gruppen auswählen.

Wählen Sie zum Einschränken des Zugriffs auf die globale Berechtigung auf bestimmte Clientcomputer die Active Directory-Sicherheitsgruppe aus, die die Namen der Computer enthält, die auf die globale Berechtigung zugreifen dürfen.

- 6 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Entfernen eines Benutzers oder einer Gruppe aus einer globalen Berechtigung in Horizon Console

Sie können einen Benutzer oder eine Gruppe mithilfe von Horizon Console aus einer globalen Berechtigung entfernen.

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Wählen Sie **Bestandsliste > Globale Berechtigungen** aus und klicken Sie auf den Namen für die globale Berechtigung.
- 3 Aktivieren Sie auf der Registerkarte „Benutzer und Gruppen“ das Kontrollkästchen für den Benutzer oder die Gruppe, den bzw. die Sie löschen möchten, und klicken Sie auf **Berechtigungen entfernen**.
- 4 Klicken Sie im Bestätigungs-Dialogfeld auf **OK**.

Ändern von Attributen oder Richtlinien für eine globale Berechtigung in Horizon Console

Sie können Horizon Console verwenden, um Attribute und Richtlinien für die globale Berechtigung zu ändern.

Sie können den Namen und die Beschreibung der globalen Berechtigung ändern, die Verbindungsserver-Tags, die mit der globalen Berechtigung verknüpft sind, sowie den Kategorienordner, der eine Startmenüverknüpfung für Windows enthält. Sie können Folgendes ändern: Geltungsbereich, Start-Site, redundante Sitzung, Standardanzeigeprotokoll, HTML Access, Vorabstart, Session Collaboration und Clienteinschränkungsrichtlinien. Sie können auch eine globale Sicherheitsberechtigung hinzufügen.

Für eine globale Anwendungsberechtigung können Sie den Anwendungspfad, die Version und den Veröffentlicher ändern, nachdem der erste Anwendungspool hinzugefügt wurde. Wenn Sie einen Anwendungspool einer globalen Anwendungsberechtigung, die bereits einen Anwendungspool enthält, hinzufügen, werden die vorherigen Werte für Anwendungspfad, Version und Veröffentlicher beibehalten.

Den Desktop-Pool-Typ, den eine globale Desktop-Berechtigung enthalten kann, können Sie nicht ändern.

Voraussetzungen

Verwenden Sie das Arbeitsblatt für die Konfiguration der globalen Berechtigung, um die Attribute und Richtlinien aufzuzeichnen, die Sie ändern möchten. Siehe [Arbeitsblatt zur Konfiguration einer globalen Berechtigung](#).

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Wählen Sie **Bestandsliste > Globale Berechtigungen**.
- 3 Wählen Sie die Zeile für die globale Berechtigung aus und klicken Sie auf **Bearbeiten**.
- 4 Ändern Sie die Attribute und Richtlinien für die globale Berechtigung.

Verwenden Sie die Konfigurationsinformationen, die Sie im Arbeitsblatt für die Konfiguration der globalen Berechtigung zusammengestellt haben.

- 5 Klicken Sie auf **Senden**, um Ihre Änderungen zu speichern.

Löschen einer globalen Berechtigung in Horizon Console

Sie können eine globale Berechtigung mit Horizon Console dauerhaft löschen. Wenn Sie eine globale Berechtigung löschen, können alle Benutzer, die von dieser globalen Berechtigung für Desktops abhängig sind, nicht auf ihre Desktops zugreifen. Die Verbindung vorhandener Desktop-Sitzungen bleibt bestehen.

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Wählen Sie **Bestandsliste > Globale Berechtigungen**.
- 3 Klicken Sie auf die Zeile für die zu löschende globale Berechtigung und dann auf **Löschen**.

- 4 Klicken Sie im Bestätigungs-Dialogfeld auf **OK**.

Verwalten von Start-Sites in Horizon Console

Mit Horizon Console können Sie Start-Sites erstellen, ändern, löschen und auflisten.

Ändern einer Start-Site-Zuweisung in Horizon Console

Sie können eine vorhandene Start-Site-Zuweisung für einen bestimmten Benutzer oder eine bestimmte Gruppe in Horizon Console ändern.

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Wählen Sie **Benutzer und Gruppen** aus und klicken Sie auf die Registerkarte **Start-Site-Zuweisung**.
- 3 Wählen Sie die Zeile für den Benutzer oder die Gruppe aus und klicken Sie auf **Bearbeiten**.
- 4 Wählen Sie aus dem Dropdown-Menü **Start-Site** eine andere Start-Site aus und klicken Sie auf **OK**.

Entfernen einer Start-Site-Zuweisung in Horizon Console

Sie können die Zuweisung zwischen einem Benutzer oder einer Gruppe und einer Start-Site in Horizon Console aufheben.

Erläuterungen zum Entfernen der Zuweisung zwischen einer Start-Site und einer globalen Berechtigung für einen bestimmten Benutzer oder eine bestimmte Gruppe finden Sie unter [Entfernen einer Außerkraftsetzung der Start-Site in Horizon Console](#).

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Wählen Sie **Benutzer und Gruppen** aus und klicken Sie auf die Registerkarte **Start-Site-Zuweisung**.
- 3 Wählen Sie die Zeile für den Benutzer oder die Gruppe aus und klicken Sie auf **Löschen**.
- 4 Um die Start-Site-Zuweisung zu entfernen, klicken Sie auf **OK**.

Festlegen der geltenden Start-Site für einen Benutzer in Horizon Console

Da Sie sowohl Benutzern als auch Gruppen Start-Sites zuweisen können, kann ein einzelner Benutzer über mehrere Start-Sites verfügen. Außerdem können Start-Sites, denen globale Berechtigungen zugewiesen sind, die Start-Sites von Benutzern außer Kraft setzen. Mit Horizon Console lässt sich die geltende Start-Site eines Benutzers anzeigen.

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Wählen Sie **Benutzer und Gruppen** aus und klicken Sie auf die Registerkarte **Auflösung der Start-Site**.
- 3 Klicken Sie auf **Benutzer suchen**.
- 4 Um nach Active Directory-Benutzern zu suchen, wählen Sie mindestens ein Suchkriterium aus und klicken Sie auf **Suchen**.
- 5 Wählen Sie den Active Directory-Benutzer aus, dessen geltende Start-Site Sie anzeigen möchten, und klicken Sie auf **OK**.

Ergebnisse

Horizon Console zeigt die geltende Start-Site für jede globale Berechtigung an, zu der der Benutzer gehört. Es werden nur die globalen Berechtigungen angezeigt, deren Richtlinie **Start-Site verwenden** aktiviert ist.

Die geltende Start-Site wird in der Spalte „Auflösung der Start-Site“ angezeigt. Wenn ein Benutzer mehrere Start-Sites verwendet, wird in der Spalte „Berechtigungen“ neben dem Namen der globalen Berechtigung ein Ordnersymbol dargestellt. Sie können diesen Ordner erweitern, um alle Start-Site-Zuweisungen anzuzeigen, die nicht für die globale Berechtigung gelten. In Horizon Console werden nicht geltende Start-Sites durchgestrichen dargestellt.

In Horizon Console wird in der Spalte „Auflösung der Start-Site“ die Herkunft einer Start-Site-Zuweisung nach dem Namen der Start-Site in Klammern dargestellt. Wenn die Start-Site aus einer Gruppe stammt, zu der der Benutzer gehört, wird in Horizon Console der Name der Gruppe angezeigt, etwa **(via Domänenbenutzer)**. Wenn die Start-Site aus der eigenen Start-Site-Zuweisung des Benutzers stammt, wird in Horizon Console **(Standard)** angezeigt. Wenn die Start-Site aus der globalen Berechtigung stammt (Außerkräftsetzung der Start-Site), wird in Horizon Console **(Direkt)** angezeigt.

Wenn ein Benutzer über keine Start-Site verfügt, wird in Horizon Console in der Spalte „Auflösung der Start-Site“ **Es wurde keine Start-Site definiert** dargestellt.

Ändern einer Außerkräftsetzung der Start-Site in Horizon Console

Sie können die Zuweisung zwischen einer globalen Berechtigung und einer Start-Site für einen bestimmten Benutzer oder eine bestimmte Gruppe in Horizon Console ändern.

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Wählen Sie **Bestandsliste > Globale Berechtigungen**.

- 3 Wählen Sie den Namen der globalen Berechtigung aus und klicken Sie auf die Registerkarte **Start-Site außer Kraft setzen**.
- 4 Wählen Sie die Start-Site aus, die Sie außer Kraft setzen möchten, und klicken Sie auf **Bearbeiten**.
- 5 Wählen Sie aus dem Dropdown-Menü **Start-Site außer Kraft setzen** eine andere Start-Site aus und klicken Sie auf **OK**.

Entfernen einer Außerkraftsetzung der Start-Site in Horizon Console

Sie können die Zuweisung zwischen einer globalen Berechtigung und einer Start-Site für einen bestimmten Benutzer oder eine bestimmte Gruppe entfernen.

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Wählen Sie **Bestandsliste > Globale Berechtigungen**.
- 3 Wählen Sie den Namen der globalen Berechtigung aus und klicken Sie auf die Registerkarte **Start-Site außer Kraft setzen**.
- 4 Wählen Sie die Außerkraftsetzung der Start-Site aus und klicken Sie auf **Entfernen**.
- 5 Um die Außerkraftsetzung der Start-Site zu entfernen, klicken Sie auf **OK**.

Entfernen eines Pods aus dem Pod-Verbund in Horizon Console

Mit Horizon Console können Sie einen Pod entfernen, der zuvor dem Pod-Verbund hinzugefügt wurde. Sie können einen Pod aus dem Pod-Verbund entfernen, wenn er anderweitig in Betrieb genommen werden soll oder fehlerhaft konfiguriert wurde.

Um den letzten Pod aus dem Pod-Verbund zu entfernen, müssen Sie die Initialisierung der Funktion Cloud-Pod-Architektur aufheben. Siehe [Aufheben der Initialisierung der Cloud-Pod-Architektur-Funktion in Horizon Console](#).

Wichtig Eine Verbindungsserver-Instanz darf weder beendet noch gestartet werden, während sie aus einem Pod-Verbund entfernt wird. Andernfalls kann der Verbindungsserver-Dienst möglicherweise nicht richtig neu gestartet werden.

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz in dem Pod an, den Sie aus dem Pod-Verbund entfernen möchten.
- 2 Wählen Sie **Einstellungen > Cloud-Pod-Architektur** aus, wählen Sie den zu entfernenden Pod aus und klicken Sie auf **Beitritt aufheben**.

- 3 Um den Vorgang zum Aufheben des Beitritts zu starten, klicken Sie auf **OK**.

In Horizon Console wird der Fortschritt des Vorgangs zum Aufheben des Beitritts angezeigt.

Aufheben der Initialisierung der Cloud-Pod-Architektur-Funktion in Horizon Console

Sie können mit Horizon Console die Initialisierung der Funktion Cloud-Pod-Architektur aufheben.

