

## Verwendung des Horizon vCenter Orchestrator-Plug-Ins

VMware Horizon 6 6.0



vmware®

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

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

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

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://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](http://www.vmware.com/de)

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

# Inhalt

Verwenden des Horizon vCenter Orchestrator-Plug-Ins	5
<b>1 Einführung in das Horizon vCenter Orchestrator-Plug-In</b>	<b>6</b>
Rolle des Horizon vCenter Orchestrator-Plug-Ins	7
Im Horizon vCenter Orchestrator-Plug-In verfügbare Funktionen	7
Architektur des Horizon vCenter Orchestrator-Plug-Ins	8
Horizon vCenter Orchestrator-Sicherheitsmodell	9
Für die Verwaltung von Arbeitsabläufen in verteilten Organisationen verwendete Personas	10
<b>2 Installation und Konfiguration des Horizon vCenter Orchestrator-Plug-Ins</b>	<b>11</b>
Funktionsvoraussetzungen für das Horizon vCenter Orchestrator-Plug-In	11
Das Horizon vCenter Orchestrator-Plug-In installieren oder aktualisieren	12
Konfigurationsaufgaben nach dem Upgrade	14
Konfigurieren der Verbindung mit einem View Pod	15
Aktualisieren der View Pod-Verbindungsinformationen	16
Zuweisen delegierter Administratoren zu Desktop- und Anwendungspools	16
Erstellen einer delegierten Administratorrolle mit vSphere Web Client	17
Festlegen von Zugriffsrechten für die Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins	18
Zuweisen delegierter Administratoren zu Pools	20
Empfohlene Vorgehensweisen für die Verwaltung von Arbeitsablaufberechtigungen	21
Festlegen einer Richtlinie für das Aufheben der Bereitstellung von virtuellen Desktop-Maschinen	22
<b>3 Verwenden der Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins</b>	<b>24</b>
Zugreifen auf die Arbeitsablaufbibliothek des Horizon vCenter Orchestrator-Plug-Ins	24
Arbeitsablaufbibliothek des Horizon vCenter Orchestrator-Plug-Ins	25
Arbeitsablaufreferenz für das Horizon vCenter Orchestrator-Plug-In	26
Syntax für die Angabe von Benutzerkonten in den Arbeitsabläufen	36
<b>4 Verfügbar machen der Arbeitsabläufe in vSphere Web Client und vCloud Automation Center</b>	<b>38</b>
Verfügbar machen der Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins in vSphere Web Client	38
Verknüpfen von vSphereWebClient-Arbeitsabläufen mit bestimmten Pods und Pools in vCenter Orchestrator	38
Erstellen lokalisierter Versionen eines Arbeitsablaufs für vSphere Web Client	40
Verfügbar machen der Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins in vCloud Automation Center	41
Erstellen von Unternehmensgruppen für delegierte Administratoren und Endbenutzer	43

Erstellen von Diensten für delegierte Administratoren und Endbenutzer	44
Erstellen von Berechtigungen für delegierte Administratoren und Endbenutzer	44
Verknüpfen von vCAC60-Arbeitsabläufen mit bestimmten Pods und Pools in vCloud Automation Center	46
vCAC61-Arbeitsabläufe mit einem vCAC-Benutzer verknüpfen	48
vCAC61-Self-Service-Arbeitsabläufe für die Verwendung bestimmter Pools konfigurieren	49
Ausgabeparameter für vCAC61-Arbeitsabläufe konfigurieren	51
Konfigurieren des Katalogelements für den Arbeitsablauf	52

## **5 Mit nicht verwalteten Maschinen arbeiten** 54

Voraussetzungen für das Hinzufügen von nicht verwalteten Maschinen zu Pools	54
Hinzufügen physischer Maschinen und nicht durch vSphere bereitgestellter virtueller Maschinen zu Pools	56
Konfiguration einer physischen Maschine für einen nicht verwalteten Pool	57
Konfiguration von vCenter Orchestrator für die Verwendung der Kerberos-Authentifizierung mit physischen Maschinen	59
Ausführen von Arbeitsabläufen zum Hinzufügen physischer Maschinen als PowerShell-Hosts	61

# Verwenden des Horizon vCenter Orchestrator-Plug-Ins

Unter *Verwenden des Horizon vCenter Orchestrator-Plug-Ins* werden das Einrichten und die ersten Schritte mit dem Horizon™-Plug-In für VMware® vCenter Orchestrator™ beschrieben. Mithilfe des Plug-Ins können IT-Organisationen VMware vCloud® Automation Center™ für die automatisierte Bereitstellung von Desktops und Anwendungen verwenden, die von VMware Horizon™ (mit View™) bereitgestellt werden.

## Zielgruppe

Diese Informationen sind für alle Personen gedacht, die das Plug-In installieren und konfigurieren oder die Bereitstellung von Desktops und Anwendungen mithilfe der Arbeitsablaufbibliothek automatisieren möchten. *Verwenden des Horizon vCenter Orchestrator-Plug-Ins* wurde für erfahrene Benutzer geschrieben, die mit der Technologie virtueller Maschinen, der Entwicklung von Orchestrator-Arbeitsabläufen und mit VMware Horizon 6 vertraut sind.

# Einführung in das Horizon vCenter Orchestrator-Plug-In

# 1

Das Horizon vCenter Orchestrator-Plug-In (vCO-Plug-In) ermöglicht die Interaktion zwischen vCenter Orchestrator und VMware Horizon 6. Mit diesem Plug-In können Sie die Einstellungen und Methoden erweitern, die Ihnen für die Bereitstellung von Remote-Desktops und -Anwendungen zur Verfügung stehen.

Das Plug-In enthält eine Reihe von Standardarbeitsabläufen für die Automatisierung, den Self-Service basierend auf einem Anforderungs- und Genehmigungsmodell sowie für die skalierbare delegierte Verwaltung in mandantenfähigen oder hochgradig verteilten Umgebungen. Sie können diese vordefinierten Arbeitsabläufe auch verwenden, um eigene Arbeitsabläufe zu erstellen.

Über die in diesem Dokument beschriebenen Arbeitsabläufe werden vordefinierte, automatisierte Aufgaben für grundlegende Vorgänge bereitgestellt, die normalerweise in View Administrator oder in anderen View-Schnittstellen durchgeführt werden. View-Administratoren können delegierten Administratoren und Endbenutzern den Zugriff auf bestimmte Arbeitsabläufe gewähren und so die IT-Effizienz optimieren.

Zur Unterstützung von Endbenutzern bietet das Horizon vCenter Orchestrator-Plug-In die Integration in vCloud Automation Center, sodass Endbenutzer Self-Service-Zugriff auf Anwendungen und Desktops erhalten. Die Plug-In-Arbeitsabläufe können in die Anforderungs- und Genehmigungsprozesse im Dienstkatalog von vCloud Automation Center integriert werden. Endbenutzer erhalten damit die Möglichkeit, ihre eigenen Desktops zu aktualisieren. Die Endbenutzer können Anforderungen stellen, die einem standardisierten und überprüfbaren Prozess folgen. In diesem Prozess kann entweder eine direkte Reaktion initiiert oder die Anforderung zur weiteren Genehmigung an zuständige Administratoren weitergeleitet werden. In Desktop-Umgebungen, in denen virtuelle Maschinen häufig verändert oder wiederverwendet werden müssen, können Endbenutzer nach Bedarf eigene Desktops bereitstellen, ihre Bereitstellungen aufheben oder Desktops wiederverwenden und auf diese Weise Ressourcen und Kapazitäten einsparen.

Das Horizon vCenter Orchestrator-Plug-In bietet einen gut organisierten und verwalteten Dienstkatalog, der entsprechenden Benutzern und Gruppen gezielt alle benötigten Funktionen bereitstellt, was die IT-Effizienz verbessert. Durch Automatisieren und Verteilen von Aufgaben an delegierte Administratoren wird der Umfang der erforderlichen E-Mail-Korrespondenz und Ausnahmebehandlungen verringert. Die Anforderungen werden in vordefinierten Prozessen verwaltet. Genehmigungen sind nur erforderlich, wenn eine Anforderung tatsächlich einer Prüfung bedarf. Durch diese standardisierten Kontrollen und Prozesse können Administratoren DaaS (Desktops-as-a-Service) mit einem effizienteren 1:n-Modell für die Benutzeradministration bereitstellen.

Dieses Kapitel enthält die folgenden Themen:

- [Rolle des Horizon vCenter Orchestrator-Plug-Ins](#)
- [Im Horizon vCenter Orchestrator-Plug-In verfügbare Funktionen](#)
- [Architektur des Horizon vCenter Orchestrator-Plug-Ins](#)
- [Horizon vCenter Orchestrator-Sicherheitsmodell](#)
- [Für die Verwaltung von Arbeitsabläufen in verteilten Organisationen verwendete Personas](#)

## Rolle des Horizon vCenter Orchestrator-Plug-Ins

Sie müssen die Orchestrator-Konfigurationsschnittstelle verwenden, um das Horizon vCenter Orchestrator-Plug-In zu installieren und zu konfigurieren. Mit dem Orchestrator-Client können Sie Arbeitsabläufe ausführen und erstellen und auf die Plug-In-API zugreifen.

Das Horizon vCenter Orchestrator-Plug-In verwendet vCenter Orchestrator als Basis. Orchestrator ist eine Plattform für die Entwicklung und Prozessautomatisierung, die eine Bibliothek mit erweiterbaren Arbeitsabläufen bereitstellt, mit denen die VMware vCenter-Infrastruktur und andere Technologien verwaltet werden können.

Orchestrator ermöglicht durch die offene Plug-In-Architektur die Integration mit Verwaltungs- und Administrationslösungen. VMware Horizon 6 ist ein Beispiel für eine Administrationslösung, die Sie mithilfe von Plug-Ins in Orchestrator integrieren können.

## Im Horizon vCenter Orchestrator-Plug-In verfügbare Funktionen

Das Horizon vCenter Orchestrator-Plug-In stellt Automatisierung, Self-Service und delegierte Verwaltung für View-Umgebungen bereit. Endbenutzer können Self-Service-Funktionen durchführen. Delegierte Administratoren können Bereitstellungsfunktionen für Endbenutzer durchführen.

Das Horizon vCenter Orchestrator-Plug-In bietet die folgenden Funktionen:

- Self-Service-Bereitstellung, Aufheben von Bereitstellungen und Wiederverwendung von Maschinen über vCloud Automation Center in vorhandenen View Desktop-Pools
- Self-Service-Anforderung und Berechtigung für Anwendungen über vCloud Automation Center
- Self-Service-Anforderung und Berechtigung für einen Desktop über vCloud Automation Center
- Self-Service-Aktualisierung einer virtuellen Maschine über vCloud Automation Center
- Bereitstellen einer virtuellen Maschine für einen Endbenutzer in einem vorhandenen Desktop-Pool
- Aufheben der Bereitstellung einer virtuellen Maschine für einen Endbenutzer und, sofern vorhanden, Beibehalten der dauerhaften Festplatte
- Ändern der Berechtigungen und Zuweisungen für Anwendungs- und Desktop-Pools

- Bearbeiten der Mindestanzahl an virtuellen Maschinen in einem Desktop-Pool, des Anzeigenamens für einen Desktop-Pool und der Anzahl der eingeschalteten virtuellen Maschinen

Mit dem Horizon vCenter Orchestrator-Plug-In wurden folgende Funktionen hinzugefügt:

- Verwaltete virtuelle Maschinen zu manuellen Desktop-Pools hinzufügen
- Nicht verwaltete virtuelle Maschinen zu nicht verwalteten Desktop-Pools hinzufügen
- Physische Maschinen zu nicht verwalteten manuellen Desktop-Pools hinzufügen
- Sitzungsverwaltung zum Trennen, Abmelden, Zurücksetzen und Senden von Nachrichten an aktive View Desktop-Sitzungen berechtigen
- Mehrere Maschinen für mehrere Benutzer bereitstellen
- Wartungsmodusvorgänge auf View-Maschinen durchführen

## Architektur des Horizon vCenter Orchestrator-Plug-Ins

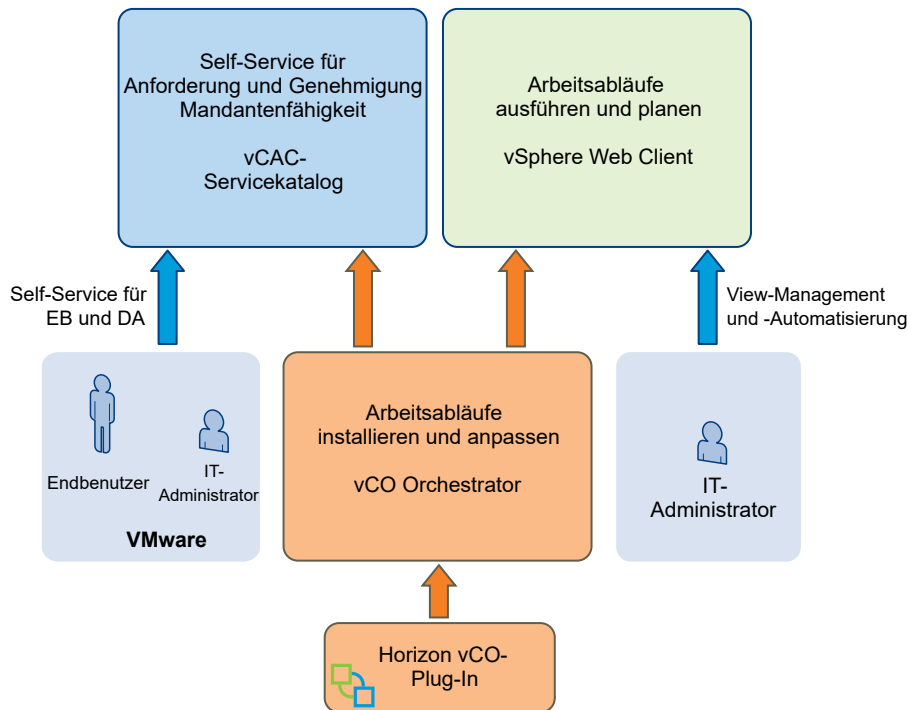
vCenter Orchestrator und vCloud Automation Center stellen die Architektur zur Unterstützung der Funktionen des Horizon vCenter Orchestrator-Plug-Ins bereit.

Das vCenter Orchestrator-Plug-In ermöglicht die nahtlose Automatisierung zwischen der Softwareumgebung, in der die Arbeitsabläufe ausgeführt werden, und den Produkten, mit denen die Arbeitsabläufe interagieren. Mit dem Horizon vCenter Orchestrator-Plug-In können Arbeitsabläufe systemintern bereitgestellt werden, sowohl in vSphere Web Client für delegierte Administratoren als auch im Dienstkatalog von vCloud Automation Center. Die Berechtigungsvergabe, Planung und Ausführung von Arbeitsabläufen werden in vSphere Web Client und vCloud Automation Center verfügbar gemacht. Anpassungen oder die Konfiguration von Arbeitsabläufen sind jedoch nur im vCenter Orchestrator-Client möglich.

Die folgende Abbildung veranschaulicht die Architektur des Horizon vCenter Orchestrator-Plug-Ins.



Abbildung 1-1. Architektur des Horizon vCenter Orchestrator-Plug-Ins



## Horizon vCenter Orchestrator-Sicherheitsmodell

Das Sicherheitsmodell des Horizon vCenter Orchestrator-Plug-Ins basiert auf vertrauenswürdigen Konten. Der Administrator stellt Anmeldeinformationen für die anfängliche Konfiguration des View Pods und des Plug-Ins bereit. Dieses vertrauenswürdige Konto bildet den Sicherheitskontext für alle Arbeitsablaufvorgänge zwischen vCenter Orchestrator und VMware Horizon 6.

Mithilfe zusätzlicher Berechtigungsebenen wird gesteuert, welche Benutzer Arbeitsabläufe in vCenter Orchestrator anzeigen oder bearbeiten können. Alle Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins müssen explizit für die Ausführung konfiguriert werden. Der Zugriff auf die Arbeitsabläufe ist nur möglich, wenn die erforderlichen Berechtigungen gewährt wurden und außerdem die Interaktion mit dem vCenter Orchestrator-Client ordnungsgemäß konfiguriert wurde.

Darüber hinaus ist eine dritte Sicherheitsebene in der Zugriffsschicht implementiert, die zwischen dem Ausführungsort von Arbeitsabläufen (in vCenter Orchestrator) und dem Ort der Anzeige bzw. Bearbeitung durch delegierte Administratoren und Endbenutzer (in vSphere Web Client und vCloud Automation Center) zur Anwendung kommt.

- Über die vCenter Single Sign-On-Implementierung können Administratoren den Zugriff und damit die Ausführung von Arbeitsabläufen durch Benutzer oder Gruppen in vSphere Web Client steuern.
- Über den Dienstkatalog und die Berechtigungsmechanismen in vCloud Automation Center können Administratoren festlegen, welche Arbeitsabläufe bestimmten Benutzern oder Gruppen verfügbar gemacht werden sollen.

## Für die Verwaltung von Arbeitsabläufen in verteilten Organisationen verwendete Personas

Die Personas für Administrator, delegierter Administrator und Endbenutzer beschreiben die verschiedenen für Einzelpersonen und Gruppen verfügbaren Rollen und Berechtigungen, wenn das Horizon vCenter Orchestrator-Plug-In implementiert ist. Organisationen können diese primären Rollen bei Bedarf weiter in geographische und funktionale Bereiche unterteilen.

### Administrator

Diese Persona umfasst die typische Administratorrolle. Zu den Aufgaben gehören Installation, Konfiguration und Zuweisung von anderen Personas zu Rollen und Berechtigungen. Diese Rolle ist verantwortlich für die verschiedenen Produkte, die Konfiguration und für die Implementierung der einmaligen Anmeldung (Single Sign-On, SSO). Der Administrator entscheidet, welche Benutzer auf die unterschiedlichen Arbeitsabläufe zugreifen dürfen und ob ein Arbeitsablauf in vSphere Web Client oder in vCloud Automation Center verfügbar sein soll. Bei diesen Entscheidungen muss der Administrator berücksichtigen, welche Mechanismen die jeweils beste Betriebseffizienz versprechen.

### Delegated Administrator (Delegierter Administrator)

Die Rolle und die Aufgaben eines delegierten Administrators (DA) werden vom Administrator zugewiesen. Beispielsweise kann ein delegierter Administrator Aktionen in bestimmten Desktop- oder Anwendungspools durchführen, zu denen er in anderen Pools nicht berechtigt ist. Delegierte Administratoren können den Umfang der ihnen zugewiesenen Aufgaben und Berechtigungen nicht ändern. Einem delegierten Administrator kann eine Vielzahl unterschiedlicher Aufgaben und Funktionen zugewiesen werden: von der Bereitstellung mehrerer Desktops auf virtuellen Maschinen bis zu einfachen Aufgaben wie dem Zurücksetzen von Desktops. Delegierte Administratoren haben die Möglichkeit, Aktionen für mehrere andere Benutzer auszuführen. Diese Berechtigung ist wesentlich für ein effektives administratives Arbeiten.

### End User (Endbenutzer)

Endbenutzer können Aktionen nur unter ihrem eigenen Benutzerkonto ausführen. Die Tätigkeiten von Endbenutzern sind meist auf eine kleine Gruppe von Ressourcen begrenzt, z. B. auf persönliche Desktops oder Anwendungen. Self-Service-Arbeitsabläufe erlauben eine Automatisierung wiederkehrender Tätigkeiten und die Ausführung komplexer Aufgaben durch Endbenutzer.

# Installation und Konfiguration des Horizon vCenter Orchestrator-Plug-Ins

## 2

Die Installation des Horizon vCenter Orchestrator-Plug-Ins ist vergleichbar mit der Installation anderer vCenter Orchestrator-Plug-Ins. Die Konfiguration des Plug-Ins beinhaltet die Ausführung verschiedener Konfigurations-Workflows, um Verbindungen zu View-Komponenten herzustellen und um Rollen und Berechtigungen zu konfigurieren.

Dieses Kapitel enthält die folgenden Themen:

- [Funktionsvoraussetzungen für das Horizon vCenter Orchestrator-Plug-In](#)
- [Das Horizon vCenter Orchestrator-Plug-In installieren oder aktualisieren](#)
- [Konfigurationsaufgaben nach dem Upgrade](#)
- [Konfigurieren der Verbindung mit einem View Pod](#)
- [Zuweisen delegierter Administratoren zu Desktop- und Anwendungspools](#)
- [Empfohlene Vorgehensweisen für die Verwaltung von Arbeitsablaufberechtigungen](#)
- [Festlegen einer Richtlinie für das Aufheben der Bereitstellung von virtuellen Desktop-Maschinen](#)

## Funktionsvoraussetzungen für das Horizon vCenter Orchestrator-Plug-In

Das Horizon vCenter Orchestrator-Plug-In agiert als Middleware zwischen Horizon 6, vCenter Orchestrator und vCloud Automation Center. Um das Horizon vCenter Orchestrator-Plug-In installieren und verwenden zu können, muss das verwendete System bestimmte Funktionsvoraussetzungen erfüllen.

### VMware Horizon 6 (mit View)

Sie benötigen Zugriff auf eine Instanz von View-Verbindungsserver 6.0 oder 6.0.1. Das Horizon vCenter Orchestrator-Plug-In kann zusammen mit VMware Horizon 6 verwendet werden.

Weitere Informationen zum Einrichten von VMware Horizon 6 (d. h. 6.0 oder 6.0.1) finden Sie in den Dokumenten *View Installation* und *View Administration* auf der Dokumentationsseite unter [https://www.vmware.com/support/pubs/view\\_pubs.html](https://www.vmware.com/support/pubs/view_pubs.html).

## vCenter Orchestrator

Stellen Sie sicher, dass eine aktive Instanz von Orchestrator verfügbar ist. Sie können sich unter [http://orchestrator\\_server:8283](http://orchestrator_server:8283) bei der Orchestrator-Konfigurationsoberfläche anmelden. Das Horizon vCenter Orchestrator-Plug-In kann mit vCenter Orchestrator 5.5.1 und 5.5.2 verwendet werden.

Weitere Informationen zum Einrichten von Orchestrator finden Sie unter *Installing and Configuring VMware vCenter Orchestrator* auf der Dokumentationsseite unter [https://www.vmware.com/support/pubs/orchestrator\\_pubs.html](https://www.vmware.com/support/pubs/orchestrator_pubs.html).

## vCloud Automation Center

Sie benötigen Zugriff auf einen vCloud Automation Center-Server. Das Horizon vCenter Orchestrator-Plug-In kann mit den vCloud Automation Center-Versionen 6.0.1 und 6.1 verwendet werden. Der eingebettete vCenter Orchestrator-Server im Paket mit den vCloud Automation Center-Versionen 6.0.1 und 6.1 ist mit diesem Plug-In kompatibel. Sie können das Plug-In auch auf einem externen vCenter Orchestrator-Server installieren.

Weitere Informationen zum Einrichten von vCloud Automation Center finden Sie unter *vCloud Automation Center Installation and Configuration* auf der Dokumentationsseite unter <https://www.vmware.com/support/pubs/vcac-pubs.html>.

## vCenter Server und vCenter Single Sign-On

Stellen Sie sicher, dass Sie Zugriff auf eine Instanz von vCenter Server 5.5.b haben und dass Sie vCenter™ Single Sign-On™ 2.0 verwenden.

Weitere Informationen zum Einrichten von vCenter Server 5.5 finden Sie unter *vSphere Installation and Setup* auf der Dokumentationsseite unter <https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html>.

## Das Horizon vCenter Orchestrator-Plug-In installieren oder aktualisieren

Um das Plug-In zu installieren oder zu aktualisieren, müssen Sie die aktuelle Installationsdatei über die Konfigurationsoberfläche von vCenter Orchestrator herunterladen, um die Plug-In-Datei hochzuladen und das Plug-In zu installieren.

Dieser Beitrag enthält eine Anleitung für die Installation des Horizon vCenter Orchestrator-Plug-Ins. Das Verfahren für die Installation von vCenter Orchestrator-Plug-Ins ist für alle Plug-Ins identisch und die Dokumentation für das Installieren und Aktualisieren allgemeiner Plug-Ins sowie die Behebung von Fehlern befindet sich an anderer Stelle. Weitere Informationen finden Sie auf der Dokumentationsseite von vCenter Orchestrator unter [https://www.vmware.com/support/pubs/orchestrator\\_pubs.html](https://www.vmware.com/support/pubs/orchestrator_pubs.html).

### Voraussetzungen

- Prüfen Sie, ob Sie die URL für das Herunterladen der Installationsdatei für das Horizon vCenter Orchestrator-Plug-In (.vmoapp-Datei) besitzen.

- Stellen Sie sicher, dass vCenter Orchestrator (entweder die virtuelle Appliance oder der Windows-Dienst) eingerichtet und für die Verwendung von vCenter Single Sign-On konfiguriert wurde. Weitere Informationen finden Sie unter „Register Orchestrator as a vCenter Single Sign On Solution in Advanced Mode“ in *Installing and Configuring VMware vCenter Orchestrator*.
- Stellen Sie sicher, dass Sie über Anmeldeinformationen für ein Konto verfügen, das berechtigt ist, vCenter Orchestrator-Plug-Ins zu installieren und sich über vCenter Single Sign-On zu authentifizieren.
- Stellen Sie sicher, dass der VMware vCenter Orchestrator-Client installiert ist und Sie sich mit Administratorberechtigungen anmelden können.

## Verfahren

- 1 Laden Sie die Plug-In-Datei an einen Speicherort herunter, auf den Sie von der vCenter Orchestrator Appliance bzw. dem Dienst aus zugreifen können.

Der Name der Installationsdatei ist `o11nplugin-horizon-1.1.0-xxxxxxx.vmoapp`, wobei `xxxxxx` für die Build-Nummer steht.

- 2 Öffnen Sie einen Browser und starten Sie die vCenter Orchestrator-Konfigurationsoberfläche.

Die URL hat folgendes Format: `https://server.mycompany.com:8283`.

- 3 Klicken Sie im linken Bereich auf das Element **Plug-ins** (Plug-Ins) und führen Sie einen Bildlauf bis zum Abschnitt **Neues Plug-In installieren** durch.

- 4 Wählen Sie im Textfeld **Plug-In-Datei** die Installationsdatei für das Plug-In aus und klicken Sie auf **Hochladen und installieren**.

Die Datei muss im `.vmoapp`-Format vorliegen.

- 5 Stimmen Sie im Bereich „Ein Plug-In installieren“ der Lizenzvereinbarung zu, wenn Sie dazu aufgefordert werden.

---

**Wichtig** Wenn Sie ein Upgrade durchführen, wird nach der Installation des Plug-Ins eine Meldung angezeigt: Ein Horizon-Plug-In (1.1.0 Build `xxxxxxx`) mit demselben Namen wurde bereits installiert (1.0.0 Build `xxxxxxx`): Das vorhandene Plug-In wird überschrieben.

---

- 6 Wechseln Sie zum Abschnitt **Installationsstatus der aktivierten Plug-Ins** und prüfen Sie, ob Horizon 1.1.0.`xxxxxxx` in der Liste angezeigt wird. `xxxxxx` steht für die Build-Nummer.

Eine Statusmeldung für die Installation oder das Upgrade wird angezeigt.

Installationstyp	Meldung
Neue Installation	Plug-In wird beim nächsten Start des Servers installiert.
Upgrade	Die Installation erfolgt beim nächsten Start des Servers.

- 7 Starten Sie den Serverdienst von vCenter Orchestrator neu.
- 8 Starten Sie den Konfigurationsdienst von vCenter Orchestrator neu.

- 9 Starten Sie die vCenter Orchestrator-Konfigurationsoberfläche erneut, klicken Sie auf das Element **Plug-ins** (Plug-Ins) und vergewissern Sie sich, dass als Status **Installation OK** (Installation OK) angezeigt wird.

### Nächste Schritte

Starten Sie die vCenter Orchestrator-Clientanwendung, melden Sie sich an und navigieren Sie auf der Registerkarte **Workflow** (Arbeitsablauf) in der Bibliothek zum Ordner **Horizon**. Sie können jetzt durch die vom Horizon vCenter Orchestrator-Plug-In bereitgestellten Arbeitsabläufe blättern.

Informationen zum Upgrade finden Sie unter [Konfigurationsaufgaben nach dem Upgrade](#).

## Konfigurationsaufgaben nach dem Upgrade

Nach dem Upgrade auf das Horizon vCenter Orchestrator-Plug-In 1.1 müssen Sie verschiedene Konfigurationsaufgaben ausführen, bevor Sie die neu hinzugefügten Arbeitsabläufe starten.

- 1 Legen Sie für die neu erstellten Konfigurationselemente **GastanmeldedatenKonfiguration** und **SelfServicePoolKonfiguration** im Ordner **View Zugriffsrechte für delegierte Administratoren** fest. Siehe [Empfohlene Vorgehensweisen für die Verwaltung von Arbeitsablaufberechtigungen](#).

- 2 Führen Sie den Arbeitsablauf „Anmeldedaten des Gasts hinzufügen“ im Ordner **Konfiguration/Horizon-Registrierungskonfiguration** aus, bevor Sie einen der neuen Arbeitsabläufe für die Registrierung nicht verwalteter Maschinen verwenden.

Nicht verwaltete Maschinen sind virtuelle Maschinen, die durch eine vCenter-Instanz verwaltet werden, die nicht zu View hinzugefügt wurde. Wenn Sie sich bei View Administrator anmelden und zu **View-Konfiguration > Server > vCenter-Server** wechseln, wird die vCenter Server-Instanz daher nicht in der Liste angezeigt.

Sie müssen eine nicht verwaltete Maschine zuerst mit einer View-Verbindungsserver-Instanz registrieren, damit Sie die virtuelle Maschine zu einem manuellen Desktop-Pool hinzufügen können. Damit Sie den Arbeitsablauf „Anmeldedaten des Gasts hinzufügen“ ausführen können, benötigen Sie Anmeldedaten eines lokalen oder Domänenadministrators für die virtuelle Maschine.

- 3 Führen Sie den Arbeitsablauf „Konfiguration des delegierten Administrators für die Registrierung verwalten“ im Ordner **Konfiguration/Horizon-Registrierungskonfiguration** aus, damit der angegebene delegierte Administrator berechtigt wird, die Gastanmeldedaten zu verwenden und auf den Ordner „datacenter“ oder „virtual machine“ zuzugreifen, der die nicht verwaltete virtuelle Maschine enthält.
- 4 Führen Sie den Arbeitsablauf „Self-Service-Poolkonfiguration verwalten“ im Ordner **Konfiguration/Self-Service-Pool-Konfiguration** aus, um festzulegen, welche Desktop- und Anwendungspools im neu hinzugefügten Ordner **Arbeitsabläufe/vCAC61** für Self-Service-Arbeitsabläufe verfügbar sein werden.

## Konfigurieren der Verbindung mit einem View Pod

Führen Sie den Arbeitsablauf „Add View Pod“ (View Pod hinzufügen) aus, um die richtigen Anmeldeinformationen für alle Arbeitsablaufvorgänge bereitzustellen, die von der View-Verbindungsserver-Instanz durchgeführt werden sollen.

### Voraussetzungen

- Stellen Sie sicher, dass der vollqualifizierte Domänenname der View-Verbindungsserver-Instanz auf dem Computer aufgelöst werden kann, auf dem der Orchestrator-Server ausgeführt wird.
- Stellen Sie sicher, dass Sie über Administratoranmeldeinformationen für den Orchestrator-Server verfügen. Das Konto muss Mitglied der Gruppe „vCenter Orchestrator Admin“ sind, die für die Authentifizierung über vCenter Single Sign-On konfiguriert ist.
- Stellen Sie sicher, dass Sie die Anmeldeinformationen eines Benutzers verwenden, dem die Rolle „View Administrator“ zugewiesen wurde. Die Benutzer und Gruppen mit der Rolle „View Administrators“ wurden bei der Installation und Einrichtung der View-Verbindungsserver-Instanz in View Administrator konfiguriert.

### Verfahren

- 1 Melden Sie sich als Administrator beim Orchestrator-Client an.
- 2 Klicken Sie im Orchestrator-Client auf die Ansicht **Arbeitsabläufe**.
- 3 Wählen Sie in der hierarchischen Liste der Arbeitsabläufe **Bibliothek > Horizon > -Konfiguration > View Pod-Konfiguration** aus und navigieren Sie zum Arbeitsablauf **Add View Pod in Configuration** (View Pod in Konfiguration einschließen).
- 4 Klicken Sie mit der rechten Maustaste auf den Arbeitsablauf **Add View Pod in Configuration (View Pod in Konfiguration einschließen)** und wählen Sie **Arbeitsablauf starten** aus.
- 5 Geben Sie einen Namen für den Pod an.
- 6 Geben Sie den vollqualifizierten Domännennamen des Computers an, auf dem die View-Verbindungsserver-Instanz installiert ist.
- 7 Geben Sie die Anmeldeinformationen eines Benutzers an, dem die Rolle „View Administrator“ zugewiesen wurde.
- 8 Überprüfen und akzeptieren Sie die Informationen zum SSL-Zertifikat.
- 9 Klicken Sie auf **Senden**, um den Arbeitsablauf auszuführen.