Voraussetzungen

Sie brauchen die Initialisierung der Funktion Cloud-Pod-Architektur nur in einem Pod im Pod-Verbund aufzuheben. Wenn der Pod-Verbund mehrere Pods enthält, müssen Sie die anderen Pods entfernen, bevor Sie den Vorgang der Aufhebung der Initialisierung starten. Siehe [Entfernen eines Pods aus dem Pod-Verbund in Horizon Console](#).

Verfahren

- 1 Melden Sie sich bei der Horizon Console-Benutzeroberfläche für eine beliebige Verbindungsserver-Instanz im Pod-Verbund an.
- 2 Wählen Sie **Einstellungen > Cloud-Pod-Architektur** aus und klicken Sie auf **Initialisierung aufheben**.
- 3 Um den Vorgang zu starten, klicken Sie auf **OK**.

In Horizon Console wird der Fortschritt des Vorgangs angezeigt. Nach Abschluss der Aufhebung der Initialisierung wird Ihre gesamte Cloud-Pod-Architektur-Konfiguration gelöscht, einschließlich Sites, Start-Sites und globaler Berechtigungen.

Verwalten der Cloud-Pod-Architektur mit Imvutil

5

Sie können die `Imvutil`-Befehlszeilenschnittstelle verwenden, um eine Cloud-Pod-Architektur-Implementierung einzurichten und zu verwalten.

Hinweis Sie können über die `vdmutil`-Befehlszeilenschnittstelle denselben Vorgang wie mit `Imvutil` durchführen.

Dieses Kapitel enthält die folgenden Themen:

- [Verwenden des Befehls „Imvutil“](#)
- [Initialisieren der Funktion Cloud-Pod-Architektur](#)
- [Deaktivieren der Funktion Cloud-Pod-Architektur](#)
- [Verwalten eines Pod-Verbunds](#)
- [Verwalten von Sites](#)
- [Verwalten von globalen Berechtigungen](#)
- [Verwalten von Start-Sites](#)
- [Anzeigen einer Cloud-Pod-Architektur-Konfiguration](#)
- [Verwalten von SSL-Zertifikaten](#)

Verwenden des Befehls „Imvutil“

Die Syntax des Befehls `Imvutil` bestimmt seine Ausführung.

Verwenden Sie den Befehl `Imvutil` an einer Windows-Eingabeaufforderung mit dem folgenden Format.

```
Imvutil command_option [additional_option argument] ...
```

Alternativ dazu können Sie den Befehl `vdmutil` verwenden, um dieselben Vorgänge wie mit dem Befehl `Imvutil` auszuführen. Verwenden Sie den Befehl `vdmutil` an einer Windows-Eingabeaufforderung mit dem folgenden Format.

```
vdmutil command_option [additional_option argument] ...
```

Welche Zusatzoptionen verwendet werden können, hängt von der Befehlsoption ab.

Der Pfad zu den ausführbaren Dateien der Befehle `lmvutil` und `vdmutl` lautet standardmäßig `C:\Programme\VMware\VMware View\Server\tools\bin`. Damit Sie den Pfad nicht in die Befehlszeile eingeben müssen, fügen Sie ihn zur PATH-Umgebungsvariable hinzu.

Authentifizierung für den `lmvutil`-Befehl

Damit Sie mit dem Befehl `lmvutil` eine Cloud-Pod-Architektur-Umgebung konfigurieren und verwalten können, müssen Sie den Befehl als Benutzer mit Administratorrolle ausführen.

Sie können einem Benutzer die Administratorrolle mithilfe von Horizon Console zuweisen. Siehe das Dokument *Horizon 7-Verwaltung*.

Der `lmvutil`-Befehl umfasst Optionen zum Angeben des Benutzernamens, der Domäne und des Kennworts für die Authentifizierung.

Tabelle 5-1. `lmvutil`-Befehlsauthentifizierungsoptionen

Option	Beschreibung
<code>--authAs</code>	Der Name eines Horizon-Administratorbenutzers. Verwenden Sie nicht das Format <i>Domäne\Benutzername</i> oder das UPN-Format (Benutzerprinzipalname).
<code>--authDomain</code>	Der vollqualifizierte Domänenname für den mit der Option <code>--authAs</code> angegebenen Horizon-Administratorbenutzer.
<code>--authPassword</code>	Das Kennwort für den mit der Option <code>--authAs</code> angegebenen Horizon-Administratorbenutzer. Wenn "*" anstelle eines Kennworts eingegeben wird, fordert der Befehl <code>lmvutil</code> zur Eingabe des Kennworts auf. Vertrauliche Kennwörter werden dann nicht im Befehlsverlauf der Befehlszeile hinterlassen.

Beispiel: Der folgende `lmvutil`-Befehl meldet den Benutzer „domainEast\adminEast“ an und initialisiert die Funktion Cloud-Pod-Architektur.

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

Sie müssen die Authentifizierungsoptionen mit allen `lmvutil`-Befehlsoptionen verwenden, mit Ausnahme von `--help` und `--verbose`.

Ausgabe des `lmvutil`-Befehls

Der Befehl `lmvutil` gibt 0 zurück, wenn ein Vorgang erfolgreich ist, und einen fehlerspezifischen Code ungleich null, wenn ein Vorgang fehlschlägt.

Der Befehl `lmvutil` schreibt Fehlermeldungen in die Standardfehler. Wenn ein Vorgang eine Ausgabe erzeugt oder die ausführliche Protokollierung mithilfe der Option `--verbose` aktiviert wurde, schreibt der Befehl `lmvutil` die Ausgabe in die Standardausgabe.

Die Ausgabe des Befehls `lmvutil` erfolgt nur auf Englisch (USA).

Optionen für den Imvutil-Befehl

Über die Optionen des Befehls `Imvutil` wird der Vorgang angegeben, der ausgeführt werden soll. Vor allen Optionen stehen zwei Bindestriche (--).

Einzelheiten zu den Authentifizierungsoptionen des Befehls `Imvutil` finden Sie unter [Authentifizierung für den Imvutil-Befehl](#).

Tabelle 5-2. Optionen für den Imvutil-Befehl

Option	Beschreibung
--activatePendingCertificate	Aktiviert ein ausstehendes SSL-Zertifikat. Siehe Aktivieren eines ausstehenden Zertifikats .
--addGroupEntitlement	Weist eine Benutzergruppe einer globalen Berechtigung zu. Siehe Hinzufügen eines Benutzers oder einer Gruppe zu einer globalen Berechtigung .
--addPoolAssociation	Weist einen Desktop-Pool einer globalen Desktop-Berechtigung oder einen Anwendungspool einer globalen Anwendungsberechtigung zu. Siehe Hinzufügen eines Pools zu einer globalen Berechtigung .
--addUserEntitlement	Weist einen Benutzer einer globalen Berechtigung zu. Siehe Hinzufügen eines Benutzers oder einer Gruppe zu einer globalen Berechtigung .
--assignPodToSite	Weist einen Pod einer Site zu. Siehe Zuweisen eines Pods zu einer Site .
--createGlobalApplicationEntitlement	Erstellt eine globale Anwendungsberechtigung. Siehe Erstellen einer globalen Berechtigung .
--createGlobalEntitlement	Erstellt eine globale Desktop-Berechtigung. Siehe Erstellen einer globalen Berechtigung .
--createSite	Erstellt eine Site. Siehe Erstellen einer Site .
--createGroupHomeSite	Weist eine Benutzergruppe einer Start-Site zu. Siehe Konfigurieren einer Start-Site .
--createPendingCertificate	Erstellt ein ausstehendes SSL-Zertifikat. Siehe Erstellen eines ausstehenden Zertifikats .
--createUserHomeSite	Weist einen Benutzer einer Start-Site zu. Siehe Konfigurieren einer Start-Site .
--deleteGlobalApplicationEntitlement	Löscht eine globale Anwendungsberechtigung. Siehe Löschen einer globalen Berechtigung .
--deleteGlobalEntitlement	Löscht eine globale Desktop-Berechtigung. Siehe Löschen einer globalen Berechtigung .
--deleteSite	Löscht eine Site. Siehe Löschen einer Site .
--deleteGroupHomeSite	Hebt die Zuweisung zwischen einer Benutzergruppe und einer Start-Site auf. Siehe Löschen einer Start-Site .
--deleteUserHomeSite	Hebt die Zuweisung zwischen einem Benutzer und einer Start-Site auf. Siehe Löschen einer Start-Site .

Tabelle 5-2. Optionen für den lmvutil-Befehl (Fortsetzung)

Option	Beschreibung
--editSite	Ändert den Namen oder die Beschreibung einer Site. Siehe Ändern des Namens oder der Beschreibung für eine Site .
--ejectPod	Entfernt einen nicht verfügbaren Pod aus einem Pod-Verbund. Siehe Entfernen eines Pods aus einem Pod-Verbund .
--help	Listet die Optionen des Befehls lmvutil auf.
--initialize	Initialisiert die Funktion Cloud-Pod-Architektur. Siehe Initialisieren der Funktion Cloud-Pod-Architektur .
--join	Fügt einen Pod einem Pod-Verbund hinzu. Siehe Hinzufügen eines Pods zu einem Pod-Verbund .
--listAssociatedPools	Listet die Desktop-Pools auf, die einer globalen Desktop-Berechtigung zugewiesen sind, oder die Anwendungspools, die einer globalen Anwendungsberechtigung zugewiesen sind. Siehe Auflisten der Pools in einer globalen Berechtigung .
--listEntitlements	Listet die Zuweisungen zwischen Benutzern oder Benutzergruppen und globalen Berechtigungen auf. Auflisten der Benutzer oder Gruppen in einer globalen Berechtigung .
--listGlobalApplicationEntitlements	Listet alle globalen Anwendungsberechtigungen auf. Siehe Auflisten von globalen Berechtigungen .
--listGlobalEntitlements	Listet alle globalen Desktop-Berechtigungen auf. Siehe Auflisten von globalen Berechtigungen .
--listPods	Listet die Pods in einer Cloud-Pod-Architektur-Topologie auf. Siehe Auflisten der Pods oder Sites in einer Cloud-Pod-Architektur-Topologie .
--listSites	Listet die Sites in einer Cloud-Pod-Architektur-Topologie auf. Siehe Auflisten der Pods oder Sites in einer Cloud-Pod-Architektur-Topologie .
--listUserAssignments	Listet die Zuweisungen dedizierter Desktop-Pods für eine Kombination aus Benutzer und globaler Berechtigung auf. Siehe Auflisten von dedizierten Desktop-Pool-Zuweisungen .
--removePoolAssociation	Hebt die Zuweisung zwischen einem Desktop-Pool und einer globalen Berechtigung auf. Siehe Entfernen eines Pools aus einer globalen Berechtigung .
--resolveUserHomeSite	Zeigt die geltende Start-Site für einen Benutzer an. Siehe Auflisten der geltenden Start-Site für einen Benutzer .
--removeGroupEntitlement	Entfernt eine Benutzergruppe aus einer globalen Berechtigung. Siehe Entfernen eines Benutzers oder einer Gruppe aus einer globalen Berechtigung .
--removeUserEntitlement	Entfernt einen Benutzer aus einer globalen Berechtigung. Siehe Entfernen eines Benutzers oder einer Gruppe aus einer globalen Berechtigung .