Klicken Sie nach dem Ausführen des Arbeitsablaufs auf die Erweiterungsschaltfläche, um den Status anzuzeigen.

### Nächste Schritte

Fügen Sie einen delegierten Administrator hinzu.

## Aktualisieren der View Pod-Verbindungsinformationen

Wenn sich die Anmeldedaten für die View-Verbindungsserver-Instanz oder die Mitglieder einer replizierten Gruppe von View-Verbindungsserver-Instanzen ändern, müssen Sie den entsprechenden Arbeitsablauf in vCenter Orchestrator ausführen.

Mit dem Orchestrator Client können Sie zu dem Ordner navigieren, der diese Arbeitsabläufe enthält, und **Bibliothek > Horizon > -Konfiguration > View Pod-Konfiguration** aufrufen.

- Wenn sich die Anmeldeinformationen für die View-Verbindungsserver-Instanz geändert haben, führen Sie den Arbeitsablauf „Update View Pod Credential Configuration“ aus.
- Wenn sich die Namen der Server oder die Anzahl der Instanzen im Pod geändert haben, führen Sie den Arbeitsablauf „View Pod-Verbindungsserverliste aktualisieren“ aus.

## Zuweisen delegierter Administratoren zu Desktop- und Anwendungspools

Der Administrator führt einen Arbeitsablauf aus, um Aufgaben an delegierte Administratoren zu delegieren. Wenn in Ihrer Konfiguration nicht bereits eine Benutzergruppe vorhanden ist, die über die Berechtigung zum Registrieren und Aktualisieren von vCenter-Erweiterungen sowie über die Berechtigung zum Ausführen von Arbeitsabläufen in Orchestrator verfügt, müssen Sie eine solche Gruppe zunächst erstellen.

Abhängig von Ihrer aktuellen Konfiguration haben Sie eine oder beide der ersten Aufgaben bereits ausgeführt.

### Verfahren

#### 1 Erstellen einer delegierten Administratorrolle mit vSphere Web Client

Für die delegierte Administration müssen Sie eine Benutzergruppe erstellen, die über Berechtigungen zum Registrieren und Aktualisieren von vCenter-Erweiterungen verfügt.

#### 2 Festlegen von Zugriffsrechten für die Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins

Nachdem Sie eine Gruppe für delegierte Administratoren erstellt und dieser Gruppe die Berechtigung zum Durchführen von Aktionen in vCenter-Erweiterungen zugewiesen haben, können Sie der Gruppe die Berechtigung zum Anzeigen und Ausführen von Arbeitsabläufen in Orchestrator gewähren.

#### 3 Zuweisen delegierter Administratoren zu Pools

Der Administrator führt den Arbeitsablauf „Konfiguration des delegierten Administrators“ aus, um den Geltungsbereich der delegierten Verwaltung einzurichten. Beispielsweise können die Berechtigungen eines bestimmten delegierten Administrators auf Vorgänge in bestimmten Pools beschränkt werden, während ein anderer delegierter Administrator nur Berechtigungen für eine andere Gruppe von Pools erhält.

### Nächste Schritte

Beschränken Sie die Berechtigungen für verschiedene Arbeitsablaufordner in Orchestrator.



## Erstellen einer delegierten Administratorrolle mit vSphere Web Client

Für die delegierte Administration müssen Sie eine Benutzergruppe erstellen, die über Berechtigungen zum Registrieren und Aktualisieren von vCenter-Erweiterungen verfügt.

Wenn Sie vCenter Orchestrator zuvor verwendet haben und bereits Benutzer und Gruppen mit Berechtigungen zum Registrieren und Aktualisieren von vCenter-Erweiterungen vorhanden sind, können einige der Schritte in diesem Thema ggf. übersprungen werden. Wenn beispielsweise eine entsprechende Gruppe vorhanden ist, der Benutzer, der die View-Desktop- und Anwendungspools verwalten wird, aber noch nicht in die Gruppe eingetragen wurde, dann müssen Sie nur den Benutzer zur Gruppe hinzufügen.

### Voraussetzungen

Stellen Sie sicher, dass die Anmeldeinformationen, mit denen Sie sich bei vSphere Web Client anmelden, für vCenter Single Sign-On konfiguriert wurden und dass Sie mit diesen Anmeldeinformationen über Administratorberechtigungen verfügen.

### Verfahren

- 1 Melden Sie sich bei vSphere Web Client als „administrator@vsphere.local“ oder als anderer Benutzer mit vCenter Single Sign-On-Administratorrechten an.
- 2 Erstellen Sie eine delegierte Administratorgruppe.
  - a Gehen Sie zu **Administration (Verwaltung) > Single Sign-On (Einmalige Anmeldung) > Benutzer und Gruppen**.
  - b Wählen Sie die Registerkarte **Groups** (Gruppen) aus und klicken Sie auf das Symbol **New Group** (Neue Gruppe).
  - c Geben Sie einen Namen an, z. B. **Delegierte Admins**, und klicken Sie auf **OK**.  
Die neue Gruppe wird in der Liste angezeigt.
- 3 Wählen Sie die eben erstellte Gruppe aus und fügen Sie dann der Gruppe im Bereich **Group Members** (Gruppenmitglieder) der Registerkarte einen delegierten Administratorbenutzer hinzu.  
Dieser Benutzer muss ein Mitglied der Domäne sein, in der die Instanz des View-Verbindungsservers ausgeführt wird.
- 4 Erstellen Sie eine Rolle, die über Berechtigungen zum Lesen von vCenter-Erweiterungen verfügt.
  - a Gehen Sie zu **Administration (Verwaltung) > Roles (Rollen)**.
  - b Klicken Sie auf der Registerkarte **Roles** (Rollen) auf das Symbol **Create role action** (Rollenaktion erstellen).

- c Geben Sie einen Namen für die Rolle an und aktivieren Sie das Kontrollkästchen **Extensions** (Erweiterungen).

Wenn Sie das Element **Extensions** (Erweiterungen) erweitern, sehen Sie, dass die Kontrollkästchen **Erweiterung registrieren**, **Unregister extension** (Registrierung für Erweiterung aufheben) und **Erweiterung aktualisieren** ebenfalls aktiviert sind.

- d Klicken Sie auf **OK**.

Die neue Rolle wird in der Liste angezeigt.

**5** Fügen Sie die neu erstellte Rolle der neuen Gruppe hinzu, die Sie zuvor erstellt haben.

- a Wechseln Sie zur „Startseite“ von vCenter und navigieren Sie zu **vCenter > Bestandslisten > vCenters**.

- b Wählen Sie im linken Bereich die entsprechende vCenter-Instanz aus und klicken Sie auf die Registerkarte **Manage** (Verwalten).

- c Klicken Sie auf der Registerkarte **Manage** (Verwalten) auf **Permissions** (Berechtigungen) und anschließend auf das Symbol **Add permission** (Berechtigung hinzufügen).

- d Klicken Sie im Bereich „Benutzer und Gruppen“ auf **Hinzufügen** und fügen Sie die eben erstellte Gruppe hinzu.

Wählen Sie die richtige Domäne aus, damit die Gruppe angezeigt wird.

Die Gruppe wird im Dialogfeld „Add Permission“ (Berechtigung hinzufügen) in der Liste der Benutzer und Gruppen angezeigt.

- e Klicken Sie im Bereich „Zugewiesene Rolle“ auf den Pfeil nach unten und wählen Sie die eben erstellte Rolle aus.

In der Liste der Berechtigungen für diese Rolle wird neben **Extensions** (Erweiterungen) ein Häkchen angezeigt.

- f Klicken Sie auf **OK**.

Die Gruppe wird, zusammen mit der eben zugewiesenen Rolle, auf der Registerkarte **Permissions** (Berechtigungen) angezeigt.

### Nächste Schritte

Gewähren Sie der delegierten Administratorgruppe Zugriff auf die Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins. Siehe [Festlegen von Zugriffsrechten für die Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins](#).

## Festlegen von Zugriffsrechten für die Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins

Nachdem Sie eine Gruppe für delegierte Administratoren erstellt und dieser Gruppe die Berechtigung zum Durchführen von Aktionen in vCenter-Erweiterungen zugewiesen haben, können Sie der Gruppe die Berechtigung zum Anzeigen und Ausführen von Arbeitsabläufen in Orchestrator gewähren.

Wenn Sie vCenter Orchestrator zuvor verwendet haben und bereits Benutzer und Gruppen mit Berechtigungen zum Anzeigen, Untersuchen und Ausführen von vCenter-Erweiterungen vorhanden sind, kann die in diesem Thema beschriebene Vorgehensweise ggf. übersprungen werden.

### Voraussetzungen

- Stellen Sie sicher, dass Sie über Administratoranmeldeinformationen für den Orchestrator-Server verfügen. Das Konto muss Mitglied der Gruppe „vCenter Orchestrator Admin“ sind, die für die Authentifizierung über vCenter Single Sign-On konfiguriert ist.
- Stellen Sie sicher, dass eine Gruppe für delegierte Administratoren erstellt und der Gruppe eine Rolle zugewiesen wurde, die über Berechtigungen für „Extensions“ (Erweiterungen) in vCenter verfügt. Siehe [Erstellen einer delegierten Administratorrolle mit vSphere Web Client](#).

### Verfahren

- 1 Melden Sie sich als Administrator beim Orchestrator-Client an und wählen Sie im oberen linken Bereich des Bildschirms im Dropdown-Menü die Option **Design** (Entwurf) aus.
- 2 Klicken Sie mit der rechten Maustaste im linken Fensterbereich auf das Stammverzeichnis und wählen Sie **Edit access rights** (Zugriffsrechte bearbeiten) aus.
- 3 Klicken Sie im Dialogfeld „Edit Access Rights“ (Zugriffsrechte bearbeiten) auf **Add access rights** (Zugriffsrechte hinzufügen).
- 4 Geben Sie im Auswahldialogfeld im Textfeld **Filter** (Filter) die ersten Zeichen des Namens der delegierten Administratorgruppe ein. Wenn der Gruppenname in der Liste angezeigt wird, wählen Sie die Gruppe aus.
- 5 Aktivieren Sie das Kontrollkästchen **View** (Anzeigen), deaktivieren Sie alle anderen Kontrollkästchen und klicken Sie dann auf **Select** (Auswählen).  
  
Die Gruppe wird nun in der Liste im Dialogfeld „Edit Access Rights“ (Zugriffsrechte bearbeiten) angezeigt.
- 6 Klicken Sie auf **Save and close** (Speichern und schließen).  
  
Die Gruppe wird der Registerkarte **Permissions** (Berechtigungen) hinzugefügt. In der Spalte „Rights“ (Rechte) wird angezeigt, dass die Gruppe über die Berechtigung „View“ (Anzeigen) verfügt.
- 7 Erweitern Sie im linken Fensterbereich die Bibliothek und klicken Sie mit der rechten Maustaste auf den Ordner **Horizon**.
- 8 Wählen Sie im Kontextmenü die Option **Edit access rights** (Zugriffsrechte bearbeiten) aus und klicken Sie auf **Add access rights** (Zugriffsrechte hinzufügen).
- 9 Geben Sie im Textfeld **Filter** den Namen der delegierten Administratorgruppe ein, wählen Sie die Gruppe in der Liste aus und aktivieren Sie dann die Kontrollkästchen **View** (Anzeigen), **Inspect** (Untersuchen) und **Execute** (Ausführen).

- 10 Klicken Sie im Auswahldialogfeld auf **Select** (Auswählen) und klicken Sie anschließend im Dialogfeld „Edit Access Rights“ (Zugriffsrechte bearbeiten) auf **Save and close** (Speichern und schließen).

Die Gruppe wird der Registerkarte **Permissions** (Berechtigungen) hinzugefügt. In der Spalte „Rights“ (Rechte) wird angezeigt, dass die Gruppe über die Berechtigungen „View“ (Anzeigen), „Inspect“ (Untersuchen) und „Execute“ (Ausführen) verfügt.

### Nächste Schritte

Weisen Sie die delegierte Administratorgruppe bestimmten Desktop- und Anwendungspools zu. Siehe [Zuweisen delegierter Administratoren zu Pools](#).

## Zuweisen delegierter Administratoren zu Pools

Der Administrator führt den Arbeitsablauf „Konfiguration des delegierten Administrators“ aus, um den Geltungsbereich der delegierten Verwaltung einzurichten. Beispielsweise können die Berechtigungen eines bestimmten delegierten Administrators auf Vorgänge in bestimmten Pools beschränkt werden, während ein anderer delegierter Administrator nur Berechtigungen für eine andere Gruppe von Pools erhält.

Der Arbeitsablauf „Konfiguration des delegierten Administrators“ muss ausgeführt werden, um das Horizon vCenter Orchestrator-Plug-In zu konfigurieren, da den Pools mindestens der primäre Administrator zugewiesen werden muss. Mit diesem Arbeitsablauf kann der Administrator genau festlegen, bei welchen Pools eine verteilte Verwaltung zulässig ist und welche Arbeitsabläufe verwendet werden können.

### Voraussetzungen

- Stellen Sie sicher, dass Sie über Administratoranmeldeinformationen für den Orchestrator-Server verfügen. Das Konto muss Mitglied der Gruppe „vCenter Orchestrator Admin“ sind, die für die Authentifizierung über vCenter Single Sign-On konfiguriert ist.
- Stellen Sie sicher, dass der delegierten Administratorgruppe Berechtigungen zum Anzeigen und Ausführen von Arbeitsabläufen des Horizon vCenter Orchestrator-Plug-Ins gewährt wurden. Weitere Informationen finden Sie unter [Festlegen von Zugriffsrechten für die Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins](#).
- Stellen Sie sicher, dass eine Verbindung mit dem View Pod hergestellt wurde, indem Sie den Arbeitsablauf „Add View Pod in Configuration“ (View Pod in Konfiguration einschließen) ausführen. Siehe [Konfigurieren der Verbindung mit einem View Pod](#).

### Verfahren

- 1 Melden Sie sich als Administrator beim Orchestrator-Client an.
- 2 Klicken Sie im Orchestrator-Client auf die Ansicht **Arbeitsabläufe**.
- 3 Wählen Sie in der hierarchischen Liste der Arbeitsabläufe **Bibliothek > Horizon > -Konfiguration > Delegated Admin Configuration** aus und navigieren Sie zum Arbeitsablauf **Add Delegated Administrator Configuration** (Konfiguration eines delegierten Administrators hinzufügen).

- 4 Klicken Sie mit der rechten Maustaste auf den Arbeitsablauf **Add Delegated Administrator Configuration (Konfiguration eines delegierten Administrators hinzufügen)** und wählen Sie **Arbeitsablauf starten** aus.
- 5 Füllen Sie das angezeigte Formular aus.

Option	Aktion
<b>Horizon View Pod</b>	Wählen Sie in der Dropdown-Liste den Pod aus. Diese Liste wird beim Ausführen des Arbeitsablaufs „Add View Pod in Configuration (View Pod in Konfiguration einschließen)“ mit Elementen gefüllt.
<b>Auswählen der Desktop-Pool-IDs</b>	Klicken Sie auf <b>Not Set</b> (Nicht festgelegt) und fügen Sie einen oder mehrere Pools aus der Dropdown-Liste <b>Neuer Wert</b> hinzu.
<b>Auswählen der Anwendungspool-IDs</b>	Klicken Sie auf <b>Not Set</b> (Nicht festgelegt) und fügen Sie einen oder mehrere Pools aus der Dropdown-Liste <b>Neuer Wert</b> hinzu.
<b>Benutzername des delegierten Administrators</b>	Klicken Sie auf <b>Not Set</b> (Nicht festgelegt) und geben Sie im Textfeld <b>Filter</b> den Namen des Benutzers ein, den Sie der delegierten Administratorgruppe hinzugefügt haben.

- 6 Klicken Sie auf **Senden**, um den Arbeitsablauf auszuführen.

Der ausgewählte delegierte Administrator ist nun berechtigt, die zuvor im Formular angegebenen Desktop- und Anwendungspools zu verwalten.

## Empfohlene Vorgehensweisen für die Verwaltung von Arbeitsablaufberechtigungen

Mit dem Orchestrator-Client können Sie die Personas beschränken, die die Arbeitsabläufe anzeigen und mit ihnen interagieren dürfen. Im Idealfall interagiert nur der Administrator über den Orchestrator-Client mit Arbeitsabläufen in vCenter Orchestrator. Delegierte Administratoren und Endbenutzer sollten über den vSphere Web Client oder den Servicekatalog in vCloud Automation Center mit den Arbeitsabläufen interagieren.