Tabelle 5-2. Optionen für den `lmvutil`-Befehl (Fortsetzung)

Option	Beschreibung
<code>--showGroupHomeSites</code>	Zeigt alle Start-Sites für eine Gruppe an. Siehe Auflisten der Start-Sites für einen Benutzer oder eine Gruppe .
<code>--showUserHomeSites</code>	Zeigt alle Start-Sites für einen Benutzer an. Siehe Auflisten der Start-Sites für einen Benutzer oder eine Gruppe .
<code>--uninitialize</code>	Deaktiviert die Funktion Cloud-Pod-Architektur. Siehe Deaktivieren der Funktion Cloud-Pod-Architektur .
<code>--unjoin</code>	Entfernt einen verfügbaren Pod aus einem Pod-Verbund. Siehe Entfernen eines Pods aus einem Pod-Verbund .
<code>--updateGlobalApplicationEntitlement</code>	Verändert eine globale Anwendungsberechtigung. Siehe Ändern einer globalen Berechtigung .
<code>--updateGlobalEntitlement</code>	Verändert eine globale Desktop-Berechtigung. Siehe Ändern einer globalen Berechtigung .
<code>--updatePod</code>	Ändert den Namen oder die Beschreibung eines Pods. Siehe Ändern des Namens oder der Beschreibung für einen Pod .
<code>--verbose</code>	Aktiviert die ausführliche Protokollierung. Sie können diese Option mit jeder anderen Option kombinieren, um eine detaillierte Befehlsausgabe zu erhalten. Mit dem Befehl <code>lmvutil</code> erhalten Sie eine Standardausgabe.

Initialisieren der Funktion Cloud-Pod-Architektur

Verwenden Sie den `lmvutil`-Befehl mit der `--initialize`-Option, um die Funktion Cloud-Pod-Architektur zu initialisieren. Wenn Sie die Funktion Cloud-Pod-Architektur initialisieren, richtet Horizon die globale Datenschicht auf jeder Verbindungsserver-Instanz im Pod ein und konfiguriert den VIPA-Kommunikationskanal.

Syntax

```
lmvutil --initialize
```

Nutzungshinweise

Führen Sie diesen Befehl nur einmal und nur auf einer Verbindungsserver-Instanz im Pod aus. Der Befehl kann auf jeder Verbindungsserver-Instanz im Pod ausgeführt werden. Sie brauchen den Befehl nicht für weitere Pods auszuführen. Alle anderen Pods werden dem initialisierten Pod hinzugefügt.

Dieser Befehl gibt eine Fehlermeldung zurück, wenn die Funktion Cloud-Pod-Architektur bereits initialisiert wurde oder der Befehl den Vorgang nicht abschließen kann.

Beispiel

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

Deaktivieren der Funktion Cloud-Pod-Architektur

Verwenden Sie den `lmvutil`-Befehl mit der `--uninitialize`-Option, um die Funktion Cloud-Pod-Architektur zu deaktivieren.

Syntax

```
lmvutil --uninitialize
```

Nutzungshinweise

Vor der Ausführung dieses Befehls entfernen Sie mit dem Befehl `lmvutil` mit der Option `--unjoin` alle anderen Pods aus dem Pod-Verbund.

Führen Sie diesen Befehl auf nur einer Verbindungsserver-Instanz in einem Pod aus. Der Befehl kann auf jeder Verbindungsserver-Instanz im Pod ausgeführt werden. Enthält Ihr Pod-Verbund mehrere Pods, müssen Sie diesen Befehl nur für einen Pod ausführen.

Dieser Befehl gibt eine Fehlermeldung zurück, wenn die Funktion Cloud-Pod-Architektur nicht initialisiert ist, wenn der Befehl den Pod nicht finden kann oder wenn der Pod-Verbund andere Pods enthält.

Beispiel

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

Verwalten eines Pod-Verbunds

Mit den Optionen des Befehls `lmvutil` können Sie einen Pod-Verbund konfigurieren und ändern.

- [Hinzufügen eines Pods zu einem Pod-Verbund](#)
Verwenden Sie den Befehl `lmvutil` mit der Option `--join`, um einen Pod zum Pod-Verbund hinzuzufügen.
- [Entfernen eines Pods aus einem Pod-Verbund](#)
Verwenden Sie den Befehl `lmvutil` mit der Option `--unjoin` oder `--ejectPod`, um einen Pod aus einem Pod-Verbund zu entfernen.
- [Ändern des Namens oder der Beschreibung für einen Pod](#)
Verwenden Sie den Befehl `lmvutil` mit der Option `--updatePod`, um den Namen oder die Beschreibung eines Pods zu aktualisieren oder zu ändern.

Hinzufügen eines Pods zu einem Pod-Verbund

Verwenden Sie den Befehl `lmvutil` mit der Option `--join`, um einen Pod zum Pod-Verbund hinzuzufügen.

Syntax

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

Nutzungshinweise

Sie müssen diesen Befehl auf jedem Pod ausführen, den Sie dem Pod-Verbund hinzufügen möchten. Der Befehl kann auf jeder Verbindungsserver-Instanz in einem Pod ausgeführt werden.

Dieser Befehl gibt eine Fehlermeldung zurück, wenn Sie ungültige Anmeldeinformationen angeben, die angegebene Verbindungsserver-Instanz nicht vorhanden ist, auf dem angegebenen Server kein Pod-Verbund vorhanden ist oder der Befehl den Vorgang nicht durchführen kann.

Optionen

Wenn Sie einen Pod einem Pod-Verbund hinzufügen, müssen Sie mehrere Optionen angeben.

Tabelle 5-3. Optionen zum Hinzufügen eines Pods zu einem Pod-Verbund

Option	Beschreibung
<code>--joinServer</code>	Der DNS-Name oder die IP-Adresse einer beliebigen Verbindungsserver-Instanz in einem initialisierten oder bereits im Pod-Verbund enthaltenen Pod.
<code>--userName</code>	Der Name eines Horizon-Administratorbenutzers auf dem bereits initialisierten Pod. Verwenden Sie das Format <i>Domäne\Benutzername</i> .
<code>--password</code>	Das Kennwort des in der Option <code>--userName</code> angegebenen Benutzers.

Beispiel

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

Entfernen eines Pods aus einem Pod-Verbund

Verwenden Sie den Befehl `lmvutil` mit der Option `--unjoin` oder `--ejectPod`, um einen Pod aus einem Pod-Verbund zu entfernen.

Syntax

```
lmvutil --unjoin
```

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

Nutzungshinweise

Um einen Pod aus einem Pod-Verbund zu entfernen, verwenden Sie die Option `--unjoin`. Der Befehl kann auf jeder Verbindungsserver-Instanz im Pod ausgeführt werden.

Um einen Pod zu entfernen, der nicht aus einem Pod-Verbund verfügbar ist, verwenden Sie die Option `--ejectPod`. Ein Pod ist z. B. im Falle eines Hardwareausfalls nicht mehr verfügbar. Dieser Vorgang kann in jedem Pod des Pod-Verbunds ausgeführt werden.

Wichtig In den meisten Fällen sollten Sie die Option `--unjoin` verwenden, um einen Pod aus einem Pod-Verbund zu entfernen.

Diese Befehle geben eine Fehlermeldung zurück, wenn die Funktion Cloud-Pod-Architektur nicht initialisiert ist, wenn der Pod nicht zu einem Pod-Verbund gehört oder wenn die Befehle die angegebenen Vorgänge nicht ausführen können.

Optionen

Bei Verwendung der Option `--ejectPod` geben Sie über die Option `--pod` den Pod an, der aus dem Pod-Verbund entfernt werden soll.

Beispiel

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

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

Ändern des Namens oder der Beschreibung für einen Pod

Verwenden Sie den Befehl `lmvutil` mit der Option `--updatePod`, um den Namen oder die Beschreibung eines Pods zu aktualisieren oder zu ändern.

Syntax

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

Nutzungshinweise

Dieser Befehl gibt eine Fehlermeldung zurück, wenn die Funktion Cloud-Pod-Architektur nicht initialisiert ist oder wenn der Befehl den Pod nicht finden oder aktualisieren kann.

Optionen

Sie können diese Optionen angeben, wenn Sie den Namen oder die Beschreibung eines Pods aktualisieren.

Tabelle 5-4. Optionen zum Ändern des Namens oder der Beschreibung für einen Pod

Option	Beschreibung
<code>--podName</code>	Name des zu aktualisierenden Pods.
<code>--newPodName</code>	(Optional) Neuer Name für den Pod. Der Name eines Pods kann 1 bis 64 Zeichen enthalten.
<code>--description</code>	(Optional) Beschreibung der Site. Die Beschreibung kann 1 bis 1024 Zeichen enthalten.

Beispiel

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

Verwalten von Sites

Mit den Optionen des Befehls `lmvutil` können Sie Cloud-Pod-Architektur-Sites erstellen, ändern und löschen. Eine Site ist eine Gruppe von Pods.

- **Erstellen einer Site**
Verwenden Sie den `lmvutil`-Befehl mit der `--createSite`-Option, um eine Site in einer Cloud-Pod-Architektur-Topologie zu erstellen.
- **Zuweisen eines Pods zu einer Site**
Verwenden Sie den Befehl `lmvutil` mit der Option `--assignPodToSite`, um einen Pod einer Site zuzuweisen.
- **Ändern des Namens oder der Beschreibung für eine Site**
Verwenden Sie den Befehl `lmvutil` mit der Option `--editSite`, um den Namen oder die Beschreibung einer Site zu bearbeiten.
- **Löschen einer Site**
Verwenden Sie den Befehl `lmvutil` mit der Option `--deleteSite`, um eine Site zu löschen.

Erstellen einer Site

Verwenden Sie den `lmvutil`-Befehl mit der `--createSite`-Option, um eine Site in einer Cloud-Pod-Architektur-Topologie zu erstellen.

Syntax

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

Nutzungshinweise

Dieser Befehl gibt eine Fehlermeldung zurück, wenn die Funktion Cloud-Pod-Architektur nicht initialisiert ist, die angegebene Site bereits vorhanden ist oder wenn der Befehl die Site nicht erstellen kann.

Optionen

Sie können diese Optionen bei der Erstellung einer Site angeben.

Tabelle 5-5. Optionen zum Erstellen einer Site

Option	Beschreibung
--siteName	Name der neuen Site. Der Name einer Site kann 1 bis 64 Zeichen enthalten.
--description	(Optional) Beschreibung der Site. Die Beschreibung kann 1 bis 1024 Zeichen enthalten.

Beispiel

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

Zuweisen eines Pods zu einer Site

Verwenden Sie den Befehl `lmvutil` mit der Option `--assignPodToSite`, um einen Pod einer Site zuzuweisen.

Syntax

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

Nutzungshinweise

Bevor Sie einer Site einen Pod zuweisen können, müssen Sie die Site erstellen. Siehe [Erstellen einer Site](#).

Dieser Befehl gibt eine Fehlermeldung zurück, wenn die Funktion Cloud-Pod-Architektur nicht initialisiert ist, wenn der Befehl den angegebenen Pod oder die angegebene Site nicht finden kann oder wenn der Befehl den Pod nicht der Site zuweisen kann.

Optionen

Sie müssen diese Optionen angeben, wenn Sie einer Site einen Pod zuweisen.

Tabelle 5-6. Optionen zum Zuweisen eines Pods zu einer Site

Option	Beschreibung
--podName	Name des Pods, der der Site zugewiesen werden soll.
--siteName	Name der Site.

Sie können den `lmvutil`-Befehl mit der `--listPods`-Option verwenden, um die Namen der Pods in einer Cloud-Pod-Architektur-Topologie aufzulisten. Siehe [Auflisten der Pods oder Sites in einer Cloud-Pod-Architektur-Topologie](#).

Beispiel

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

Ändern des Namens oder der Beschreibung für eine Site

Verwenden Sie den Befehl `lmvutil` mit der Option `--editSite`, um den Namen oder die Beschreibung einer Site zu bearbeiten.

Syntax

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

Nutzungshinweise

Dieser Befehl gibt eine Fehlermeldung zurück, wenn die angegebene Site nicht vorhanden ist oder der Befehl die Site nicht finden oder aktualisieren kann.

Optionen

Sie können diese Optionen angeben, wenn Sie den Namen oder die Beschreibung einer Site ändern.

Tabelle 5-7. Optionen zum Ändern des Namens oder der Beschreibung einer Site

Option	Beschreibung
<code>--siteName</code>	Name der zu bearbeitenden Site.
<code>--newSiteName</code>	(Optional) Neuer Name für die Site. Der Name einer Site kann 1 bis 64 Zeichen enthalten.
<code>--description</code>	(Optional) Beschreibung der Site. Die Beschreibung kann 1 bis 1024 Zeichen enthalten.

Beispiel

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

Löschen einer Site

Verwenden Sie den Befehl `lmvutil` mit der Option `--deleteSite`, um eine Site zu löschen.

Syntax

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

Nutzungshinweise

Wenn die angegebene Site nicht existiert oder wenn der Befehl die Site nicht finden oder nicht löschen kann, wird eine Fehlermeldung zurückgegeben.

Optionen

Mit der Option `--sitename` geben Sie den Namen der zu löschenden Site an.

Beispiel

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

Verwalten von globalen Berechtigungen

Mit den Optionen des Befehls `lmvutil` können Sie globale Desktop- und Anwendungsberechtigungen in einer Cloud-Pod-Architektur-Umgebung erstellen, ändern und auflisten.

■ Erstellen einer globalen Berechtigung

Zum Erstellen einer globalen Desktop-Berechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--createGlobalEntitlement`. Zum Erstellen einer globalen Anwendungsberechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--createGlobalApplicationEntitlement`.

■ Ändern einer globalen Berechtigung

Zum Verändern einer globalen Desktop-Berechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--updateGlobalEntitlement`. Zum Verändern einer globalen Anwendungsberechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--updateGlobalApplicationEntitlement`.

■ Löschen einer globalen Berechtigung

Zum Löschen einer globalen Desktop-Berechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--deleteGlobalEntitlement`. Zum Löschen einer globalen Anwendungsberechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--deleteGlobalApplicationEntitlement`.

■ Hinzufügen eines Pools zu einer globalen Berechtigung

Verwenden Sie den `lmvutil`-Befehl mit der `--addPoolAssociation`-Option, um einen Desktop-Pool einer globalen Desktop-Berechtigung oder einen Anwendungspool einer globalen Anwendungsberechtigung hinzuzufügen.

■ Entfernen eines Pools aus einer globalen Berechtigung

Verwenden Sie den `lmvutil`-Befehl mit der `--removePoolAssociation`-Option, um einen Desktop-Pool aus einer globalen Desktop-Berechtigung oder einen Anwendungspool aus einer globalen Anwendungsberechtigung zu entfernen.

■ Hinzufügen eines Benutzers oder einer Gruppe zu einer globalen Berechtigung

Zum Hinzufügen eines Benutzers zu einer globalen Berechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--addUserEntitlement`. Zum Hinzufügen einer Gruppe zu einer globalen Berechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--addGroupEntitlement`.

■ Entfernen eines Benutzers oder einer Gruppe aus einer globalen Berechtigung

Zum Entfernen eines Benutzers aus einer globalen Berechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--removeUserEntitlement`. Zum Entfernen einer Gruppe aus einer globalen Berechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--removeGroupEntitlement`.

Erstellen einer globalen Berechtigung

Zum Erstellen einer globalen Desktop-Berechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--createGlobalEntitlement`. Zum Erstellen einer globalen Anwendungsberechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--createGlobalApplicationEntitlement`.

Globale Berechtigungen ermöglichen die Verbindung zwischen Benutzern und ihren Desktops bzw. Anwendungen, unabhängig davon, wo sich diese Desktops und Anwendungen im Pod-Verbund befinden. Globale Berechtigungen beinhalten auch Richtlinien, die festlegen, wie die Funktion Cloud-Pod-Architektur Desktops und Anwendungen berechtigten Benutzer zuweist.

Syntax

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

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

Nutzungshinweise

Sie können diese Befehle auf jeder Verbindungsserver-Instanz in einem Pod-Verbund verwenden. Die Cloud-Pod-Architektur-Funktion speichert neue Daten in der globalen Datenschicht und repliziert diese Daten in allen Pods im Pod-Verbund.

Diese Befehle geben eine Fehlermeldung zurück, wenn die globale Berechtigung bereits vorhanden ist, der Geltungsbereich ungültig ist, die Funktion Cloud-Pod-Architektur nicht initialisiert ist oder wenn die Befehle die globale Berechtigung nicht erstellen können.

Optionen

Sie können diese Optionen bei der Erstellung einer globalen Berechtigung angeben. Einige Optionen können nur für globale Desktop-Berechtigungen verwendet werden.

Tabelle 5-8. Optionen zum Erstellen von globalen Berechtigungen

Option	Beschreibung
<code>--entitlementName</code>	Der Name der globalen Berechtigung. Der Name kann zwischen 1 und 64 Zeichen enthalten. Der Name der globalen Berechtigung erscheint in der Liste der Desktops und Anwendungen in Horizon Client für berechtigte Benutzer.
<code>--scope</code>	Der Geltungsbereich der globalen Berechtigung. Folgende Werte sind gültig: <ul style="list-style-type: none"> ■ BELIEBIG. Horizon sucht nach Ressourcen in jedem Pod im Pod-Verbund. ■ SITE. Horizon sucht nach Ressourcen nur auf Pods in der Site des Pods, mit dem der Benutzer verbunden ist. ■ LOCAL. Horizon sucht nach Ressourcen nur in dem Pod, zu dem der Benutzer eine Verbindung hergestellt hat.
<code>--isDedicated</code>	Erstellt eine dedizierte Desktop-Berechtigung. Eine dedizierte Desktop-Berechtigung kann nur dedizierte Desktop-Pools enthalten. Um eine dynamische Desktop-Berechtigung zu erstellen, verwenden Sie die Option <code>--isFloating</code> . Eine globale Desktop-Berechtigung kann entweder dediziert oder dynamisch sein. Sie können die Optionen <code>--isDedicated</code> und <code>--multipleSessionAutoClean</code> nicht zusammen angeben. Gilt nur für globale Desktop-Berechtigungen.
<code>--isFloating</code>	Erstellt eine dynamische Desktop-Berechtigung. Eine dynamische Desktop-Berechtigung kann nur dynamische Desktop-Pools enthalten. Um eine dedizierte Desktop-Berechtigung zu erstellen, geben Sie die Option <code>--isDedicated</code> an. Eine globale Desktop-Berechtigung kann entweder dynamisch oder dediziert sein. Gilt nur für globale Desktop-Berechtigungen.
<code>--disabled</code>	(Optional) Erstellt die globale Berechtigung im deaktivierten Status.
<code>--description</code>	(Optional) Eine Beschreibung der globalen Berechtigung. Die Beschreibung kann 1 bis 1024 Zeichen enthalten.
<code>--fromHome</code>	(Optional) Verfügt der Benutzer über eine Start-Site, beginnt Horizon auf der Start-Site des Benutzers mit der Suche nach Ressourcen. Hat der Benutzer keine Start-Site, sucht Horizon nach Ressourcen auf der Site, mit der der Benutzer derzeit verbunden ist.

Tabelle 5-8. Optionen zum Erstellen von globalen Berechtigungen (Fortsetzung)

Option	Beschreibung
<code>--multipleSessionAutoClean</code>	<p>(Optional) Meldet zusätzliche Benutzersitzungen für dieselbe Berechtigung ab. Mehrere Sitzungen sind möglich, wenn ein Pod, der eine Sitzung enthält, offline geschaltet wird, der Benutzer sich erneut anmeldet und eine andere Sitzung startet und der problematische Pod wieder mit der ursprünglichen Sitzung online geschaltet wird.</p> <p>Wenn mehrere Sitzungen vorhanden sind, fordert Horizon Client den Benutzer auf, eine Sitzung auszuwählen. Diese Option legt fest, was mit Sitzungen passiert, die der Benutzer nicht auswählt.</p> <p>Wenn Sie diese Option nicht angeben, müssen die Benutzer ihre eigenen zusätzlichen Sitzungen durch Abmeldung im Horizon Client oder durch Start der Sitzungen und deren Abmeldung manuell beenden.</p>
<code>--requireHomeSite</code>	<p>(Optional) Bewirkt, dass die globale Berechtigung nur dann verfügbar ist, wenn der Benutzer eine Start-Site besitzt. Diese Option ist nur dann anwendbar, wenn auch die Option <code>--fromHome</code> angegeben wird.</p>
<code>--defaultProtocol</code>	<p>(Optional) Legt ein Standardanzeigeprotokoll für Desktops oder Anwendungen in der globalen Berechtigung fest. Zulässig sind die Werte RDP, PCOIP sowie BLAST für globale Desktop-Berechtigungen und PCOIP sowie BLAST für globale Anwendungsberechtigungen.</p>
<code>--preventProtocolOverride</code>	<p>(Optional) Verhindert, dass Benutzer das Standardanzeigeprotokoll überschreiben.</p>
<code>--allowReset</code>	<p>(Optional) Ermöglicht Benutzern das Zurücksetzen von Desktops. Gilt nur für globale Desktop-Berechtigungen.</p>
<code>--htmlAccess</code>	<p>(Optional) Aktiviert die HTML Access-Richtlinie, mit der Benutzer die HTML Access-Funktion für den Zugriff auf Ressourcen in der globalen Berechtigung verwenden können. Bei HTML Access können Endbenutzer mithilfe eines Webbrowsers auf Remote-Ressourcen zugreifen und müssen keine Clientsoftware auf ihren lokalen Systemen installieren.</p>
<code>--multipleSessionsPerUser</code>	<p>(Optional) Aktiviert die Richtlinie für mehrere Sitzungen pro Benutzer, mit der Benutzer separate Desktop-Sitzungen von unterschiedlichen Clientgeräten aus initiieren können. Benutzer, die eine Verbindung mit der globalen Desktop-Berechtigung von unterschiedlichen Clientgeräten aus herstellen, werden mit unterschiedlichen Desktop-Sitzungen verbunden. Um erneut eine Verbindung mit einer vorhandenen Desktop-Sitzung herzustellen, müssen Benutzer das Gerät verwenden, von dem aus die Sitzung initiiert wurde. Wenn Sie diese Richtlinie nicht aktivieren, werden Benutzer immer erneut mit ihren vorhandenen Desktop-Sitzungen verbunden, unabhängig vom verwendeten Clientgerät. Gilt nur für dynamische Desktop-Berechtigungen.</p>
<code>--preLaunch</code>	<p>(Optional) Aktiviert die Richtlinie für den Vorabstart, die die Anwendungssitzung startet, bevor ein Benutzer die globale Anwendungsberechtigung in Horizon Client öffnet. Wenn Sie die Richtlinie für den Vorabstart aktivieren, können Benutzer die globale Anwendungsberechtigung schneller starten. Alle Anwendungspools in der globalen Anwendungsberechtigung müssen die Funktion für den Vorabstart der Sitzung unterstützen, und die Zeitüberschreitung für die vorab gestartete Sitzung muss für alle Farmen identisch sein.</p>