Das Horizon vCenter Orchestrator-Plug-In installiert eine Reihe von Arbeitsabläufen, in der vCenter Orchestrator-Benutzeroberfläche in Verzeichnissen organisiert sind. Die Ordner **API access** und **Business logic** sollten nicht verändert werden, da ihr Inhalt die Grundlage für andere ausführbare Arbeitsabläufe bildet. Um eine nicht autorisierte Anpassung von Arbeitsabläufen zu verhindern, empfiehlt es sich, bei bestimmten Ordnern die Berechtigung zum Bearbeiten für alle Benutzer mit Ausnahme des Administrators zu entfernen.

**Wichtig** Die hier aufgeführten empfohlenen Berechtigungseinstellungen sind nur erforderlich, wenn der Ordner **CoreModules** und die Konfigurationselemente im Ordner **View** für delegierte Administratoren und Endbenutzer nicht sichtbar sein sollen.

In der Ansicht **Workflows** können Sie die folgenden Zugriffsrechte festlegen:

- Legen Sie die Zugriffsrechte für den Stammordner im linken Fensterbereich so fest, dass delegierte Administratoren nur über die Berechtigungen „View“ (Anzeigen) und „Execute“ (Ausführen) verfügen.

- Legen Sie die Zugriffsrechte für die Ordner **Configuration** und **CoreModules** so fest, dass delegierte Administratoren über keine Berechtigungen verfügen und diese Ordner ihnen daher auch nicht angezeigt werden. Diese Einschränkung setzt die für den Stammordner festgelegten Berechtigungen außer Kraft.
- Legen Sie die Zugriffsrechte für den Ordner **Business logic** im Ordner **CoreModules** so fest, dass delegierte Administratoren nur über die Berechtigung „View“ (Anzeigen) verfügen.
- Legen Sie die Zugriffsrechte für die Ordner **vCAC60** und **vSphereWebClient** so fest, dass delegierte Administratoren nur über die Berechtigung „View“ (Anzeigen) verfügen.

Wenn Sie mit der Vorgehensweise zum Festlegen von Zugriffsrechten nicht vertraut sind, finden Sie weitere Informationen unter "Set User Permissions on a Workflow" in der Dokumentation zu vCenter Orchestrator, die auf der Seite für die VMware vCenter Orchestrator-Dokumentation unter [https://www.vmware.com/support/pubs/orchestrator\\_pubs.html](https://www.vmware.com/support/pubs/orchestrator_pubs.html) verfügbar ist.

In der Ansicht **Configurations** (Konfigurationen) können Sie die folgenden Zugriffsrechte festlegen:

- Legen Sie die Zugriffsrechte für den Ordner **View** so fest, dass delegierte Administratoren über keine Berechtigungen verfügen.
- Legen Sie die Zugriffsrechte für die Konfigurationselemente **viewPodConfiguration**, **DA-configuration** und **PoolPolicyConfiguration** im Ordner **View** so fest, dass delegierte Administratoren nur über die Berechtigung „View“ (Anzeigen) verfügen.
- Wenn Sie das Horizon vCenter Orchestrator-Plug-in 1.1 haben, müssen Sie außerdem Zugriffsrechte für die Konfigurationselemente **GastanmeldedatenKonfiguration** und **SelfServicePoolKonfiguration** im Ordner **View** festlegen, damit delegierte Administratoren ausschließlich View-Berechtigungen besitzen.

Wenn Sie mit der Vorgehensweise zum Festlegen von Zugriffsrechten nicht vertraut sind, finden Sie weitere Informationen unter "Create a Configuration Element" in der Dokumentation zu vCenter Orchestrator, die auf der Seite für die VMware vCenter Orchestrator-Dokumentation unter [https://www.vmware.com/support/pubs/orchestrator\\_pubs.html](https://www.vmware.com/support/pubs/orchestrator_pubs.html) verfügbar ist.

## Festlegen einer Richtlinie für das Aufheben der Bereitstellung von virtuellen Desktop-Maschinen

Mithilfe des Arbeitsablaufs „Add Pool Policy Configuration“ können Administratoren Sicherheitsmaßnahmen für delegierte Administratoren und Endbenutzer konfigurieren, die das Aufheben der Bereitstellung und das Wiederverwenden von Desktops betreffen. Die Administratoren können hierbei angeben, ob die virtuelle Maschine tatsächlich gelöscht werden soll und wie ggf. zugeordnete dauerhafte Festplatten verwaltet werden sollen.

Sie müssen diesen Arbeitsablauf einmal für jeden Pool ausführen, für den ein Arbeitsablauf zum Aufheben von Bereitstellungen aktiviert wurde. Beim Aufheben der Bereitstellung von virtuellen Maschinen in einem Desktop-Pool haben Sie verschiedene Möglichkeiten:

- Sie können die virtuelle Maschine löschen oder lediglich die Zuweisung und die Berechtigung des Benutzers aufheben.

- Wenn Sie die virtuelle Maschine löschen und die Maschine über eine dauerhafte View Composer-Festplatte verfügt, können Sie die Festplatte speichern oder ebenfalls löschen.
- Wenn Sie die dauerhaften View Composer-Festplatten speichern möchten, können Sie hierfür den aktuellen Datenspeicher der Festplatte oder einen anderen Datenspeicher auswählen.

### Voraussetzungen

- Stellen Sie sicher, dass Sie über Administratoranmeldeinformationen für den Orchestrator-Server verfügen. Das Konto muss Mitglied der Gruppe „vCenter Orchestrator Admin“ sind, die für die Authentifizierung über vCenter Single Sign-On konfiguriert ist.
- Konfigurieren Sie Verbindung mit dem View Pod.
- Überlegen Sie, welche Richtlinien Sie für das Löschen virtueller Maschinen und das Speichern dauerhafter Festplatten konfigurieren möchten. Weitere Informationen zu dauerhaften Festplatten finden Sie in den Themen zur Verwaltung von dauerhaften Festplatten in View Composer im Dokument *View Administration*.

Wenn Sie angeben, dass die virtuelle Maschine gelöscht werden soll, müssen Sie außerdem angeben, ob ggf. vorhandene dauerhafte Festplatten gespeichert werden sollen. Wenn Sie angeben, dass die Festplatte in einem anderen Datenspeicher gespeichert werden soll, benötigen Sie den Namen des Datenspeichers und den Pfad zu dem Ordner, in dem die dauerhafte Festplatte gespeichert werden soll.

### Verfahren

- 1 Melden Sie sich als Administrator beim Orchestrator-Client an.
- 2 Klicken Sie im Orchestrator-Client auf die Ansicht **Arbeitsabläufe**.
- 3 Wählen Sie in der hierarchischen Liste der Arbeitsabläufe **Bibliothek > Horizon > -Konfiguration > Pool Policy Configuration (Pool-Richtlinienkonfiguration)** aus und navigieren Sie zum Arbeitsablauf **Add Pool Policy Configuration (Pool-Richtlinienkonfiguration hinzufügen)**.
- 4 Klicken Sie mit der rechten Maustaste auf den Arbeitsablauf **Add Pool Policy Configuration (Pool-Richtlinienkonfiguration hinzufügen)** und wählen Sie **Arbeitsablauf starten** aus.
- 5 Füllen Sie das angezeigte Formular aus und klicken Sie auf **Senden**.

Wenn Sie eine dauerhafte Festplatte speichern möchten, geben Sie den Datenspeicher und den Pfad zu dem Ordner an, in dem die dauerhafte Festplatte gespeichert werden soll.

### Nächste Schritte

Wenn Sie eine Poolrichtlinie entfernen oder aktualisieren möchten, können Sie den Arbeitsablauf „Pool-Richtlinienkonfiguration entfernen“ oder „Pool-Richtlinienkonfiguration aktualisieren“ ausführen.

# Verwenden der Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins

## 3

Sie können die zusammen mit dem Horizon vCenter Orchestrator-Plug-In installierten, vordefinierten Arbeitsabläufe verwenden oder Kopien der Arbeitsabläufe erstellen und diese anpassen.

---

**Wichtig** Aus Sicherheitsgründen können Konfigurationsarbeitsabläufe nur im Orchestrator-Client ausgeführt werden.

---

Die vordefinierten Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins finden Sie im Ordner Horizon. Wenn Sie einen Arbeitsablauf anpassen möchten, erstellen Sie ein Duplikat des entsprechenden Arbeitsablaufs. Von Ihnen erstellte duplizierte bzw. angepasste, benutzerdefinierte Arbeitsabläufe können vollständig bearbeitet werden.

Weitere Informationen zu den unterschiedlichen Zugriffsrechten, die beim Arbeiten mit dem Orchestrator-Server und abhängig vom Lizenztyp von vCenter Server gewährt werden, finden Sie unter *Installing and Configuring VMware vCenter Orchestrator* (Installieren und Konfigurieren von VMware vCenter Orchestrator).

Dieses Kapitel enthält die folgenden Themen:

- [Zugreifen auf die Arbeitsablaufbibliothek des Horizon vCenter Orchestrator-Plug-Ins](#)
- [Arbeitsablaufbibliothek des Horizon vCenter Orchestrator-Plug-Ins](#)
- [Arbeitsablaufreferenz für das Horizon vCenter Orchestrator-Plug-In](#)
- [Syntax für die Angabe von Benutzerkonten in den Arbeitsabläufen](#)

## Zugreifen auf die Arbeitsablaufbibliothek des Horizon vCenter Orchestrator-Plug-Ins

Für den Zugriff auf die Elemente aus der Arbeitsablaufbibliothek des Horizon vCenter Orchestrator-Plug-Ins müssen Sie den Orchestrator-Client oder vSphere Web Client verwenden.

### Voraussetzungen

- Konfigurieren Sie Verbindung mit dem View Pod. Siehe [Konfigurieren der Verbindung mit einem View Pod](#)



- Stellen Sie sicher, dass Sie über Anmeldeinformationen für die Anmeldung beim Orchestrator-Client als Benutzer verfügen, der berechtigt ist, Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins auszuführen.

## Verfahren

- 1 Melden Sie sich beim Orchestrator-Client an.
- 2 Klicken Sie im Orchestrator-Client auf die Ansicht **Arbeitsabläufe**.
- 3 Erweitern Sie in der hierarchischen Liste **Bibliothek > Horizon > Arbeitsabläufe**.
- 4 Die Arbeitsablaufbibliothek wird angezeigt.

# Arbeitsablaufbibliothek des Horizon vCenter Orchestrator-Plug-Ins

Die Arbeitsablaufbibliothek für das Plug-In enthält Arbeitsabläufe für die Ausführung verschiedener automatisierter Prozesse, mit denen Sie View-Pods verwalten können. Dies umfasst Objekte wie Remote-Desktops und -Anwendungen, Pools, Berechtigungen oder View Server-Konfigurationen.

Die vom Horizon vCenter Orchestrator-Plug-In bereitgestellten Ordner und Arbeitsabläufe werden im Ordner **Horizon** gespeichert und sind nach Zweck und Funktionalität in verschiedenen Unterordnern organisiert. Sie können die vorhandene Ordnerstruktur nach Bedarf ändern. Dies hat keinen Einfluss auf die Ausführung der Arbeitsabläufe.

**Vorsicht** Einige Ordner enthalten Arbeitsabläufe, die für die Ausführung anderer Arbeitsabläufe erforderlich sind. Diese Arbeitsabläufe dürfen nicht geändert werden.

**Tabelle 3-1. Zum Horizon vCenter Orchestrator-Plug-In gehörende Ordner**

Ordnername	Beschreibung
Horizon	Stammordner des Horizon vCenter Orchestrator-Plug-Ins.
CoreModules/API Access	API-Schicht für die Arbeitsabläufe.
	<b>Wichtig</b> Der Inhalt dieses Ordners darf nicht geändert werden.
CoreModules/Business Logic	Geschäftslogik für Interaktionen der Arbeitsabläufe zwischen den Ausführungsschichten und der API Access-Schicht.
	<b>Wichtig</b> Der Inhalt dieses Ordners darf nicht geändert werden.
Konfiguration	Arbeitsabläufe für die Einrichtung und Verwaltung anderer Arbeitsabläufe. Konfigurationsarbeitsabläufe sollten nur von Administratoren im vCenter Orchestrator-Client ausgeführt werden.
Configuration /Workflow Delegation	Arbeitsabläufe, mit denen ein Administrator testen kann, ob ein bestimmter delegierter Administrator einen Arbeitsablauf erfolgreich ausführen kann. Einige Arbeitsabläufe können in vSphere Web Client ausgeführt werden, zeigen aber keinen Berechtigungsfehler an, wenn der delegierte Administrator nicht über die richtigen Berechtigungen verfügt.

Ordnername	Beschreibung
Workflows/Example	Arbeitsabläufe, die als Grundlage zum Erstellen benutzerdefinierter Arbeitsabläufe verwendet werden können.  <b>Hinweis</b> Wenn die Arbeitsablaufberechtigungen wie in diesem Dokument empfohlen festgelegt werden, kann nur der primäre Administrator den Arbeitsablauf „Add Pool Policy in Batch“ ausführen.
Arbeitsabläufe/vCAC60 Arbeitsabläufe/vCAC61	Arbeitsabläufe, mit denen ein Administrator Katalogelemente in vCloud Automation Center erstellen kann. Bei einigen der Arbeitsabläufe in diesem Ordner handelt es sich um Self-Service-Arbeitsabläufe, die von Endbenutzern für Self-Service-Zugriffe auf virtuelle Desktops und Remoteanwendungen verwendet werden können. Diese Arbeitsabläufe sind ausschließlich für die Ausführung in vCloud Automation Center vorgesehen.  <b>Hinweis</b> Sie benötigen das Horizon vCenter Orchestrator-Plug-In 1.1, um die Arbeitsabläufe im Ordner vCAC61 zu verwenden.
Workflows/vSphereWebClient	Arbeitsabläufe, die für die Ausführung durch Administratoren oder delegierte Administratoren in vSphere Web Client vorgesehen sind. Eine Ausführung im Orchestrator-Client ist aber ebenfalls möglich.

## Arbeitsablaufreferenz für das Horizon vCenter Orchestrator-Plug-In

Jeder Arbeitsablauf erfüllt einen spezifischen Zweck und erfordert bestimmte Eingaben.

Der Administrator muss die Arbeitsabläufe im Ordner vCAC60 mit einem Pod und einem Pool verknüpfen. Siehe [Verknüpfen von vSphereWebClient-Arbeitsabläufen mit bestimmten Pods und Pools in vCenter Orchestrator](#). Wenn ein delegierter Administrator oder ein Endbenutzer den Arbeitsablauf ausführt, wird der Arbeitsablauf nur auf den zugewiesenen Pod und Pool angewendet.

### Add Managed Machines to Pool (Verwaltete Maschinen zu einem Pool hinzufügen)

Zweck	(Verfügbar mit dem Horizon vCenter Orchestrator-Plug-In 1.1) Erlaubt einem delegierten Administrator das Hinzufügen von durch vCenter verwalteten Maschinen zu einem manuellen Desktop-Pool in View. Hier wurde die vCenter-Instanz, die die Maschinen verwaltet, zu View hinzugefügt. Wenn Sie z. B. in View Administrator nachsehen, können Sie zu <b>View Configuration &gt; Servers &gt; vCenter Servers</b> (View-Konfiguration/Server/vCenter-Server) wechseln, wo Sie die Instanz in der Liste finden.
Eingaben/Parameter	Pod, Pool-ID, Liste der virtuellen Maschinen
Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen.
Ergebnisse	Die ausgewählten virtuellen Maschinen werden zu einem manuellen Desktop-Pool hinzugefügt.

## Add Unmanaged Machines to Pool (Nicht verwaltete Maschinen zu einem Pool hinzufügen)

Zweck	<p>(Verfügbar mit dem Horizon vCenter Orchestrator-Plug-In 1.1) Erlaubt einem delegierten Administrator das Hinzufügen von nicht verwalteten Maschinen zu einem manuellen Desktop-Pool in View. Die nicht verwalteten Maschinen werden tatsächlich durch eine vCenter-Instanz verwaltet, die jedoch nicht zu View hinzugefügt wurde.</p> <p><b>Hinweis</b> Dieser Arbeitsablauf dient nicht dazu, physische Maschinen oder nicht mit vSphere bereitgestellte virtuelle Maschinen hinzuzufügen. Informationen zum Hinzufügen dieser Maschinentypen finden Sie unter <a href="#">Hinzufügen physischer Maschinen und nicht durch vSphere bereitgestellter virtueller Maschinen zu Pools</a>.</p>
Eingaben/Parameter	Pod, Pool-ID, Liste der virtuellen Maschinen, Anmeldedaten des Gasts (siehe die Zeile mit den Einschränkungen in dieser Tabelle)
Voraussetzungen	Siehe <a href="#">Voraussetzungen für das Hinzufügen von nicht verwalteten Maschinen zu Pools</a> .
Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool, Pod und Gastanmeldedaten verknüpfen.
Ergebnisse	<p>Die ausgewählten virtuellen Maschinen werden registriert und zu einem manuellen Desktop-Pool hinzugefügt.</p> <p>Wenn Sie versuchen mit diesem Arbeitsablauf mehrere Maschinen hinzuzufügen und dabei aus irgendwelchen Gründen einige Maschinen nicht hinzugefügt werden, schlägt der Arbeitsablauf fehl und die Protokolldatei enthält Fehlermeldungen mit Angaben dazu, warum diese Maschinen nicht hinzugefügt wurden. Andere Maschinen werden erfolgreich hinzugefügt.</p>
Einschränkungen	<ul style="list-style-type: none"> <li>■ Wenn Sie eine Maschine, die Sie zuvor in View aus dem Pool entfernt hatten, wieder zu einem nicht verwalteten Pool hinzufügen möchten, müssen Sie ein wenig warten, bevor Sie die Maschine wieder zum Pool hinzufügen.</li> <li>■ Wählen Sie virtuelle Maschinen nur aus vCenter Server-Instanzen aus, die nicht zu View hinzugefügt wurden. Es werden alle vCenter Server-Instanzen gelistet, das heißt, dass vCenter Server-Instanzen, die zu View hinzugefügt wurden, nicht herausgefiltert werden.</li> <li>■ Wenn nicht alle virtuellen Maschinen der vCenter Server-Instanz im Ordner der virtuellen Maschine angezeigt werden, können Sie Maschinen aus einzelnen Hostordnern auswählen. Dieses Problem kann auftreten, wenn die Anzahl der virtuellen Maschinen sehr groß ist.</li> <li>■ Nachdem Sie den Arbeitsablauf „Add Guest Credentials“ (Anmeldedaten des Gasts hinzufügen) und den Arbeitsablauf „Manage Delegated Administrator Configuration for Registration“ (Konfiguration des delegierten Administrators für die Registrierung verwalten) ausgeführt haben, kann es einen Moment dauern, bis die Gastanmeldedaten im Dienstkatalog von vCloud Automation Center 6.1 angezeigt werden. Sie müssen sich eventuell auch von vCloud Automation Center abmelden und erneut anmelden, damit die Anmeldedaten angezeigt werden.</li> <li>■ Wenn Sie Gastanmeldedaten entfernen, indem Sie den Arbeitsablauf „Remove Guest Credential“ (Anmeldedaten des Gasts entfernen) ausführen, müssen Sie auch den Arbeitsablauf „Refresh Delegated Administrator Configuration“ (Konfiguration des delegierten Administrators aktualisieren) im Ordner Configuration/Delegated Admin Configuration ausführen.</li> </ul> <p>Wenn Sie dies nicht tun, kann es passieren, dass beim Ausführen des Arbeitsablaufs „Add Unmanaged Machines to Pool“ (Nicht verwaltete Maschinen zu einem Pool hinzufügen) im Dropdown-Menü des Arbeitsablaufs die alten Anmeldedaten des Gasts angezeigt werden. Wenn Sie diese Anmeldedaten auswählen und den Arbeitsablauf ausführen, führt dies zur folgenden Fehlermeldung: Cannot find credential named TestCredentials Dynamic Script Module name :getGuestCredential#7)</p>

## Add User(s) to App Pool (Benutzer zu einem Anwendungspool hinzufügen)

Zweck	Ermöglicht es einem delegierten Administrator, Benutzern Berechtigungen für einen Anwendungspool zu gewähren.
Eingaben/Parameter	Pod, Pool-ID, Benutzernamen
Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen. Im Ordner vSphereWebClient ist keine Verknüpfung erforderlich. Wenn Sie den Arbeitsablauf mit einem Pod verknüpfen, wird in vSphere Web Client eine Dropdown-Liste der Pools und Benutzer mit Berechtigungen für den jeweiligen Pool angezeigt.
Ergebnisse	Berechtigte Benutzer erhalten direkten Zugriff auf die angegebenen Anwendungen.

## Add User(s) to App Pools (Benutzer zu Anwendungspools hinzufügen)

Zweck	Ermöglicht es einem delegierten Administrator, Benutzern Berechtigungen für mehrere Anwendungspools zu gewähren.
Eingaben/Parameter	Pod, Pool-IDs, Benutzernamen
Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit Pools und einem Pod verknüpfen. Im Ordner vSphereWebClient muss der Administrator diesen Arbeitsablauf mit einem Pod verknüpfen. In vSphere Web Client wird eine Dropdown-Liste der Pools und Benutzer mit Berechtigungen für den jeweiligen Pool angezeigt.
Ergebnisse	Berechtigte Benutzer erhalten direkten Zugriff auf die angegebene Anwendung.

## Add User(s) to Desktop Pool (Benutzer zu einem Desktop-Pool hinzufügen)

Zweck	Ermöglicht es einem delegierten Administrator, Benutzern Berechtigungen für einen Desktop-Pool zu gewähren.
Eingaben/Parameter	Pod, Pool-ID, Benutzernamen
Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen. Im Ordner vSphereWebClient ist keine Verknüpfung erforderlich. Wenn Sie den Arbeitsablauf mit einem Pod verknüpfen, wird in vSphere Web Client eine Dropdown-Liste der Pools und Benutzer mit Berechtigungen für den jeweiligen Pool angezeigt.
Ergebnisse	Den Benutzern werden Berechtigungen für den angegebenen Desktop-Pool gewährt. Sie können eine Maschine aus dynamischen Pools oder automatisch zugewiesenen dedizierten Pools abrufen (abhängig von der Verfügbarkeit). Bei ändern Pooltypen müssen die Benutzer mithilfe der Zuordnungsarbeitsabläufe explizit der Maschine zugeordnet werden.

## Application Entitlement (Anwendungsberechtigung)

Zweck	Ermöglicht es einem delegierten Administrator, Benutzern Berechtigungen für einen Anwendungspool zu gewähren oder die Berechtigungen zu entfernen.
Eingaben/Parameter	Pod, Pool-ID, zu berechtigende Benutzer sowie Benutzer, deren Berechtigungen entfernt werden sollen (Auswahl aus einer Standardliste)

Verknüpfungsanforderungen	In den Ordnern vCAC60 und vSphereWebClient muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen.
Ergebnisse	Berechtigungen können im selben Arbeitsablauf hinzugefügt und entfernt werden.

## Benutzer zuweisen

Zweck	Weist einen Benutzer einer bestimmten Maschine in einem Desktop-Pool zu. Zusätzlich steht eine Option zur Verfügung, um dem Benutzer gleichzeitig Berechtigungen für einen Desktop-Pool zu gewähren.
Eingaben/Parameter	Pod, Pool-ID, Maschinennamen, Benutzername
Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen. Im Ordner vSphereWebClient ist keine Verknüpfung erforderlich.
Ergebnisse	Der Benutzer wird der angegebenen Maschine zugewiesen. Die vorhandene Zuweisung wird entfernt und der Benutzer wird aus einer ggf. bestehenden aktiven Sitzung abgemeldet.

## Desktop Allocation (Desktop-Zuordnung)

Zweck	Berechtigt den Benutzer zur Verwendung des angegebenen Desktop-Pools und weist dem Benutzer, wenn es sich um einen Pool mit dedizierten Zuweisungen handelt, eine Maschine zu (abhängig von der Verfügbarkeit). Für den Benutzer wird eine neue Maschine bereitgestellt, wenn für den Pool der Typ „specified naming“ (angegebene Benennung) definiert wurde.
Eingaben/Parameter	Pod, Pool-ID, Benutzername
Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen. Im Ordner vSphereWebClient ist keine Verknüpfung erforderlich.
Ergebnisse	<ul style="list-style-type: none"> <li>■ Bei dynamischen Desktop-Pools und sitzungsbasierten Pools von RDS-Hosts, werden dem Benutzer Berechtigungen für den Pool gewährt.</li> <li>■ Bei automatisch zugewiesenen dedizierten Pools werden dem Benutzer Berechtigungen für den Pool gewährt und der Benutzer wird einer verfügbaren Maschine zugewiesen (sofern vorhanden).</li> <li>■ Bei dedizierten Pools ohne automatisches Benennungsschema wird für den Benutzer eine virtuelle Maschine mit dem von Administrator angegebenen Namen bereitgestellt.</li> </ul>

## Desktopzuordnung für Benutzer

Zweck	<p>(Verfügbar mit dem Horizon vCenter Orchestrator-Plug-In 1.1) Berechtigt mehrere Benutzer für Desktops in Pools mit dynamischer Zuordnung oder RDS-Desktop-Pools.</p> <p>Berechtigt mehrere Benutzer und weist diese Maschinen für Pools mit dedizierter Zuweisung zu (abhängig von der Verfügbarkeit).</p> <p>Neue Maschinen werden für Benutzer bereitgestellt, wenn für den Pool der Typ „specified naming“ (angegebene Benennung) definiert wurde.</p>
Eingaben/Parameter	Pod, Pool-ID, Benutzernamen, Maschinennamen (für den angegebenen Benennungspool)
Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen.

Ergebnisse	<ul style="list-style-type: none"> <li>■ Bei dynamischen Desktop-Pools und sitzungsbasierten Pools von RDS-Hosts werden den Benutzern Berechtigungen für den Pool gewährt.</li> <li>■ Bei automatisch zugewiesenen dedizierten Pools werden den Benutzern Berechtigungen für den Pool gewährt und die Benutzer werden einer verfügbaren Maschine zugewiesen (sofern vorhanden).</li> <li>■ Bei dedizierten Pools ohne automatisches Benennungsschema werden für die Benutzer virtuelle Maschinen mit den vom Administrator angegebenen Namen bereitgestellt.</li> </ul>
Einschränkungen	<ul style="list-style-type: none"> <li>■ Die Maschinen werden zeilenweise bereitgestellt. Wenn der Arbeitsablauf für eine Maschine fehlschlägt, werden die anderen Maschinen nicht bereitgestellt.</li> <li>■ Wenn Sie einen angegebenen Benennungspool auswählen, um im Textfeld für das Hinzufügen von Maschinennamen eine neue Zeile hinzuzufügen, drücken Sie Strg+Eingabe, um mehrere Namen hinzuzufügen. Wenn Sie nur die Eingabetaste drücken, wird keine neue Zeile hinzugefügt, sondern der Arbeitsablauf gesendet.</li> </ul>

## Desktop Assignment (Desktop-Zuweisung)

Zweck	Ermöglicht es einem delegierten Administrator, einen Benutzer einer bestimmten virtuellen Maschine zuzuweisen und dem Benutzer optional Berechtigungen für die Maschine zu gewähren. Gleichzeitig kann in demselben Arbeitsablauf die Zuweisung eines Benutzers zu einer virtuellen Maschine entfernt werden.
Eingaben/Parameter	Pod, Pool-ID, Maschinename, zuzuweisender Benutzer, Benutzer, dessen Zuweisung entfernt werden soll
Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen. Im Ordner vSphereWebClient ist keine Verknüpfung erforderlich.
Ergebnisse	Desktop-Zuweisungen können im selben Arbeitsablauf hinzugefügt und entfernt werden.

## Desktop Entitlement (Desktop-Berechtigung)

Zweck	Ermöglicht es einem delegierten Administrator, Benutzern Berechtigungen für einen Desktop-Pool zu gewähren oder die Berechtigungen zu entfernen.
Eingaben/Parameter	Pod, Pool-ID, zu berechtigende Benutzer sowie Benutzer, deren Berechtigungen entfernt werden sollen (Auswahl aus einer Standardliste)
Verknüpfungsanforderungen	In den Ordnern vCAC60 und vSphereWebClient muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen.
Ergebnisse	Berechtigungen können im selben Arbeitsablauf hinzugefügt und entfernt werden.

## Desktop Recycle (Desktop-Wiederverwendung)

Zweck	Dieser Arbeitsablauf für die Aufhebung von Bereitstellungen entfernt Benutzerzuweisungen oder -berechtigungen für den angegebenen virtuellen Desktop. Abhängig von der Poolrichtlinie wird die virtuelle Maschine ggf. gelöscht und vorhandene dauerhafte Festplatten werden möglicherweise gespeichert.
Eingaben/Parameter	Pod, Pool-ID, Benutzername
Geltungsbereich	Kann bei allen Pooltypen verwendet werden.
Voraussetzungen	Führen Sie den Arbeitsablauf „Add Pool Policy Configuration“ aus, bevor Sie diesen Arbeitsablauf ausführen.

Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen. Im Ordner vSphereWebClient ist keine Verknüpfung erforderlich. Wenn Sie den Arbeitsablauf mit einem Pod verknüpfen, wird in vSphere Web Client eine Dropdown-Liste der Pools und Benutzer mit Berechtigungen für den jeweiligen Pool angezeigt.
Ergebnisse	<p>Bei dynamischen Pools wird die Benutzerberechtigung entfernt. Bei anderen Desktop-Pooltypen wird die Benutzerzuweisung entfernt.</p> <p>Bei dedizierten Linked-Clone-Pools wird die virtuelle Maschine gelöscht und dauerhafte Festplatten werden entsprechend den Einstellungen im Arbeitsablauf „Add Pool Policy Configuration“ gespeichert.</p> <p>Bei Full-Clone-Pools wird die dauerhafte Festplatte beim Löschen der virtuellen Maschine ebenfalls gelöscht.</p>
Einschränkungen	<ul style="list-style-type: none"> <li>■ Dauerhafte Festplatten (manchmal auch als „User Data Disk“ oder UDD bezeichnet) können nur gespeichert werden, wenn es sich um einen automatisierten dedizierten Linked-Clone-Desktop-Pool handelt.</li> <li>■ Das Löschen der virtuellen Maschine wird bei dynamischen und manuellen Pools nicht unterstützt.</li> </ul>

## Desktop Refresh (Desktop-Aktualisierung)

Zweck	Setzt eine bestimmte virtuelle Maschine auf ihren Ausgangszustand zurück.
Eingaben/Parameter	Pod, Pool-ID, Maschinenname
Geltungsbereich	Kann nur bei automatisierten Linked-Clone-Pools von View Composer verwendet werden.
Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen. Im Ordner vSphereWebClient ist keine Verknüpfung erforderlich.
Ergebnisse	Bei virtuellen Linked-Clone-View Composer-Maschinen wird eine Warnung an den Benutzer gesendet, wenn eine aktive Sitzung vorhanden ist, und der Benutzer wird nach einer gewissen Zeit automatisch abgemeldet. Anschließend wird ein Aktualisierungsvorgang gestartet.

## Register Machines to Pool (Maschinen in einem Pool registrieren)

Zweck	<p>(Verfügbar mit dem Horizon vCenter Orchestrator-Plug-In 1.1) Registriert die angegebenen DNS-Namen der Maschinen in einem manuellen Pool nicht verwalteter Desktops in View. Verwenden Sie diesen Arbeitsablauf nur für physische Maschinen und nicht für mit vSphere bereitgestellte virtuelle Maschinen.</p> <p><b>Hinweis</b> Alternativ zu diesem Arbeitsablauf können Sie den Arbeitsablauf „Add Physical Machines to Pool“ (Physische Maschinen zu einem Pool hinzufügen) verwenden, der im Ordner Workflows/Example verfügbar ist. Dieser Arbeitsablauf kombiniert die in <a href="#">Ausführen von Arbeitsabläufen zum Hinzufügen physischer Maschinen als PowerShell-Hosts</a> vorgestellten Aktionen des Arbeitsablaufs „Maschinen in einem Pool registrieren“ und des PowerShell-Arbeitsablaufs. Vor dem Ausführen des Arbeitsablaufs „Add Physical Machines to Pool“ (Physische Maschinen zu einem Pool hinzufügen) müssen Sie die unter <a href="#">Konfiguration einer physischen Maschine für einen nicht verwalteten Pool</a> und <a href="#">Konfiguration von vCenter Orchestrator für die Verwendung der Kerberos-Authentifizierung mit physischen Maschinen</a> beschriebenen Aufgaben ausführen. Sie müssen außerdem die unter <a href="#">Voraussetzungen für das Hinzufügen von nicht verwalteten Maschinen zu Pools</a> aufgeführten Voraussetzungen erfüllen.</p>
Eingaben/Parameter	Pod, Pool-ID, DNS-Namen der Maschine, Gastbetriebssystem
Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen.