Tabelle 5-8. Optionen zum Erstellen von globalen Berechtigungen (Fortsetzung)

Option	Beschreibung
--tags	(Optional) Legt ein oder mehrere Kennzeichen fest, mit denen der Zugriff auf globale Berechtigungen von Verbindungsserver-Instanzen aus eingeschränkt wird. Wenn Sie mehrere Kennzeichen angeben möchten, geben Sie eine Liste der Kennzeichen in Anführungszeichen ein. Die Kennzeichen müssen durch ein Komma oder durch ein Semikolon getrennt sein. Weitere Informationen finden Sie unter Implementieren von Verbindungsserver-Einschränkungen für globale Berechtigungen .
--categoryFolder	(Optional) Legt den Namen des Kategorienordners fest, der eine Verknüpfung für die globale Berechtigung auf Clientgeräten enthält. Sie können bis zu vier Ordnebenen konfigurieren. Ein Ordnername darf bis zu 64 Zeichen enthalten. Geben Sie einen umgekehrten Schrägstrich (\) ein, z. B. dir1\dir2\dir3\dir4, um einen Unterordner anzugeben. Sie können bis zu vier Ordnebenen eingeben. Sie können einen Ordnernamen nicht mit einem umgekehrten Schrägstrich beginnen oder beenden und auch nicht zwei oder mehr umgekehrte Schrägstriche kombinieren. Beispielsweise sind \dir1, dir1\dir2\, dir1\\dir2 und dir1\\dir2 ungültig. Sie können keine für Windows reservierten Schlüsselwörter eingeben. Sie müssen auch die --shortcutLocations-Option angeben, um den Speicherort der Verknüpfung auf einem Windows-Clientgerät anzugeben. Weitere Informationen finden Sie unter Konfigurieren von Verknüpfungen für globale Berechtigungen .
--clientRestrictions	(Optional) Aktiviert die Clienteinschränkungsrichtlinie, die den Zugriff auf die globale Berechtigung auf bestimmte Clientcomputer einschränkt. Weitere Informationen finden Sie unter Implementieren von Clienteinschränkungen für globale Berechtigungen .
--collaboration	(Optional) Aktiviert die Session Collaboration-Richtlinie, die es Benutzern von Remote-Desktop-Sitzungen ermöglicht, andere Benutzer zur Teilname an ihren Sitzungen einzuladen. Alle Desktop-Pools in der globalen Desktop-Berechtigung müssen die Funktion „Session Collaboration“ unterstützen. Gilt nur für globale Desktop-Berechtigungen.
--shortcutLocations	(Optional) Verwenden Sie diese Option mit der --categoryFolder-Option, um den Speicherort der Verknüpfung auf dem Clientgerät anzugeben. Gültige Werte sind desktop, wodurch die Verknüpfung auf dem Windows-Desktop erstellt wird, und launcher, wodurch die Verknüpfung im Startmenü von Windows erstellt wird. Sie können auch beides angeben, desktop und launcher, durch Kommas getrennt, um damit eine Windows-Desktop-Verknüpfung und eine Verknüpfung mit dem Windows-Startmenü zu erstellen.
--multiSessionMode	(Optional) Konfiguriert die Funktion „Mehrfachsitzungsmodus“ für die globale Anwendungsberechtigung. Geben Sie einen der folgenden Werte an: DISABLED, ENABLED_DEFAULT_OFF, ENABLED_DEFAULT_ON oder ENABLED_ENFORCED. Weitere Informationen finden Sie unter Aktivieren des Mehrfachsitzungsmodus für globale Anwendungsberechtigungen .
--displayAssignedHostName	(Optional) Zeigt in Horizon Client anstelle des namens der globalen Berechtigung den Hostnamen der Maschine an, die dem Benutzer zugewiesen ist. Gilt nur für dedizierte Desktop-Berechtigungen.

Beispiele

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

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

Ändern einer globalen Berechtigung

Zum Verändern einer globalen Desktop-Berechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--updateGlobalEntitlement`. Zum Verändern einer globalen Anwendungsberechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--updateGlobalApplicationEntitlement`.

Syntax

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

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

Nutzungshinweise

Sie können diese Befehle auf jeder Verbindungsserver-Instanz in einem Pod-Verbund verwenden. Die Cloud-Pod-Architektur-Funktion speichert neue Daten in der globalen Datenschicht und repliziert diese Daten in allen Pods im Pod-Verbund.

Diese Befehle geben eine Fehlermeldung zurück, wenn die globale Berechtigung nicht vorhanden ist, wenn der Geltungsbereich ungültig ist, wenn die Funktion Cloud-Pod-Architektur nicht initialisiert ist oder wenn die Befehle die globale Berechtigung nicht aktualisieren können.

Optionen

Sie können diese Optionen beim Ändern einer globalen Berechtigung angeben. Einige Optionen gelten nur für globale Desktop-Berechtigungen oder nur für globale Anwendungsberechtigungen.

Tabelle 5-9. Optionen zum Ändern von globalen Berechtigungen

Option	Beschreibung
--entitlementName	Name der globalen Berechtigung, die geändert werden soll.
--scope	Der Geltungsbereich der globalen Berechtigung. Folgende Werte sind gültig: <ul style="list-style-type: none"> ■ BELIEBIG. Horizon sucht nach Ressourcen in jedem Pod im Pod-Verbund. ■ SITE. Horizon sucht nach Ressourcen nur auf Pods in der Site des Pods, mit dem der Benutzer verbunden ist. ■ LOCAL. Horizon sucht nach Ressourcen nur in dem Pod, zu dem der Benutzer eine Verbindung hergestellt hat.
--description	(Optional) Eine Beschreibung der globalen Berechtigung. Die Beschreibung kann 1 bis 1024 Zeichen enthalten.
--disabled	(Optional) Deaktiviert eine globale Berechtigung, die zuvor aktiviert wurde.
--enabled	(Optional) Aktiviert eine globale Berechtigung, die zuvor deaktiviert wurde.
--fromHome	(Optional) Verfügt der Benutzer über eine Start-Site, beginnt Horizon auf der Start-Site des Benutzers mit der Suche nach Ressourcen. Hat der Benutzer keine Start-Site, sucht Horizon nach Ressourcen auf der Site, mit der der Benutzer derzeit verbunden ist.
--disableFromHome	(Optional) Deaktiviert die --fromHome-Funktion für die globale Berechtigung.
--multipleSessionAutoClean	(Optional) Meldet zusätzliche Benutzersitzungen für dieselbe Berechtigung ab. Mehrere Sitzungen sind möglich, wenn ein Pod, der eine Sitzung enthält, offline geschaltet wird, der Benutzer sich erneut anmeldet und eine andere Sitzung startet und der problematische Pod wieder mit der ursprünglichen Sitzung online geschaltet wird. Wenn mehrere Sitzungen vorhanden sind, fordert Horizon Client den Benutzer auf, eine Sitzung auszuwählen. Diese Option legt fest, was mit Sitzungen passiert, die der Benutzer nicht auswählt. Wenn Sie diese Option nicht angeben, müssen die Benutzer ihre eigenen zusätzlichen Sitzungen durch Abmeldung im Horizon Client oder durch Start der Sitzungen und deren Abmeldung manuell beenden.
--disableMultipleSessionAutoClean	(Optional) Deaktiviert die --multipleSessionAutoClean-Funktion für die globale Berechtigung.

Tabelle 5-9. Optionen zum Ändern von globalen Berechtigungen (Fortsetzung)

Option	Beschreibung
<code>--multipleSessionsPerUser</code>	(Optional) Aktiviert die Richtlinie für mehrere Sitzungen pro Benutzer, mit der Benutzer separate Desktop-Sitzungen von unterschiedlichen Clientgeräten aus initiieren können. Benutzer, die eine Verbindung mit der globalen Desktop-Berechtigung von unterschiedlichen Clientgeräten aus herstellen, werden mit unterschiedlichen Desktop-Sitzungen verbunden. Um erneut eine Verbindung mit einer vorhandenen Desktop-Sitzung herzustellen, müssen Benutzer das Gerät verwenden, von dem aus die Sitzung initiiert wurde. Wenn Sie diese Richtlinie nicht aktivieren, werden Benutzer immer erneut mit ihren vorhandenen Desktop-Sitzungen verbunden, unabhängig vom verwendeten Clientgerät. Gilt nur für dynamische Desktop-Berechtigungen.
<code>--disableMultipleSessionsPerUser</code>	(Optional) Deaktiviert die Richtlinie für mehrere Sitzungen pro Benutzer für die globale Desktop-Berechtigung.
<code>--requireHomeSite</code>	(Optional) Bewirkt, dass die globale Berechtigung nur dann verfügbar ist, wenn der Benutzer eine Start-Site besitzt. Diese Option ist nur dann anwendbar, wenn auch die Option <code>--fromHome</code> angegeben wird.
<code>--disableRequireHomeSite</code>	(Optional) Deaktiviert die <code>--requireHomeSite</code> -Funktion für die globale Berechtigung.
<code>--defaultProtocol</code>	(Optional) Legt ein Standardanzeigeprotokoll für Desktops oder Anwendungen in der globalen Berechtigung fest. Zulässig sind die Werte RDP, PCoIP sowie BLAST für globale Desktop-Berechtigungen und PCoIP sowie BLAST für globale Anwendungsberechtigungen.
<code>--htmlAccess</code>	(Optional) Aktiviert die HTML Access-Richtlinie, mit der Benutzer die HTML Access-Funktion für den Zugriff auf Ressourcen in der globalen Berechtigung verwenden können. Bei HTML Access können Endbenutzer mithilfe eines Webbrowsers auf Remote-Ressourcen zugreifen und müssen keine Clientsoftware auf ihren lokalen Systemen installieren.
<code>--disableHtmlAccess</code>	(Optional) Deaktiviert die HTML Access-Richtlinie für die globale Berechtigung.
<code>--appVersion</code>	(Optional) Version der Anwendung. Gilt nur für globale Anwendungsberechtigungen.
<code>--appPublisher</code>	(Optional) Veröffentlicher der Anwendung. Gilt nur für globale Anwendungsberechtigungen.
<code>--appPath</code>	(Optional) Kompletter Pfadname der Anwendung, z. B. C:\Program Files\app1.exe. Gilt nur für globale Anwendungsberechtigungen.
<code>--tags</code>	(Optional) Legt ein oder mehrere Kennzeichen fest, mit denen der Zugriff auf globale Berechtigungen von Verbindungsserver-Instanzen aus eingeschränkt wird. Wenn Sie mehrere Kennzeichen angeben möchten, geben Sie eine Liste der Kennzeichen in Anführungszeichen ein. Die Kennzeichen müssen durch ein Komma oder durch ein Semikolon getrennt sein. Weitere Informationen finden Sie unter Implementieren von Verbindungsserver-Einschränkungen für globale Berechtigungen .

Tabelle 5-9. Optionen zum Ändern von globalen Berechtigungen (Fortsetzung)

Option	Beschreibung
--notags	(Optional) Entfernt Kennzeichen aus der globalen Berechtigung.
--preLaunch	(Optional) Aktiviert die Richtlinie für den Vorabstart, die die Anwendungssitzung startet, bevor ein Benutzer die globale Anwendungsberechtigung in Horizon Client öffnet. Wenn Sie die Richtlinie für den Vorabstart aktivieren, können Benutzer die globale Anwendungsberechtigung schneller starten. Alle Anwendungspools in der globalen Anwendungsberechtigung müssen die Funktion für den Vorabstart der Sitzung unterstützen, und die Zeitüberschreitung für die vorab gestartete Sitzung muss für alle Farmen identisch sein.
--disablePreLaunch	(Optional) Deaktiviert die Richtlinie für den Vorabstart für die globale Anwendungsberechtigung.
--categoryFolder	(Optional) Legt den Namen des Kategorienordners fest, der eine Verknüpfung für die globale Berechtigung auf Clientgeräten enthält. Sie können bis zu vier Ordnebenen konfigurieren. Ein Ordnername darf bis zu 64 Zeichen enthalten. Geben Sie einen umgekehrten Schrägstrich (\) ein, z. B. dir1\dir2\dir3\dir4, um einen Unterordner anzugeben. Sie können bis zu vier Ordnebenen eingeben. Sie können einen Ordnernamen nicht mit einem umgekehrten Schrägstrich beginnen oder beenden und auch nicht zwei oder mehr umgekehrte Schrägstriche kombinieren. Beispielsweise sind \dir1, dir1\dir2\, dir1\\dir2 und dir1\\\dir2 ungültig. Sie können keine für Windows reservierten Schlüsselwörter eingeben. Sie müssen auch die --shortcutLocations-Option angeben, um den Speicherort der Verknüpfung auf einem Windows-Clientgerät anzugeben. Weitere Informationen finden Sie unter Konfigurieren von Verknüpfungen für globale Berechtigungen .
--disableCategoryFolder	(Optional) Entfernt den Kategorienordner für die globale Berechtigung.
--clientRestrictions	(Optional) Aktiviert die Clienteinschränkungsrichtlinie, die den Zugriff auf die globale Berechtigung auf bestimmte Clientcomputer einschränkt. Weitere Informationen finden Sie unter Implementieren von Clienteinschränkungen für globale Berechtigungen .
--disableClientRestrictions	(Optional) Deaktiviert die Client-Einschränkungsrichtlinie für die globale Berechtigung.
--collaboration	(Optional) Aktiviert die Session Collaboration-Richtlinie, die es Benutzern von Remote-Desktop-Sitzungen ermöglicht, andere Benutzer zur Teilnahme an ihren Sitzungen einzuladen. Alle Desktop-Pools in der globalen Desktop-Berechtigung müssen die Funktion „Session Collaboration“ unterstützen. Gilt nur für globale Desktop-Berechtigungen.
--disableCollaboration	(Optional) Deaktiviert die Session Collaboration-Richtlinie für die globale Desktop-Berechtigung.

Tabelle 5-9. Optionen zum Ändern von globalen Berechtigungen (Fortsetzung)

Option	Beschreibung
--shortcutLocations	<p>(Optional) Verwenden Sie diese Option, um eine Verknüpfung auf dem Clientgerät zu ändern oder zu erstellen. Gültige Werte sind <code>desktop</code>, wodurch die Verknüpfung auf dem Desktop erstellt wird, und <code>launcher</code>, wodurch die Verknüpfung im Startmenü von Windows erstellt wird. Sie können auch beides angeben, <code>desktop</code> und <code>launcher</code>, durch Kommas getrennt, um damit eine Desktop-Verknüpfung und eine Verknüpfung mit dem Windows-Startmenü zu erstellen.</p> <p>Wenn Sie eine Verknüpfung ändern (d. h. der Kategorienordner bereits erstellt wurde), müssen Sie die <code>--categoryFolder</code>-Option nicht angeben, es sei denn, Sie möchten auch den Namen des Kategorienordners ändern.</p> <p>Wenn der Kategorienordner noch nicht erstellt wurde, müssen Sie die <code>--categoryFolder</code>-Option zusammen mit der <code>--shortcutLocations</code>-Option angeben.</p> <p>Hinweis Verwenden Sie diese Option nicht mit der <code>--disableCategoryFolder</code>-Option.</p>
--multiSessionMode	<p>(Optional) Konfiguriert die Funktion „Mehrfachsitzungsmodus“ für die globale Anwendungsberechtigung. Geben Sie einen der folgenden Werte an: <code>DISABLED</code>, <code>ENABLED_DEFAULT_OFF</code>, <code>ENABLED_DEFAULT_ON</code> oder <code>ENABLED_ENFORCED</code>. Weitere Informationen finden Sie unter Aktivieren des Mehrfachsitzungsmodus für globale Anwendungsberechtigungen.</p>
--backupEntitlementName	<p>(Optional) Gibt den Namen einer globalen Sicherungsberechtigung an. Eine globale Sicherungsberechtigung stellt Remote-Desktops oder veröffentlichte Anwendungen bereit, wenn mit der primären globalen Berechtigung keine Sitzung gestartet werden kann. Für globale Desktop-Berechtigungen muss der Benutzerzuweisungstyp „Dynamisch“ festgelegt sein. Weitere Informationen finden Sie unter Implementieren von globalen Sicherungsberechtigungen.</p>
--disableBackupEntitlement	<p>(Optional) Deaktiviert die globale Sicherungsberechtigung.</p>
--displayAssignedHostName	<p>(Optional) Zeigt in Horizon Client anstelle des Namens der globalen Berechtigung den Hostnamen der Maschine an, die dem Benutzer zugewiesen ist. Gilt nur für dedizierte Desktop-Berechtigungen.</p>
--disableDisplayAssignedHostName	<p>(Optional) Gibt an, dass der Hostname der zugewiesenen Maschine in Horizon Client nicht angezeigt wird. Gilt nur für dedizierte Desktop-Berechtigungen.</p>

Beispiele

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

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

Löschen einer globalen Berechtigung

Zum Löschen einer globalen Desktop-Berechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--deleteGlobalEntitlement`. Zum Löschen einer globalen Anwendungsberechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--deleteGlobalApplicationEntitlement`.

Syntax

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

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

Verwendung des Befehls

Diese Befehle geben eine Fehlermeldung zurück, wenn die angegebene globale Berechtigung nicht vorhanden ist, die Funktion Cloud-Pod-Architektur nicht initialisiert ist oder wenn die Befehle die globale Berechtigung nicht löschen können.

Optionen

Mit der Option `--entitlementName` geben Sie den Namen der zu löschenden globalen Berechtigung an.

Beispiele

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

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

Hinzufügen eines Pools zu einer globalen Berechtigung

Verwenden Sie den `lmvutil`-Befehl mit der `--addPoolAssociation`-Option, um einen Desktop-Pool einer globalen Desktop-Berechtigung oder einen Anwendungspool einer globalen Anwendungsberechtigung hinzuzufügen.

Syntax

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

Nutzungshinweise

Dieser Befehl muss auf einer Verbindungsserver-Instanz in dem Pod verwendet werden, der den Pool enthält. Wenn beispielsweise „Pod 1“ einen Desktop-Pool enthält, der einer globalen Desktop-Berechtigung zugewiesen werden soll, müssen Sie diesen Befehl auf einer Verbindungsserver-Instanz in „Pod 1“ ausführen.

Wiederholen Sie diesen Befehl für jeden Pool, der Teil der globalen Berechtigung werden soll. Ein bestimmter Pool kann nur einer globalen Berechtigung hinzugefügt werden.

Wichtig Wenn Sie mehrere Anwendungspools einer globalen Anwendungsberechtigung hinzufügen, müssen Sie jeweils dieselbe Anwendung hinzufügen. Beispielsweise sollten Sie nicht den Rechner und Microsoft Office PowerPoint derselben globalen Anwendungsberechtigung hinzufügen. Wenn Sie unterschiedliche Anwendungen hinzufügen, kann es zu unvorhersehbaren Situationen kommen, indem etwa berechtigte Benutzer unterschiedliche Anwendungen zu unterschiedlichen Zeitpunkten erhalten.

Dieser Befehl gibt eine Fehlermeldung zurück, wenn die Funktion Cloud-Pod-Architektur nicht initialisiert ist, wenn die angegebene Berechtigung nicht vorhanden ist, wenn der Pool bereits mit der angegebenen Berechtigung verknüpft ist, wenn der Pool nicht vorhanden ist oder wenn der Befehl den Pool nicht zu der globalen Berechtigung hinzufügen kann.

Optionen

Sie können diese Optionen angeben, wenn Sie einen Pool einer globalen Berechtigung hinzufügen.

Tabelle 5-10. Optionen zum Hinzufügen eines Pools zu einer globalen Berechtigung

Option	Beschreibung
<code>--entitlementName</code>	Der Name der globalen Berechtigung.
<code>--poolId</code>	ID des Pools, der zu der globalen Berechtigung hinzugefügt werden soll. Die Pool-ID muss dem Namen des Pools entsprechen, der im Pod angezeigt wird.

Beispiel

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

Entfernen eines Pools aus einer globalen Berechtigung

Verwenden Sie den `lmvutil`-Befehl mit der `--removePoolAssociation`-Option, um einen Desktop-Pool aus einer globalen Desktop-Berechtigung oder einen Anwendungspool aus einer globalen Anwendungsberechtigung zu entfernen.

Syntax

```
lmvutil --removePoolAssociation --entitlementName name --poolId poolid
```

Nutzungshinweise

Dieser Befehl gibt eine Fehlermeldung zurück, wenn die Funktion Cloud-Pod-Architektur nicht initialisiert ist, wenn die angegebene globale Berechtigung oder der angegebene Pool nicht vorhanden ist oder wenn der Befehl den Pool nicht aus der globalen Berechtigung entfernen kann.

Optionen

Sie können diese Optionen angeben, wenn Sie einen Pool aus einer globalen Berechtigung entfernen.

Tabelle 5-11. Optionen zum Entfernen eines Pools aus einer globalen Berechtigung

Option	Beschreibung
<code>--entitlementName</code>	Der Name der globalen Berechtigung.
<code>--poolId</code>	ID des Pools, der aus der globalen Berechtigung entfernt werden soll. Die Pool-ID muss dem Namen des Pools entsprechen, der im Pod angezeigt wird.

Beispiel

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

Hinzufügen eines Benutzers oder einer Gruppe zu einer globalen Berechtigung

Zum Hinzufügen eines Benutzers zu einer globalen Berechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--addUserEntitlement`. Zum Hinzufügen einer Gruppe zu einer globalen Berechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--addGroupEntitlement`.