Ergebnisse	Bereitgestellte Maschinennamen werden im festgelegten nicht verwalteten Desktop-Pool in View registriert.
Einschränkungen	<ul style="list-style-type: none"> <li>■ Dieser Arbeitsablauf registriert sämtliche bereitgestellten DNS-Namen ohne irgendeine Validierung. Der Administrator muss das zurückgegebene Registrierungs-Token manuell an die registrierte Maschine übertragen.</li> <li>■ Drücken Sie Strg+Eingabe, um im Textfeld für die DNS-Namen eine neue Zeile hinzuzufügen. So können Sie mehrere DNS-Namen hinzufügen. Wenn Sie nur die Eingabetaste drücken, wird keine neue Zeile hinzugefügt, sondern der Arbeitsablauf gesendet.</li> <li>■ Um einen Windows Server 2008 R2-Computer zu registrieren, müssen Sie sich zuerst bei View Administrator anmelden, <b>View Configuration &gt; Global Settings &gt; General</b> (Globale Einstellungen/Allgemein) auswählen und auf <b>Edit</b> (Bearbeiten) klicken. Aktivieren Sie dann das Kontrollkästchen <b>Enable Windows Server 2008 R2 desktops</b> (Windows Server 2008 R2-Desktops aktivieren).</li> </ul>

## Remove Users from Application Pool (Benutzer aus Anwendungspool entfernen)

Zweck	Entfernt die Berechtigungen mehrerer Benutzer aus einem Anwendungspool.
Eingaben/Parameter	Pod, Pool-ID, Benutzer (ausgewählt aus einer Standardliste)
Verknüpfungsanforderungen	In den Ordnern vCAC60 und vSphereWebClient muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen.
Ergebnisse	Die angegebenen Benutzer sind nicht länger berechtigt, den angegebenen Anwendungspool zu verwenden.

## Remove Users from Desktop Pool (Benutzer aus Desktop-Pool entfernen)

Zweck	Entfernt die Berechtigungen mehrerer Benutzer aus einem Desktop-Pool.
Eingaben/Parameter	Pod, Pool-ID, Benutzer (ausgewählt aus einer Standardliste)
Verknüpfungsanforderungen	In den Ordnern vCAC60 und vSphereWebClient muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen.
Ergebnisse	Die angegebenen Benutzer sind nicht länger berechtigt, den angegebenen Desktop-Pool zu verwenden.

## Self-Service Desktop Allocation (Self-Service-Desktop-Zuordnung)

Zweck	Ermöglicht Endbenutzern, sich selbst eine Maschine zuzuordnen. Eine neue Maschine wird nur bei Desktops-Pools des Typs „specified naming“ (angegebene Benennung) bereitgestellt.
Eingaben/Parameter	Keine
Geltungsbereich	Kann nur bei automatisierten Pools verwendet werden.



Voraussetzungen/ Verknüpfungsanforderungen	<ul style="list-style-type: none"> <li>■ Im Ordner vCAC61 muss der Administrator den Arbeitsablauf „Manage Self Service Pool Configuration“ (Self-Service-Poolkonfiguration verwalten) ausführen, um festzulegen, welche Pools für die Endbenutzer als Auswahlmöglichkeit verfügbar sind.</li> <li>■ Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen. Dieser Arbeitsablauf ist im Ordner vSphereWebClient nicht verfügbar.</li> </ul>
Ergebnisse	<ul style="list-style-type: none"> <li>■ Bei dynamischen Desktop-Pools und sitzungsbasierten Pools von RDS-Hosts, werden dem Benutzer Berechtigungen für den Pool gewährt.</li> <li>■ Bei automatisch zugewiesenen dedizierten Pools werden dem Benutzer Berechtigungen für den Pool gewährt und der Benutzer wird einer verfügbaren Maschine zugewiesen (sofern vorhanden).</li> <li>■ Bei dedizierten Pools ohne automatisches Benennungsschema wird für den Benutzer eine virtuelle Maschine mit dem von Administrator angegebenen Namen bereitgestellt.</li> </ul>

## Self-Service Desktop Recycle (Self-Service-Desktop-Wiederverwendung)

Zweck	<p>Ermöglicht Endbenutzern, die Bereitstellung ihrer eigenen virtuellen Maschinen im angegebenen Pod und Desktop-Pool aufzuheben. Dieser Arbeitsablauf entfernt Benutzerberechtigungen und -zuweisungen.</p> <p>Abhängig von der Poolrichtlinie wird die virtuelle Maschine ggf. gelöscht und vorhandene dauerhafte Festplatten werden möglicherweise gespeichert.</p>
Eingaben/Parameter	Keine
Einschränkungen	<ul style="list-style-type: none"> <li>■ Dauerhafte Festplatten (manchmal auch als „User Data Disk“ oder UDD bezeichnet) können nur gespeichert werden, wenn es sich um einen automatisierten dedizierten Linked-Clone-Desktop-Pool handelt.</li> <li>■ Das Löschen der virtuellen Maschine wird bei dynamischen und manuellen Pools nicht unterstützt.</li> </ul>
Voraussetzungen/ Verknüpfungsanforderungen	<ul style="list-style-type: none"> <li>■ Im Ordner vCAC61 muss der Administrator den Arbeitsablauf „Manage Self Service Pool Configuration“ (Self-Service-Poolkonfiguration verwalten) ausführen, um festzulegen, welche Pools für die Endbenutzer als Auswahlmöglichkeit verfügbar sind.</li> <li>■ Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen. Dieser Arbeitsablauf ist im Ordner vSphereWebClient nicht verfügbar.</li> </ul>
Ergebnisse	<p>Bei dynamischen Pools wird die Benutzerberechtigung entfernt. Bei anderen Desktop-Pooltypen wird die Benutzerzuweisung entfernt.</p> <p>Bei dedizierten Linked-Clone-Pools wird die virtuelle Maschine gelöscht und dauerhafte Festplatten werden entsprechend den Einstellungen im Arbeitsablauf „Add Pool Policy Configuration“ gespeichert.</p> <p>Bei Full-Clone-Pools wird die dauerhafte Festplatte beim Löschen der virtuellen Maschine ebenfalls gelöscht.</p>

## Self-Service Desktop Refresh (Self-Service-Desktop-Aktualisierung)

Zweck	Setzt die virtuelle Maschine des Endbenutzers im angegebenen Desktop-Pool auf ihren Ausgangszustand zurück.
Eingaben/Parameter	Keine
Geltungsbereich	Kann nur bei automatisierten dedizierten Linked-Clone-Pools von View Composer verwendet werden.

Voraussetzungen/ Verknüpfungsanforderungen	<ul style="list-style-type: none"> <li>■ Im Ordner vCAC61 muss der Administrator den Arbeitsablauf „Manage Self Service Pool Configuration“ (Self-Service-Poolkonfiguration verwalten) ausführen, um festzulegen, welche Pools für die Endbenutzer als Auswahlmöglichkeit verfügbar sind.</li> <li>■ Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen. Dieser Arbeitsablauf ist im Ordner vSphereWebClient nicht verfügbar.</li> </ul>
Ergebnisse	Bei virtuellen Linked-Clone-View Composer-Maschinen wird eine Warnung an den Benutzer gesendet, wenn eine aktive Sitzung vorhanden ist, und der Benutzer wird nach einer gewissen Zeit automatisch abgemeldet. Anschließend wird ein Aktualisierungsvorgang gestartet.

## Self-Service Release Application (Anwendung im Self-Service freigeben)

Zweck	Ermöglicht es Endbenutzern, ihre Berechtigung aus dem angegebenen Anwendungspool zu entfernen.
Eingaben/Parameter	Keine
Voraussetzungen/ Verknüpfungsanforderungen	<ul style="list-style-type: none"> <li>■ Im Ordner vCAC61 muss der Administrator den Arbeitsablauf „Manage Self Service Pool Configuration“ (Self-Service-Poolkonfiguration verwalten) ausführen, um festzulegen, welche Pools für die Endbenutzer als Auswahlmöglichkeit verfügbar sind.</li> <li>■ Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen. Dieser Arbeitsablauf ist im Ordner vSphereWebClient nicht verfügbar.</li> </ul>

## Self-Service Request Application (Anwendung im Self-Service anfordern)

Zweck	Erlaubt Endbenutzern, eine Anwendung für die eigene Verwendung anzufordern. Der Benutzer erhält eine Berechtigung für den angegebenen Anwendungspool.
Eingaben/Parameter	Keine
Voraussetzungen/ Verknüpfungsanforderungen	<ul style="list-style-type: none"> <li>■ Im Ordner vCAC61 muss der Administrator den Arbeitsablauf „Manage Self Service Pool Configuration“ (Self-Service-Poolkonfiguration verwalten) ausführen, um festzulegen, welche Pools für die Endbenutzer als Auswahlmöglichkeit verfügbar sind.</li> <li>■ Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen. Dieser Arbeitsablauf ist im Ordner vSphereWebClient nicht verfügbar.</li> </ul>

## Session Management (Sitzungsverwaltung)

Zweck	(Verfügbar mit dem Horizon vCenter Orchestrator-Plug-In 1.1) Ermöglicht einem delegierten Administrator das Trennen, Abmelden, Zurücksetzen und Senden von Nachrichten an aktive Horizon Desktop-Sitzungen. Delegierte Administratoren können diese Vorgänge auch für Benutzersitzungen ausführen.
Eingaben/Parameter	Pod, Pool-ID, Vorgang, Nachricht (für den Vorgang des Nachrichtensendens), Benutzername und weitere Optionen
Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen.

Ergebnisse	Der ausgewählte Vorgang wird in der festgelegten Sitzung ausgeführt.
Einschränkungen	<ul style="list-style-type: none"> <li>■ Es werden keine Anwendungssitzungen unterstützt.</li> <li>■ Der Zurücksetzungsvorgang wird für RDS-Pools und manuelle nicht verwaltete Desktop-Pools nicht unterstützt.</li> <li>■ Die Auswahl mehrerer Sitzungen wird nicht unterstützt, wenn der Arbeitsablauf über den vSphere Web Client oder den Orchestrator-Client ausgeführt wird.</li> <li>■ Die vordefinierte Benutzerliste wird nicht angezeigt, wenn der Arbeitsablauf aus vCloud Automation Center 6.0 ausgeführt wird.</li> </ul>

## Wartungsmodus einstellen

Zweck	(Verfügbar mit dem Horizon vCenter Orchestrator-Plug-In 1.1) Erlaubt es einem delegierten Administrator, Maschinen in den Wartungsmodus zu versetzen und den Wartungsmodus für Maschinen zu beenden.
Eingaben/Parameter	Pod, Pool-ID, Vorgang, virtuelle Maschine
Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen.
Ergebnisse	Die ausgewählten Maschinen werden in den Wartungsmodus versetzt oder der Wartungsmodus für die angegebenen Maschinen wird beendet.
Einschränkungen	Dieser Arbeitsablauf wird für RDS-Pools und manuelle nicht verwaltete Desktop-Pools nicht unterstützt.

## Benutzerzuweisung aufheben

Zweck	Entfernt die Zuweisung eines Benutzers zu einer virtuellen Maschine.
Eingaben/Parameter	Pod, Pool-ID, Maschinenname (wie in der Benutzeroberfläche von View Administrator angezeigt)
Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen. Im Ordner vSphereWebClient ist keine Verknüpfung erforderlich.
Ergebnisse	Die Zuweisung des Benutzers wird entfernt. Die Berechtigung des Benutzers für den Pool bleibt unverändert. Die Sitzung des Benutzers wird abgemeldet.

## Update App Pool Display Name (Anzeigenamen des Anwendungspools aktualisieren)

Zweck	Ändert den Anzeigenamen eines Anwendungspools.
Eingaben/Parameter	Pod, Pool-ID, neuer Anzeigename für den Pool
Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen. Im Ordner vSphereWebClient ist keine Verknüpfung erforderlich.
Ergebnisse	Der Anzeigename wird geändert, die Pool-ID bleibt jedoch dieselbe.

## Update Desktop Pool Display Name (Anzeigenamen des Desktop-Pools aktualisieren)

Zweck	Ändert den Anzeigenamen eines Desktop-Pools.
Eingaben/Parameter	Pod, Pool-ID, neuer Anzeigename für den Pool

Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen. Im Ordner vSphereWebClient ist keine Verknüpfung erforderlich.
Ergebnisse	Der Anzeigename wird geändert, die Pool-ID bleibt jedoch dieselbe.

## Update Desktop Pool Min Size (Mindestgröße des Desktop-Pools aktualisieren)

Zweck	Ändert die Mindestanzahl an Desktops, die der Pool enthält.
Geltungsbereich	Kann nur für automatisierte dynamische und automatisierte dedizierte Pools verwendet werden, die ein Benennungsmuster verwenden.
Eingaben/Parameter	Pod, Pool-ID, Wert für die minimale Poolgröße (Ganzzahl)
Ergebnisse	Die Mindestanzahl an virtuellen Maschinen im Pool wird geändert.  <b>Hinweis</b> Prüfen Sie, ob genügend Hardwareressourcen im Unternehmen zur Verfügung stehen, bevor Sie diese Zahl erhöhen.
Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen. Im Ordner vSphereWebClient ist keine Verknüpfung erforderlich.

## Update Desktop Pool Spare Size (Reservegröße des Desktop-Pools aktualisieren)

Zweck	Ändert die Anzahl der eingeschalteten Reservemaschinen im Pool, die für neue Benutzer verfügbar sind.
Geltungsbereich	Kann nur bei automatisierten Pools verwendet werden.
Eingaben/Parameter	Pod, Pool-ID, Anzahl der bereitzuhaltenden Reservemaschinen (Ganzzahl)
Verknüpfungsanforderungen	Im Ordner vCAC60 muss der Administrator diesen Arbeitsablauf mit einem Pool und einem Pod verknüpfen. Im Ordner vSphereWebClient ist keine Verknüpfung erforderlich.
Ergebnisse	Ändert die Anzahl der virtuellen Reservemaschinen, die im Pool eingeschaltet bleiben und für neue Benutzer bereitgehalten werden.  <b>Hinweis</b> Prüfen Sie, ob genügend Hardwareressourcen im Unternehmen zur Verfügung stehen, bevor Sie diese Zahl erhöhen.

## Syntax für die Angabe von Benutzerkonten in den Arbeitsabläufen

Für alle Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins wird die gleiche Syntax zum Angeben von Benutzern verwendet.

Wenn Sie einen Benutzernamen angeben, müssen Sie den Benutzer und die Domäne in einem der folgenden Formate angeben:

- benutzername@domäne.com
- benutzername@domäne
- domäne.com\benutzername

- domäne\benutzername

---

**Wichtig** Es werden nur ASCII-Zeichen unterstützt.

---

# Verfügbar machen der Arbeitsabläufe in vSphere Web Client und vCloud Automation Center

## 4

Administratoren können die View-Arbeitsabläufe im Dienstkatalog von vCloud Automation Center oder in vSphere Web Client verfügbar machen. Außerdem können Administratoren die Arbeitsabläufe mit spezifischen Pools verknüpfen. Delegierte Administratoren können dann einen Pool auswählen und in einer Dropdown-Liste berechnete Benutzer auswählen.

Bevor Endbenutzer und delegierte Administratoren Arbeitsabläufe in vCloud Automation Center ausführen, müssen Sie angeben, auf welche Pools die Arbeitsabläufe angewendet werden sollen. Bei einigen Arbeitsabläufen, die delegierte Administratoren in vSphere Web Client ausführen, müssen Sie angeben, auf welche Pods oder Pools die Arbeitsabläufe angewendet werden sollen.

Dieses Kapitel enthält die folgenden Themen:

- [Verfügbar machen der Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins in vSphere Web Client](#)
- [Verfügbar machen der Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins in vCloud Automation Center](#)

## Verfügbar machen der Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins in vSphere Web Client

Administratoren können die Horizon-Arbeitsabläufe so konfigurieren, dass diese von delegierten Administratoren in vSphere Web Client ausgeführt werden können. Delegierte Administratoren können nach dem Namen eines bestimmten Arbeitsablaufs suchen und vCenter Orchestrator-Arbeitsabläufe ausführen und planen.

## Verknüpfen von vSphereWebClient-Arbeitsabläufen mit bestimmten Pods und Pools in vCenter Orchestrator

Wenn der Zugriff eines delegierten Administrators auf bestimmte Pools oder Pods beschränkt werden muss, können Sie einen Arbeitsablauf mit einem bestimmten Pool oder Pod verknüpfen. Administratoren können Arbeitsabläufe duplizieren und nach Bedarf mit unterschiedlichen Pools verknüpfen.