Syntax

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

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

Nutzungshinweise

Wiederholen Sie diese Befehle für jeden Benutzer oder jede Gruppe, der bzw. die zur globalen Berechtigung hinzugefügt werden soll.

Wenn Sie eine Berechtigung, einen Benutzer oder eine Gruppe angeben, die bzw. der nicht existiert, oder wenn die Befehle den Benutzer oder die Gruppe nicht zur Berechtigung hinzufügen können, wird eine Fehlermeldung zurückgegeben.

Optionen

Sie können diese Optionen angeben, wenn Sie einer globalen Berechtigung einen Benutzer oder eine Gruppe hinzufügen.

Tabelle 5-12. Optionen beim Hinzufügen eines Benutzers oder einer Gruppe zu einer globalen Berechtigung

Option	Beschreibung
<code>--userName</code>	Name eines Benutzers, der zu der globalen Berechtigung hinzugefügt werden soll. Verwenden Sie das Format <i>Domäne\Benutzername</i> .
<code>--groupName</code>	Name einer Gruppe, die zu der globalen Berechtigung hinzugefügt werden soll. Verwenden Sie das Format <i>Domäne\Gruppenname</i> .
<code>--entitlementName</code>	Name der globalen Berechtigung, zu der der Benutzer oder die Gruppe hinzugefügt werden soll.

Beispiele

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

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

Entfernen eines Benutzers oder einer Gruppe aus einer globalen Berechtigung

Zum Entfernen eines Benutzers aus einer globalen Berechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--removeUserEntitlement`. Zum Entfernen einer Gruppe aus einer globalen Berechtigung verwenden Sie den Befehl `lmvutil` mit der Option `--removeGroupEntitlement`.

Syntax

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

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

Nutzungshinweise

Diese Befehle geben eine Fehlermeldung zurück, wenn die Funktion Cloud-Pod-Architektur nicht initialisiert wurde, wenn der angegebene Benutzername oder Gruppenname oder die angegebene Berechtigung nicht vorhanden ist oder wenn der Befehl den Benutzer oder die Gruppe nicht aus der Berechtigung entfernen kann.

Optionen

Sie müssen diese Optionen angeben, wenn Sie einen Benutzer oder eine Gruppe aus einer globalen Berechtigung entfernen möchten.

Tabelle 5-13. Optionen zum Entfernen eines Benutzers oder einer Gruppe aus einer globalen Berechtigung

Option	Beschreibung
--userName	Name eines Benutzers, der aus der globalen Berechtigung entfernt werden soll. Verwenden Sie das Format <i>Domäne\Benutzername</i> .
--groupName	Name einer Gruppe, die aus der globalen Berechtigung entfernt werden soll. Verwenden Sie das Format <i>Domäne\Gruppenname</i> .
--entitlementName	Namen der globalen Berechtigung, aus der der Benutzer oder die Gruppe entfernt werden soll.

Beispiele

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

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

Verwalten von Start-Sites

Mit den Optionen des Befehls `lmvutil` können Sie Start-Sites erstellen, ändern, löschen und auflisten.

■ Konfigurieren einer Start-Site

Zum Erstellen einer Start-Site für einen Benutzer verwenden Sie den Befehl `lmvutil` mit der Option `--createUserHomeSite`. Zum Erstellen einer Start-Site für eine Gruppe verwenden Sie den Befehl `lmvutil` mit der Option `--createGroupHomeSite`. Weiterhin können Sie diese Optionen verwenden, um eine Start-Site einer globalen Desktop-Berechtigung oder einer globalen Anwendungsberechtigung zuzuweisen.

■ Löschen einer Start-Site

Um die Zuweisung eines Benutzers zu einer Start-Site zu entfernen, verwenden Sie den Befehl `lmvutil` mit `--deleteUserHomeSite`-Option. Um die Zuweisung einer Gruppe zu einer Start-Site zu entfernen, verwenden Sie den Befehl `lmvutil` mit `--deleteGroupHomeSite`-Option.

Konfigurieren einer Start-Site

Zum Erstellen einer Start-Site für einen Benutzer verwenden Sie den Befehl `lmvutil` mit der Option `--createUserHomeSite`. Zum Erstellen einer Start-Site für eine Gruppe verwenden Sie den Befehl `lmvutil` mit der Option `--createGroupHomeSite`. Weiterhin können Sie diese Optionen verwenden, um eine Start-Site einer globalen Desktop-Berechtigung oder einer globalen Anwendungsberechtigung zuzuweisen.

Syntax

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

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

Nutzungshinweise

Sie müssen eine Site erstellen, bevor Sie sie als Start-Site konfigurieren können. Siehe [Erstellen einer Site](#).

Diese Befehle geben eine Fehlermeldung zurück, wenn die Funktion Cloud-Pod-Architektur nicht initialisiert ist, der angegebene Benutzer, die angegebene Gruppe, die angegebene Site oder die angegebene Berechtigung nicht vorhanden ist oder wenn die Befehle die Start-Site nicht erstellen können.

Optionen

Sie können diese Optionen beim Erstellen einer Start-Site für einen Benutzer oder eine Gruppe angeben.

Tabelle 5-14. Optionen zum Erstellen einer Start-Site für einen Benutzer oder eine Gruppe

Option	Beschreibung
--userName	Name des Benutzers, der mit der Start-Site verbunden werden soll. Verwenden Sie das Format <i>Domäne\Benutzername</i> .
--groupName	Name der Gruppe, die mit der Start-Site verbunden werden soll. Verwenden Sie das Format <i>Domäne\Gruppenname</i> .
--siteName	Name der Site, die mit dem Benutzer oder der Gruppe als die Start-Site verbunden werden soll.
--entitlementName	(Optional) Name einer globalen Desktop-Berechtigung oder einer globalen Anwendungsberechtigung, die mit der Start-Site verbunden werden soll. Wenn ein Benutzer die angegebene globale Berechtigung auswählt, hat die Start-Site Vorrang vor der eigenen Start-Site des Benutzers. Wenn Sie diese Option nicht angeben, wird mit diesem Befehl eine globale Start-Site für den Benutzer oder die Gruppe erstellt.

Beispiele

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

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

Löschen einer Start-Site

Um die Zuweisung eines Benutzers zu einer Start-Site zu entfernen, verwenden Sie den Befehl `lmvutil` mit `--deleteUserHomeSite`-Option. Um die Zuweisung einer Gruppe zu einer Start-Site zu entfernen, verwenden Sie den Befehl `lmvutil` mit `--deleteGroupHomeSite`-Option.

Syntax

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

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

Nutzungshinweise

Wenn der angegebene Benutzer, die angegebene Gruppe oder die angegebene globale Berechtigung nicht existiert oder wenn die Befehle die Einstellung für die Start-Site nicht löschen können, wird eine Fehlermeldung zurückgegeben.

Optionen

Sie können diese Optionen angeben, wenn Sie die Zuweisung zwischen einem Benutzer oder einer Gruppe und einer Start-Site aufheben.

Tabelle 5-15. Optionen zum Löschen einer Start-Site

Option	Beschreibung
<code>--userName</code>	Name eines Benutzers. Verwenden Sie das Format <i>Domäne\Benutzername</i> .
<code>--groupName</code>	Name einer Gruppe. Verwenden Sie das Format <i>Domäne\Gruppenname</i> .
<code>--entitlementName</code>	(Optional) Name einer globalen Desktop- oder Anwendungsberechtigung. Mit dieser Option können Sie die Zuweisung zwischen der Start-Site und einer globalen Berechtigung für den angegebenen Benutzer oder die angegebene Gruppe aufheben.

Beispiele

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

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


Anzeigen einer Cloud-Pod-Architektur-Konfiguration

Mit den Optionen des Befehls `lmvutil` können Sie Informationen über die Cloud-Pod-Architektur-Konfiguration auflisten.

- **Auflisten von globalen Berechtigungen**

Für die Auflistung der Informationen zu allen globalen Desktop-Berechtigungen, inklusive ihrer Richtlinien und Attribute, verwenden Sie den Befehl `lmvutil` mit der Option `--listGlobalEntitlements`. Für die Auflistung der Informationen zu allen globalen Anwendungsberechtigungen, inklusive ihrer Richtlinien und Attribute, verwenden Sie den Befehl `lmvutil` mit der Option `--listGlobalApplicationEntitlements`.

- **Auflisten der Pools in einer globalen Berechtigung**

Verwenden Sie den Befehl `lmvutil` mit der Option `--listAssociatedPools`, um die Desktop- oder Anwendungspools aufzulisten, die zu einer bestimmten globalen Berechtigung gehören.

- **Auflisten der Benutzer oder Gruppen in einer globalen Berechtigung**

Verwenden Sie den Befehl `lmvutil` mit der Option `--listEntitlements`, um alle Benutzer oder Gruppen aufzulisten, die zu einer bestimmten globalen Berechtigung gehören.

- **Auflisten der Start-Sites für einen Benutzer oder eine Gruppe**

Zum Auflisten aller konfigurierten Start-Sites für einen bestimmten Benutzer verwenden Sie den Befehl `lmvutil` mit der Option `--showUserHomeSites`. Zum Auflisten aller konfigurierten Start-Sites für eine bestimmte Gruppe verwenden Sie den Befehl `lmvutil` mit der Option `--showGroupHomeSites`.

- **Auflisten der geltenden Start-Site für einen Benutzer**

Verwenden Sie den Befehl `lmvutil` mit der Option `--resolveUserHomeSite`, um die geltende Start-Site für einen bestimmten Benutzer zu bestimmen. Da Start-Sites Benutzern, Gruppen und globalen Berechtigungen zugewiesen werden können, ist es möglich, mehr als eine Start-Site für einen bestimmten Benutzer zu konfigurieren.

- **Auflisten von dedizierten Desktop-Pool-Zuweisungen**

Verwenden Sie den Befehl `lmvutil` mit der Option `--listUserAssignments`, um die dedizierten Desktop-Pool-Zuweisungen für eine Kombination von Benutzer und globaler Berechtigung aufzulisten.

- **Auflisten der Pods oder Sites in einer Cloud-Pod-Architektur-Topologie**

Zum Anzeigen der Pods im Pod-Verbund verwenden Sie den Befehl `lmvutil` mit der Option `--listPods`. Zum Anzeigen der Sites im Pod-Verbund verwenden Sie den Befehl `lmvutil` mit der Option `--listSites`.

Auflisten von globalen Berechtigungen

Für die Auflistung der Informationen zu allen globalen Desktop-Berechtigungen, inklusive ihrer Richtlinien und Attribute, verwenden Sie den Befehl `lmvutil` mit der Option

`--listGlobalEntitlements`. Für die Auflistung der Informationen zu allen globalen Anwendungsberechtigungen, inklusive ihrer Richtlinien und Attribute, verwenden Sie den Befehl `lmvutil` mit der Option `--listGlobalApplicationEntitlements`.

Syntax

```
lmvutil --listGlobalEntitlements
```

```
lmvutil --listGlobalApplicationEntitlements
```

Nutzungshinweise

Diese Befehle geben eine Fehlermeldung zurück, wenn die Cloud-Pod-Architektur-Funktion nicht initialisiert ist oder wenn die Befehle die globalen Berechtigungen nicht auflisten kann.

Beispiele

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

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

Auflisten der Pools in einer globalen Berechtigung

Verwenden Sie den Befehl `lmvutil` mit der Option `--listAssociatedPools`, um die Desktop- oder Anwendungspools aufzulisten, die zu einer bestimmten globalen Berechtigung gehören.

Syntax

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

Nutzungshinweise

Dieser Befehl gibt eine Fehlermeldung zurück, wenn die Cloud-Pod-Architektur-Funktion nicht initialisiert ist oder wenn die angegebene globale Berechtigung nicht vorhanden ist.

Optionen

Mit der Option `--entitlementName` geben Sie den Namen der globalen Berechtigung an, deren zugewiesene Desktop- oder Anwendungspools aufgelistet werden sollen.

Beispiel

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

Auflisten der Benutzer oder Gruppen in einer globalen Berechtigung

Verwenden Sie den Befehl `lmvutil` mit der Option `--listEntitlements`, um alle Benutzer oder Gruppen aufzulisten, die zu einer bestimmten globalen Berechtigung gehören.

Syntax

```
lmvutil --listEntitlements [--userName domain\username | --groupName domain\groupname | --entitlementName name]
```

Nutzungshinweise

Dieser Befehl gibt eine Fehlermeldung zurück, wenn die Funktion Cloud-Pod-Architektur nicht initialisiert ist oder wenn der angegebene Benutzer, die angegebene Gruppe oder die globale Berechtigung nicht vorhanden ist.

Optionen

Sie können diese Optionen beim Auflisten der zugewiesenen globalen Berechtigungen angeben.

Tabelle 5-16. Optionen zum Auflisten der zugewiesenen globalen Berechtigungen

Option	Beschreibung
<code>--userName</code>	Der Name des Benutzers, für den Sie globale Berechtigungen auflisten möchten. Verwenden Sie das Format <i>Domäne\Benutzername</i> . Diese Option listet alle globalen Berechtigungen für den angegebenen Benutzer auf.
<code>--groupName</code>	Der Name der Gruppe, für die Sie globale Berechtigungen auflisten möchten. Verwenden Sie das Format <i>Domäne\Gruppenname</i> . Diese Option listet alle globalen Berechtigungen für die angegebene Gruppe auf.
<code>--entitlementName</code>	Der Name einer globalen Berechtigung. Diese Option listet alle Benutzer und Gruppen in der angegebenen globalen Berechtigung auf.

Beispiel

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

Auflisten der Start-Sites für einen Benutzer oder eine Gruppe

Zum Auflisten aller konfigurierten Start-Sites für einen bestimmten Benutzer verwenden Sie den Befehl `lmvutil` mit der Option `--showUserHomeSites`. Zum Auflisten aller konfigurierten Start-Sites für eine bestimmte Gruppe verwenden Sie den Befehl `lmvutil` mit der Option `--showGroupHomeSites`.

Syntax

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

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

Nutzungshinweise

Diese Befehle geben eine Fehlermeldung zurück, wenn die Funktion Cloud-Pod-Architektur nicht initialisiert ist oder wenn der angegebene Benutzer, die angegebene Gruppe oder die globale Berechtigung nicht vorhanden ist.

Optionen

Sie können diese Optionen beim Auflisten der Start-Sites für einen Benutzer oder eine Gruppe angeben.

Tabelle 5-17. Optionen zum Auflisten der Start-Sites für einen Benutzer oder eine Gruppe

Option	Beschreibung
<code>--userName</code>	Name eines Benutzers. Verwenden Sie das Format <i>Domäne\Benutzername</i> .
<code>--groupName</code>	Name einer Gruppe. Verwenden Sie das Format <i>Domäne\Gruppenname</i> .
<code>--entitlementName</code>	(Optional) Name einer globalen Berechtigung. Verwenden Sie diese Option, wenn Sie die Start-Sites für eine Kombination aus Benutzer oder Gruppe und globaler Berechtigung anzeigen möchten.

Beispiel

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

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

Auflisten der geltenden Start-Site für einen Benutzer

Verwenden Sie den Befehl `lmvutil` mit der Option `--resolveUserHomeSite`, um die geltende Start-Site für einen bestimmten Benutzer zu bestimmen. Da Start-Sites Benutzern, Gruppen und globalen Berechtigungen zugewiesen werden können, ist es möglich, mehr als eine Start-Site für einen bestimmten Benutzer zu konfigurieren.

Syntax

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

Nutzungshinweise

Dieser Befehl gibt eine Fehlermeldung zurück, wenn die Cloud-Pod-Architektur-Funktion nicht initialisiert ist oder wenn die angegebene globale Berechtigung oder der Benutzer nicht vorhanden ist.

Optionen

Sie müssen diese Optionen angeben, wenn Sie die geltende Start-Site für einen Benutzer auflisten.

Tabelle 5-18. Optionen zum Auflisten der geltenden Start-Site für einen Benutzer

Option	Beschreibung
<code>--entitlementName</code>	Der Name einer globalen Berechtigung. Mit dieser Option können Sie die geltende Start-Site für eine bestimmte Kombination aus Benutzer und globaler Berechtigung bestimmen, die sich von der Start-Site unterscheiden kann, die für den Benutzer konfiguriert ist.
<code>--userName</code>	Name des Benutzers, dessen Start-Site Sie auflisten möchten. Verwenden Sie das Format <i>Domäne\Benutzername</i> .

Beispiel

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

Auflisten von dedizierten Desktop-Pool-Zuweisungen

Verwenden Sie den Befehl `lmvutil` mit der Option `--listUserAssignments`, um die dedizierten Desktop-Pool-Zuweisungen für eine Kombination von Benutzer und globaler Berechtigung aufzulisten.

Syntax

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

Nutzungshinweise

Die von diesem Befehl erzeugten Daten werden intern von der Cloud-Pod-Architektur-Brokering-Software verwaltet.

Dieser Befehl gibt einen Fehler zurück, wenn die Funktion Cloud-Pod-Architektur nicht initialisiert wurde oder wenn der Befehl den angegebenen Benutzer, die globale Berechtigung, den Pod oder die Site nicht finden kann.

Optionen

Sie müssen eine der folgenden Optionen angeben, wenn Sie Benutzerzuweisungen auflisten.

Tabelle 5-19. Optionen zum Auflisten von Benutzerzuweisungen

Option	Beschreibung
<code>--userName</code>	Der Name des Benutzers, für den Sie Zuweisungen auflisten möchten. Verwenden Sie das Format <i>Domäne\Benutzername</i> . Diese Option listet die globale Berechtigung, den Pod und die Sitezuweisungen für den angegebenen Benutzer auf.
<code>--entitlementName</code>	Der Name einer globalen Berechtigung. Diese Option listet die der angegebenen globalen Berechtigung zugewiesenen Benutzer auf.

Tabelle 5-19. Optionen zum Auflisten von Benutzerzuweisungen (Fortsetzung)

Option	Beschreibung
<code>--podName</code>	Der Name eines Pods. Diese Option listet die dem angegebenen Pod zugewiesenen Benutzer auf.
<code>--siteName</code>	Der Name einer Site. Diese Option listet die der angegebenen Site zugewiesenen Benutzer auf.

Beispiel

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

Auflisten der Pods oder Sites in einer Cloud-Pod-Architektur-Topologie

Zum Anzeigen der Pods im Pod-Verbund verwenden Sie den Befehl `lmvutil` mit der Option `--listPods`. Zum Anzeigen der Sites im Pod-Verbund verwenden Sie den Befehl `lmvutil` mit der Option `--listSites`.

Syntax

```
lmvutil --listPods
```

```
lmvutil --listSites
```

Nutzungshinweise

Diese Befehle geben eine Fehlermeldung zurück, wenn die Funktion Cloud-Pod-Architektur nicht initialisiert wurde oder die Befehle die Pods oder Sites nicht auflisten können.

Beispiel

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

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

Verwalten von SSL-Zertifikaten

Sie können die Optionen des Befehls `lmvutil` verwenden, um ausstehende SSL-Zertifikate in einer Cloud-Pod-Architektur-Umgebung zu erstellen und zu aktivieren.

Die Funktion Cloud-Pod-Architektur verwendet signierte Zertifikate für bidirektionales SSL, um den VIPA-Kommunikationskanal zu schützen und zu validieren. Die Zertifikate werden in der globalen Datenschicht verteilt. Die Funktion Cloud-Pod-Architektur ersetzt diese Zertifikate alle sieben Tage.

Erstellen Sie zum Ändern eines Zertifikats für eine bestimmte Verbindungsserver-Instanz ein ausstehendes Zertifikat, warten Sie darauf, dass der Replikationsprozess der globalen Datenschicht das Zertifikat an alle Verbindungsserver-Instanzen verteilt, und aktivieren Sie das Zertifikat.

Die Zertifikatoptionen des Befehls `lmvutil` sind nur für Fälle vorgesehen, in denen ein Zertifikat beschädigt wird und der Horizon-Administrator das Zertifikat bereits vor Ablauf der sieben Tage aktualisieren möchte. Diese Optionen wirken sich nur auf die Verbindungsserver-Instanz aus, auf der sie ausgeführt werden. Wenn Sie alle Zertifikate ändern möchten, müssen Sie die Optionen auf allen Verbindungsserver-Instanzen ausführen.

- **Erstellen eines ausstehenden Zertifikats**

Verwenden Sie den Befehl `lmvutil` mit der Option `--createPendingCertificate`, um ein ausstehendes SSL-Zertifikat zu erstellen.

- **Aktivieren eines ausstehenden Zertifikats**

Aktivieren Sie ein ausstehendes Zertifikat unter Verwendung des Befehls `lmvutil` mit der Option `--activatePendingCertificate`.

Erstellen eines ausstehenden Zertifikats

Verwenden Sie den Befehl `lmvutil` mit der Option `--createPendingCertificate`, um ein ausstehendes SSL-Zertifikat zu erstellen.

Syntax

```
lmvutil --createPendingCertificate
```

Nutzungshinweise

Dieser Befehl gibt eine Fehlermeldung zurück, wenn die Funktion Cloud-Pod-Architektur nicht initialisiert ist oder wenn der Befehl das Zertifikat nicht erstellen kann.

Beispiel

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

Aktivieren eines ausstehenden Zertifikats

Aktivieren Sie ein ausstehendes Zertifikat unter Verwendung des Befehls `lmvutil` mit der Option `--activatePendingCertificate`.

Syntax

```
lmvutil --activatePendingCertificate
```

Nutzungshinweise

Bevor Sie diesen Befehl verwenden können, müssen Sie ein ausstehendes Zertifikat unter Verwendung des Befehls `lmvutil` mit der Option `--createPendingCertificate` erstellen. Bevor Sie das ausstehende Zertifikat aktivieren, warten Sie, bis der Replikationsprozess der globalen Datenschicht das Zertifikat an alle Verbindungsserver-Instanzen verteilt hat. VIPA-Verbindungsfehler und sich daraus ergebende Brokering-Probleme können auftreten, wenn Sie ein ausstehendes Zertifikat aktivieren, bevor es vollständig in alle Verbindungsserver-Instanzen repliziert wurde.

Dieser Befehl gibt eine Fehlermeldung zurück, wenn die Funktion Cloud-Pod-Architektur nicht initialisiert ist oder wenn der Befehl das Zertifikat nicht aktivieren kann.

Beispiel

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