Nachdem ein Administrator einen Arbeitsablauf mit einem Pod verknüpft hat, wird dem delegierten Administrator in vSphere Web Client eine Dropdown-Liste mit den Pools angezeigt, die zu diesem Pod gehören. Sie können den Arbeitsablauf aber auch mit einem bestimmten Pool verknüpfen und die Dropdown-Liste der Pools deaktivieren. Dropdown-Listen mit Pools werden von den meisten Arbeitsabläufen unterstützt. Dabei spielt es keine Rolle, ob die Arbeitsabläufe lokalisiert wurden.

**Wichtig** Bei den folgenden Arbeitsabläufen müssen Sie, wenn Sie eine Lokalisierung der Arbeitsabläufe planen, den Arbeitsablauf mit einem bestimmten Pool verknüpfen und die Dropdown-Liste mit Pools deaktivieren:

- Application Entitlement (Anwendungsberechtigung)
- Benutzer zuweisen
- Desktop Assignment (Desktop-Zuweisung)
- Desktop Entitlement (Desktop-Berechtigung)
- Benutzerzuweisung aufheben

#### Voraussetzungen

- Stellen Sie sicher, dass Sie über Administratoranmeldeinformationen für den Orchestrator-Server verfügen. Das Konto muss Mitglied der Gruppe „vCenter Orchestrator Admin“ sind, die für die Authentifizierung über vCenter Single Sign-On konfiguriert ist.
- Stellen Sie sicher, dass eine Verbindung mit dem View Pod hergestellt wurde, indem Sie den Arbeitsablauf „Add View Pod in Configuration“ (View Pod in Konfiguration einschließen) ausführen. Siehe [Konfigurieren der Verbindung mit einem View Pod](#).
- Stellen Sie sicher, dass Sie den Pools, die Sie in vSphere Web Client verfügbar machen möchten, die richtigen delegierten Administratoren zugewiesen haben. Siehe [Zuweisen delegierter Administratoren zu Pools](#).

#### Verfahren

- 1 Melden Sie sich als Administrator beim Orchestrator-Client an und wählen Sie im oberen linken Bereich des Bildschirms im Dropdown-Menü die Option **Design** (Entwurf) aus.
- 2 Wählen Sie in der hierarchischen Liste der Arbeitsabläufe **Bibliothek > Horizon** aus, und navigieren Sie zu dem Unterordner und Arbeitsablauf.  
  
Sie können z. B. zum Arbeitsablauf „Add User(s) to Desktop Pool“ in **Bibliothek > Horizon > Arbeitsabläufe > vSphereWebClient** navigieren.
- 3 Klicken Sie mit der rechten Maustaste auf den Arbeitsablauf, wählen Sie **Duplicate Workflow** (Arbeitsablauf duplizieren) und füllen Sie das Formular aus.  
  
Der neue Arbeitsablauf wird in dem von Ihnen ausgewählten Ordner gespeichert.
- 4 Wählen Sie im linken Bereich den neu erstellten Arbeitsablauf aus, klicken Sie im rechten Bereich auf die Registerkarte **Presentation** (Präsentation) und klicken Sie in der Symbolleiste über dem Bereich auf das (Stift-)Symbol **Bearbeiten**.

- 5 Wählen Sie im oberen Bereich der Registerkarte **(string)podAlias *Horizon View Pod*** aus und bearbeiten Sie die Eigenschaften.
  - a Klicken Sie im unteren Bereich der Registerkarte auf die Registerkarte **Properties** (Eigenschaften) und geben Sie in der Zeile **Data Binding** (Datenverknüpfung) den Pod-Namen in Anführungszeichen ein. Beispiel: **"ViewPod1"**.
  - b Wählen Sie die Eigenschaft **Predefined answers** (Vordefinierte Antworten) aus und löschen Sie sie.
  - c Fügen Sie die Eigenschaft **Default value** (Standardwert) hinzu und geben Sie denselben Pod-Namen in Anführungszeichen ein.

Wenn Sie die Eigenschaft **Predefined answers** (Vordefinierte Antworten) nicht löschen und die Eigenschaft **Default value** (Standardwert) nicht festlegen, wird ggf. eine Dropdown-Liste mit Pods in vSphere Web Client angezeigt, auch wenn der Arbeitsablauf nur mit einem Pod verknüpft ist.

- 6 Um den Arbeitsablauf mit nur einem Pool zu verknüpfen, wählen Sie im oberen Bereich der Registerkarte **(string)poolId *Desktop Pool ID*** aus und bearbeiten Sie die Eigenschaften.
  - a Klicken Sie im unteren Bereich der Registerkarte auf die Registerkarte **Properties** (Eigenschaften) und geben Sie in der Zeile **Data Binding** (Datenverknüpfung) die Pool-ID in Anführungszeichen ein, z. B. **"DesktopPool"**.
  - b Wählen Sie die Eigenschaft **Predefined answers** (Vordefinierte Antworten) aus und löschen Sie sie.
  - c Fügen Sie die Eigenschaft **Default value** (Standardwert) hinzu und geben Sie denselben Poolnamen in Anführungszeichen ein.

Wenn Sie die Eigenschaft **Predefined answers** (Vordefinierte Antworten) nicht löschen und die Eigenschaft **Default value** (Standardwert) nicht festlegen, wird ggf. eine Dropdown-Liste mit Pools in vSphere Web Client angezeigt, auch wenn der Arbeitsablauf nur mit einem Pool verknüpft ist.

Beim Starten dieses Arbeitsablaufs sind der Pod-Name und die Pool-ID bereits eingetragen und können nicht geändert werden.

#### Nächste Schritte

Erstellen Sie Versionen des Arbeitsablaufs in anderen Sprachen.

## Erstellen lokalisierter Versionen eines Arbeitsablaufs für vSphere Web Client

Zum Erstellen der Lokalisierungsressourcen für vSphere Web Client können Administratoren den Arbeitsablauf „Clone Localization Resources“ aus dem Ordner „Configuration“ ausführen.

#### Voraussetzungen

- Verknüpfen Sie den Arbeitsablauf mit einem Pod und optional mit einem Pool. Siehe [Verknüpfen von vSphereWebClient-Arbeitsabläufen mit bestimmten Pods und Pools in vCenter Orchestrator](#).



- Stellen Sie sicher, dass Sie über Administratoranmeldeinformationen für den Orchestrator-Server verfügen. Das Konto muss Mitglied der Gruppe „vCenter Orchestrator Admin“ sind, die für die Authentifizierung über vCenter Single Sign-On konfiguriert ist.

## Verfahren

- 1 Melden Sie sich als Administrator beim Orchestrator-Client an und wählen Sie im oberen linken Bereich des Bildschirms im Dropdown-Menü die Option **Design** (Entwurf) aus.
- 2 Klicken Sie auf die Ansicht **Resources** (Ressourcen) und navigieren Sie zu dem Ordner, der den duplizierten Arbeitsablauf enthält, den Sie mit einem Pod verknüpft haben.
- 3 Erstellen Sie in diesem Ordner einen Unterordner mit demselben Namen, der für den duplizierten Arbeitsablauf verwendet wurde.  
  
Der Ordnername muss exakt mit dem Namen des duplizierten Arbeitsablaufs übereinstimmen und der Ordner muss sich in demselben Ordner wie der Arbeitsablauf befinden.
- 4 Klicken Sie auf die Ansicht **Arbeitsabläufe** und navigieren Sie zu **Bibliothek > Horizon > - Konfiguration**.
- 5 Erweitern Sie das Element **Konfiguration**, klicken Sie mit der rechten Maustaste auf den Arbeitsablauf **Clone localization resources (Lokalisierungsressourcen klonen)** und wählen Sie **Arbeitsablauf starten**.
- 6 Füllen Sie das angezeigte Formular aus.

Option	Aktion
<b>Source Workflow (Quellarbeitsablauf)</b>	Klicken Sie auf <b>Not Set</b> (Nicht festgelegt) und wählen Sie den ursprünglichen Arbeitsablauf aus, den Sie für das Verknüpfen mit einem Pod dupliziert haben.
<b>Target Workflow (Zielarbeitsablauf)</b>	Klicken Sie auf <b>Not Set</b> (Nicht festgelegt) und wählen Sie den Arbeitsablauf aus, den Sie dupliziert haben.

- 7 Klicken Sie auf **Senden**, um den Arbeitsablauf auszuführen.

Wenn der Arbeitsablauf erfolgreich abgeschlossen wurde, wechseln Sie zur Ansicht **Resources** (Ressourcen) und erweitern Sie den Ordner, den Sie erstellt haben. In dem Ordner sind nun Eigenschaftendateien für die einzelnen Sprachen verfügbar.

## Verfügbar machen der Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins in vCloud Automation Center

vCloud Automation Center stellt einen Dienstkatalog mit einem Anforderungs- und Genehmigungsmodul bereit, das eine genaue Kontrolle der Arbeitsabläufe mithilfe von Berechtigungen und Überwachung erlaubt. Die in Orchestrator im Ordner vCAC60 enthaltenen Arbeitsabläufe wurden für die Ausführung in vCloud Automation Center erstellt. Der Administrator muss diese Arbeitsabläufe konfigurieren, bevor sie delegierten Administratoren und Endbenutzern zur Verfügung gestellt werden können.

Um Dienstvorlagen hinzuzufügen, können Administratoren **Orchestrator > Bibliothek > Horizon** öffnen und dort einen bestimmten Arbeitsablauf auswählen. Für Veröffentlichungen und Berechtigungsvergabe können Sie die normalen vCloud Automation Center-Verfahren für die Katalogverwaltung verwenden. Da üblicherweise sehr spezifische Berechtigungen vergeben werden, wenn der Arbeitsablauf in vCloud Automation Center verwendet wird, müssen Sie den Arbeitsablauf mit einem bestimmten View Pod, Desktop- oder Anwendungspool verknüpfen.

## Verfahren

### 1 Erstellen von Unternehmensgruppen für delegierte Administratoren und Endbenutzer

In vCloud Automation Center müssen Benutzer einer Unternehmensgruppe angehören, damit ihnen die Berechtigung zur Verwendung eines Diensts gewährt werden kann, der für einen View-Plug-In-Arbeitsablauf erstellt wurde.

### 2 Erstellen von Diensten für delegierte Administratoren und Endbenutzer

Administratoren müssen in vCloud Automation Center einen Dienst erstellen, um Benutzern Berechtigungen für Katalogelemente zu gewähren.

### 3 Erstellen von Berechtigungen für delegierte Administratoren und Endbenutzer

Zum Erstellen einer Berechtigung in vCloud Automation Center geben Administratoren eine Unternehmensgruppe und den Dienst an, der dieser Gruppe entspricht.

### 4 Verknüpfen von vCAC60-Arbeitsabläufen mit bestimmten Pods und Pools in vCloud Automation Center

Um einen Arbeitsablauf im Dienstkatalog von vCloud Automation Center verfügbar zu machen, muss der Administrator den Arbeitsablauf in vCloud Automation Center mit einem bestimmten Pod und Pool verknüpfen.

### 5 vCAC61-Arbeitsabläufe mit einem vCAC-Benutzer verknüpfen

Einer der für die Arbeitsabläufe im Ordner vCAC61 erforderlichen Parameter ist „vCAC User“. Sie müssen konfigurieren, dass dieser Parameter durch eine Prinzipal-ID angefordert wird.

### 6 vCAC61-Self-Service-Arbeitsabläufe für die Verwendung bestimmter Pools konfigurieren

Sie können einen Arbeitsablauf ausführen, der die Pools einschränkt, die über die Self-Service-Arbeitsabläufe von vCloud Automation Center verfügbar sind.

### 7 Ausgabeparameter für vCAC61-Arbeitsabläufe konfigurieren

Für Arbeitsabläufe, die Ausgabeparameter zurückgeben, können Sie die Ausgabeparameter zum Dienst-Blueprint hinzufügen.

### 8 Konfigurieren des Katalogelements für den Arbeitsablauf

Administratoren können Arbeitsabläufe in vCloud Automation Center so konfigurieren, dass sie im Katalog für delegierte Administratoren und Endbenutzer angezeigt werden.

## Erstellen von Unternehmensgruppen für delegierte Administratoren und Endbenutzer

In vCloud Automation Center müssen Benutzer einer Unternehmensgruppe angehören, damit ihnen die Berechtigung zur Verwendung eines Diensts gewährt werden kann, der für einen View-Plug-In-Arbeitsablauf erstellt wurde.

Wenn Sie vCloud Automation Center bereits verwenden, wurden ggf. schon Unternehmensgruppen oder äquivalente Gruppen erstellt.

### Voraussetzungen

- Stellen Sie sicher, dass Sie über Administratoranmeldeinformationen für den Orchestrator-Server verfügen. Das Konto muss Mitglied der Gruppe „vCenter Orchestrator Admin“ sind, die für die Authentifizierung über vCenter Single Sign-On konfiguriert ist.
- Machen Sie sich mit den Verfahren zum Erstellen von Gruppen in vCloud Automation Center vertraut. Die Dokumentation zu vCloud Automation Center erhalten Sie unter <https://www.vmware.com/support/pubs/vcac-pubs.html>.

### Verfahren

- 1 Melden Sie sich als Administrator bei vCloud Automation Center an.
- 2 Klicken Sie auf die Registerkarte **Infrastructure** (Infrastruktur).
- 3 Wählen Sie **Groups (Gruppen) > Fabric Groups (Fabric-Gruppen)** aus und erstellen Sie eine Fabric-Gruppe mit dem Administrator als Mitglied.
- 4 Klicken Sie auf **Business Groups** (Unternehmensgruppen) und erstellen Sie eine Unternehmensgruppe für delegierte Administratoren.

Option	Aktion
Rolle "Group manager" (Gruppenmanager)	Verwenden Sie das Administratorkonto, das Sie der Fabric-Gruppe hinzugefügt haben.
Rolle "Users" (Benutzer)	Fügen Sie die delegierten Administratorbenutzer hinzu.

- 5 Klicken Sie auf **OK**, um die neue Gruppe hinzuzufügen.
- 6 Klicken Sie auf **Business Groups** (Unternehmensgruppen) und erstellen Sie eine Unternehmensgruppe für Endbenutzer.

Option	Aktion
Rolle "Group manager" (Gruppenmanager)	Verwenden Sie das Administratorkonto, das Sie der Fabric-Gruppe hinzugefügt haben.
Rolle "Users" (Benutzer)	Fügen Sie die Endbenutzer hinzu.

- 7 Klicken Sie auf **OK**, um die neue Gruppe hinzuzufügen.

## Nächste Schritte

Erstellen Sie entsprechende Dienste für delegierte Administratoren und Endbenutzer.

## Erstellen von Diensten für delegierte Administratoren und Endbenutzer

Administratoren müssen in vCloud Automation Center einen Dienst erstellen, um Benutzern Berechtigungen für Katalogelemente zu gewähren.

Wenn Sie vCloud Automation Center bereits verwendet haben, wurden diese oder äquivalente Dienste möglicherweise schon erstellt.

### Voraussetzungen

- Stellen Sie sicher, dass Sie über Administratoranmeldeinformationen für den Orchestrator-Server verfügen. Das Konto muss Mitglied der Gruppe „vCenter Orchestrator Admin“ sind, die für die Authentifizierung über vCenter Single Sign-On konfiguriert ist.
- Machen Sie sich mit den Verfahren für das Erstellen von Diensten in vCloud Automation Center vertraut. Die Dokumentation zu vCloud Automation Center erhalten Sie unter <https://www.vmware.com/support/pubs/vcac-pubs.html>.

### Verfahren

- 1 Melden Sie sich als Administrator bei vCloud Automation Center an.
- 2 Klicken Sie auf die Registerkarte **Administration** (Verwaltung).
- 3 Wählen Sie **Catalog Management (Katalogverwaltung) > Services (Dienste)** aus.
- 4 Erstellen Sie einen Dienst für die Unternehmensgruppe der delegierten Administratoren.
  - a Klicken Sie auf das Symbol **Add Service (+)** (Dienst hinzufügen).
  - b Geben Sie auf der Registerkarte **Details** (Details) einen Namen an und wählen Sie in der Liste **Status** (Status) die Option **Active** (Aktiv) aus.
  - c Klicken Sie auf **Hinzufügen**.
- 5 Wiederholen Sie die Schritte für die Unternehmensgruppe der Endbenutzer.

## Nächste Schritte

Erstellen Sie Berechtigungen für delegierte Administratoren und Endbenutzer.

## Erstellen von Berechtigungen für delegierte Administratoren und Endbenutzer

Zum Erstellen einer Berechtigung in vCloud Automation Center geben Administratoren eine Unternehmensgruppe und den Dienst an, der dieser Gruppe entspricht.

Wenn Sie vCloud Automation Center bereits verwendet haben, wurden diese oder äquivalente Berechtigungen möglicherweise schon erstellt.

## Voraussetzungen

- Stellen Sie sicher, dass Sie über Administratoranmeldeinformationen für den Orchestrator-Server verfügen. Das Konto muss Mitglied der Gruppe „vCenter Orchestrator Admin“ sind, die für die Authentifizierung über vCenter Single Sign-On konfiguriert ist.
- Erstellen Sie die Unternehmensgruppen, die die Benutzer enthalten, denen Sie Berechtigungen erteilen möchten. Siehe [Erstellen von Unternehmensgruppen für delegierte Administratoren und Endbenutzer](#).
- Erstellen Sie die zu den Unternehmensgruppen, denen Sie Berechtigungen erteilen möchten, gehörenden Dienste. Siehe [Erstellen von Diensten für delegierte Administratoren und Endbenutzer](#).
- Machen Sie sich mit den Verfahren zum Erstellen von Berechtigungen in vCloud Automation Center vertraut. Die Dokumentation zu vCloud Automation Center erhalten Sie unter <https://www.vmware.com/support/pubs/vcac-pubs.html>.

## Verfahren

- 1 Melden Sie sich als Administrator bei vCloud Automation Center an.
- 2 Klicken Sie auf die Registerkarte **Administration** (Verwaltung).
- 3 Wählen Sie **Catalog Management (Katalogverwaltung) > Entitlements (Berechtigungen)** aus.
- 4 Erstellen Sie eine Berechtigung für delegierte Administratoren.
  - a Klicken Sie auf das Symbol **Add Entitlement (+)** (Berechtigung hinzufügen).
  - b Geben Sie auf der Registerkarte **Details** (Details) einen Namen an und wählen Sie in der Liste **Status** (Status) die Option **Active** (Aktiv) aus.
  - c Wählen Sie in der Liste **Unternehmensgruppe** die eben erstellte Unternehmensgruppe für delegierte Administratoren aus.
  - d Geben Sie im Feld **Users & Groups** (Benutzer und Gruppen) Benutzer aus der Unternehmensgruppe für die delegierten Administratoren an und klicken Sie auf **Weiter**.
  - e Klicken Sie auf der Registerkarte **Items & Approvals** (Elemente und Genehmigungen) auf das Symbol **Add (+)** (Hinzufügen) für **Entitled Services** (Berechtigte Dienste) und wählen Sie den zuvor erstellten Dienst für delegierte Administratoren aus.
  - f Klicken Sie auf **Add (Hinzufügen)**.
- 5 Wiederholen Sie die Schritte für die Berechtigung der Endbenutzer.

## Nächste Schritte

Verknüpfen Sie Arbeitsabläufe des Horizon vCenter Orchestrator-Plug-Ins mit Pods und Pools.

## Verknüpfen von vCAC60-Arbeitsabläufen mit bestimmten Pods und Pools in vCloud Automation Center

Um einen Arbeitsablauf im Dienstkatalog von vCloud Automation Center verfügbar zu machen, muss der Administrator den Arbeitsablauf in vCloud Automation Center mit einem bestimmten Pod und Pool verknüpfen.

Arbeitsabläufe, die in vCloud Automation Center verfügbar gemacht werden, können mit dem Formular-Editor von vCloud Automation Center angepasst werden. Sie können Felder ausblenden oder neu anordnen und kosmetische Änderungen vornehmen, um die Formulare an den Dienstkatalog des Unternehmens anzupassen. Fügen Sie den Blueprint für den jeweiligen Arbeitsablauf hinzu und bearbeiten Sie ihn nach Bedarf. Sie können jedes Arbeitsablauffeld in ein Textfeld umwandeln oder vorgegebene Anzeigewerte hinzufügen, sodass die Benutzer aus einer Dropdown-Liste auswählen können.

### Voraussetzungen

- Stellen Sie sicher, dass Sie über Administratoranmeldeinformationen für den Orchestrator-Server verfügen. Das Konto muss Mitglied der Gruppe „vCenter Orchestrator Admin“ sind, die für die Authentifizierung über vCenter Single Sign-On konfiguriert ist.
- Stellen Sie sicher, dass eine Verbindung mit dem View Pod hergestellt wurde, indem Sie den Arbeitsablauf „Add View Pod in Configuration“ (View Pod in Konfiguration einschließen) ausführen. Siehe [Konfigurieren der Verbindung mit einem View Pod](#).
- Stellen Sie sicher, dass vCloud Automation Center für die Kommunikation mit dem vCenter Orchestrator-Server konfiguriert wurde, sodass die vCenter Orchestrator-Arbeitsabläufe verfügbar sind.
- Stellen Sie sicher, dass Sie über den Pod-Aliasnamen und die Pool-IDs verfügen. Den Pod-Alias haben Sie beim Durchführen der Vorgehensweise unter [Konfigurieren der Verbindung mit einem View Pod](#) angegeben. Die Pool-IDs entsprechen den Desktop- oder Anwendungs-Pool-IDs, die in View Administrator angezeigt werden.

### Verfahren

- 1 Melden Sie sich als Administrator bei vCloud Automation Center an.
- 2 Wählen Sie **Advanced Services (Erweiterte Dienste) > Service Blueprints (Dienst-Blueprints)** aus.
- 3 Klicken Sie auf das Symbol **Blueprint hinzufügen (+)**.
- 4 Wählen Sie in der Arbeitsablaufbibliothek von vCenter Orchestrator einen Arbeitsablauf aus dem Ordner **Bibliothek > Horizon > Arbeitsabläufe > vCAC60** aus.
- 5 Klicken Sie auf **Weiter** und geben Sie den Namen und die Beschreibung des Arbeitsablaufs an, die im Dienstkatalog von vCloud Automation Center angezeigt werden sollen.

**6** Klicken Sie auf **Weiter** und bearbeiten Sie auf der Registerkarte **Blueprint-Formular** das Feld **PodAlias**.

- a Klicken Sie in das Textfeld **PodAlias** und klicken Sie dann auf das (Stift-)Symbol **Bearbeiten**.
- b Klicken Sie im Dialogfeld „Edit Form Field - PodAlias“ auf die Registerkarte **Einschränkungen** und konfigurieren Sie die folgenden Felder.

Option	Aktion
<b>Wert</b>	Wählen Sie <b>Konstante</b> und geben Sie den Pod-Alias an, den Sie beim Ausführen des Arbeitsablaufs „Add View Pod in Configuration“ konfiguriert haben.
<b>Sichtbar</b>	Vergewissern Sie sich, dass <b>Nein</b> ausgewählt ist.

- c Klicken Sie auf **Senden**.

**7** Bearbeiten Sie das Feld **PoolIds**.

- a Klicken Sie in das Textfeld **PoolIds** und klicken Sie dann auf das (Stift-)Symbol **Bearbeiten**.  
Das Dialogfeld „Edit Form Field - PoolIds“ wird angezeigt.
- b Wählen Sie zum Erstellen einer Dropdown-Liste mit Pools auf der Registerkarte **Details** (Details) in der Liste **Type** (Typ) die Option **Drop-down** aus. Nehmen Sie andernfalls keine Änderungen auf dieser Registerkarte vor.
- c Klicken Sie auf die Registerkarte **Einschränkungen** und konfigurieren Sie die folgenden Felder.

Option	Aktion
<b>Wert</b>	<ul style="list-style-type: none"> <li>■ Wenn Sie diesen Arbeitsablauf mit einem einzelnen Pool verknüpfen möchten, wählen Sie <b>Constant</b> (Konstante) aus und geben Sie die Pool-ID aus View Administrator an.</li> <li>■ Wenn Sie eine Dropdown-Liste erstellen möchten, wählen Sie <b>Not Set</b> (Nicht festgelegt) aus.</li> </ul>
<b>Sichtbar</b>	<ul style="list-style-type: none"> <li>■ Wenn Sie diesen Arbeitsablauf mit einem einzelnen Pool verknüpfen möchten, stellen Sie sicher, dass <b>Nein</b> ausgewählt ist.</li> <li>■ Wenn Sie eine Dropdown-Liste erstellen möchten, stellen Sie sicher, dass <b>Yes</b> (Ja) ausgewählt ist.</li> </ul>

- d Wenn Sie eine Dropdown-Liste erstellen möchten, fügen Sie auf der Registerkarte **Values** (Werte) mehrere Pool-IDs und Anzeigenamen hinzu.
- e Klicken Sie auf **Senden**.

**8** Klicken Sie auf der Registerkarte **Blueprint-Formular** auf **Weiter**.

**9** Klicken Sie auf der Registerkarte **Bereitgestellte Ressource** auf **Add** (Hinzufügen).

Der Blueprint wird auf der Seite „Service Blueprints“ (Dienst-Blueprints) mit dem Status „Draft“ (Entwurf) hinzugefügt.

- 10 Um den Blueprint zu veröffentlichen, wählen Sie in der Liste **Actions** (Aktionen) für den Blueprint die Option **Publish** (Veröffentlichen) aus.

Das Element wird jetzt auf der Registerkarte **Administrator (Administrator) > Catalog Management (Katalogverwaltung) > Catalog Items (Katalogelemente)** angezeigt.

### Nächste Schritte

Konfigurieren Sie das Katalogelement für diesen Dienst.

## vCAC61-Arbeitsabläufe mit einem vCAC-Benutzer verknüpfen

Einer der für die Arbeitsabläufe im Ordner vCAC61 erforderlichen Parameter ist „vCAC User“. Sie müssen konfigurieren, dass dieser Parameter durch eine Prinzipal-ID angefordert wird.

Dieses Verfahren gilt nur für Arbeitsabläufe, die von delegierten Administratoren ausgeführt werden. Informationen zu den Self-Service-Arbeitsabläufen für Endbenutzer im Ordner vCAC61 finden Sie unter [vCAC61-Self-Service-Arbeitsabläufe für die Verwendung bestimmter Pools konfigurieren](#).

Arbeitsabläufe, die in vCloud Automation Center verfügbar gemacht werden, können mit dem Formular-Editor von vCloud Automation Center angepasst werden. Sie können Felder ausblenden oder neu anordnen und kosmetische Änderungen vornehmen, um die Formulare an den Dienstkatalog des Unternehmens anzupassen. Fügen Sie den Blueprint für den jeweiligen Arbeitsablauf hinzu und bearbeiten Sie ihn nach Bedarf. Sie können jedes Arbeitsablauffeld in ein Textfeld umwandeln oder vorgegebene Anzeigewerte hinzufügen, sodass die Benutzer aus einer Dropdown-Liste auswählen können.

### Voraussetzungen

- Stellen Sie sicher, dass Sie über Administratoranmeldeinformationen für den Orchestrator-Server verfügen. Das Konto muss Mitglied der Gruppe „vCenter Orchestrator Admin“ sind, die für die Authentifizierung über vCenter Single Sign-On konfiguriert ist.
- Stellen Sie sicher, dass eine Verbindung mit dem View Pod hergestellt wurde, indem Sie den Arbeitsablauf „Add View Pod in Configuration“ (View Pod in Konfiguration einschließen) ausführen. Siehe [Konfigurieren der Verbindung mit einem View Pod](#).
- Stellen Sie sicher, dass vCloud Automation Center für die Kommunikation mit dem vCenter Orchestrator-Server konfiguriert wurde, sodass die vCenter Orchestrator-Arbeitsabläufe verfügbar sind.

### Verfahren

- 1 Melden Sie sich als Administrator bei vCloud Automation Center an.
- 2 Wählen Sie **Advanced Services (Erweiterte Dienste) > Service Blueprints (Dienst-Blueprints)** aus.
- 3 Klicken Sie auf das Symbol **Add Blueprint (+)** (Blueprint hinzufügen).
- 4 Wählen Sie in der Arbeitsablaufbibliothek von vCenter Orchestrator einen Arbeitsablauf aus dem Ordner **Bibliothek > Horizon > Arbeitsabläufe > vCAC61** aus.



- 5 Klicken Sie auf **Weiter** und geben Sie den Namen und die Beschreibung des Arbeitsablaufs an, die im Dienstkatalog von vCloud Automation Center angezeigt werden sollen.
- 6 Klicken Sie auf **Weiter** und bearbeiten Sie auf der Registerkarte **Blueprint-Formular** das Feld **vCACUser**.
  - a Klicken Sie in das Textfeld **vCACUser** und klicken Sie dann auf das (Stift-)Symbol **Bearbeiten**.
  - b Klicken Sie im Dialogfeld „Formularfeld bearbeiten – vCACUser“ auf die Registerkarte **Einschränkungen**.
  - c Klicken Sie auf die Dropdown-Liste **Wert:** .
  - d Aktivieren Sie die Optionsschaltfläche **Feld** und erweitern Sie das Element **Anforderungsinformationen**.
  - e Erweitern Sie das Element **Angefordert von** und wählen Sie **Prinzipal-ID** aus.
  - f Erweitern Sie die Dropdown-Liste **Sichtbar:** .
  - g Aktivieren Sie die Optionsschaltfläche **Konstant** und wählen Sie **Nein** aus, um diesen Parameter in einer Kataloganforderung auszublenden.
  - h Klicken Sie auf **Senden**.
- 7 Klicken Sie auf der Registerkarte **Bereitgestellte Ressource** auf **Add** (Hinzufügen).

Der Blueprint wird auf der Seite „Service Blueprints“ (Dienst-Blueprints) mit dem Status „Draft“ (Entwurf) hinzugefügt.
- 8 Um den Blueprint zu veröffentlichen, wählen Sie in der Liste **Actions** (Aktionen) für den Blueprint die Option **Publish** (Veröffentlichen) aus.

Das Element wird jetzt auf der Registerkarte **Administrator (Administrator) > Catalog Management (Katalogverwaltung) > Catalog Items (Katalogelemente)** angezeigt.

#### Nächste Schritte

Konfigurieren Sie das Katalogelement für diesen Dienst.

## vCAC61-Self-Service-Arbeitsabläufe für die Verwendung bestimmter Pools konfigurieren

Sie können einen Arbeitsablauf ausführen, der die Pools einschränkt, die über die Self-Service-Arbeitsabläufe von vCloud Automation Center verfügbar sind.

Dieses Verfahren gilt nur für Self-Service-Arbeitsabläufe. Informationen zu den anderen Arbeitsabläufen im Ordner vCAC61 finden Sie unter [vCAC61-Arbeitsabläufe mit einem vCAC-Benutzer verknüpfen](#).

Arbeitsabläufe, die in vCloud Automation Center verfügbar gemacht werden, können mit dem Formular-Editor von vCloud Automation Center angepasst werden. Sie können Felder ausblenden oder neu anordnen und kosmetische Änderungen vornehmen, um die Formulare an den Dienstkatalog des Unternehmens anzupassen. Fügen Sie den Blueprint für den jeweiligen Arbeitsablauf hinzu und bearbeiten Sie ihn nach Bedarf. Sie können jedes Arbeitsablauffeld in ein Textfeld umwandeln oder vorgegebene Anzeigewerte hinzufügen, sodass die Benutzer aus einer Dropdown-Liste auswählen können.

### Voraussetzungen

- Stellen Sie sicher, dass Sie über Administratoranmeldeinformationen für den Orchestrator-Server verfügen. Das Konto muss Mitglied der Gruppe „vCenter Orchestrator Admin“ sind, die für die Authentifizierung über vCenter Single Sign-On konfiguriert ist.
- Stellen Sie sicher, dass eine Verbindung mit dem View Pod hergestellt wurde, indem Sie den Arbeitsablauf „Add View Pod in Configuration“ (View Pod in Konfiguration einschließen) ausführen. Siehe [Konfigurieren der Verbindung mit einem View Pod](#).
- Stellen Sie sicher, dass vCloud Automation Center für die Kommunikation mit dem vCenter Orchestrator-Server konfiguriert wurde, sodass die vCenter Orchestrator-Arbeitsabläufe verfügbar sind.

### Verfahren

- 1 Melden Sie sich als Administrator beim Orchestrator-Client an.
- 2 Klicken Sie im Orchestrator-Client auf die Ansicht **Arbeitsabläufe**.
- 3 Wählen Sie in der hierarchischen Liste der Arbeitsabläufe **Bibliothek > Horizon > -Konfiguration > Self-Service-Pool-Konfiguration** aus und navigieren Sie zum Arbeitsablauf **Self-Service-Pool-Konfiguration verwalten**.
- 4 Klicken Sie mit der rechten Maustaste auf den Arbeitsablauf **Self-Service-Pool-Konfiguration verwalten** und wählen Sie **Arbeitsablauf starten** aus.
- 5 Wählen Sie den Pod in der Liste aus und klicken Sie auf die entsprechende Optionsschaltfläche, um festzulegen, ob alle Pools einbezogen werden.
- 6 Wenn Sie nicht alle Pools verfügbar machen möchten, legen Sie fest, welche Pools einbezogen werden sollen:
  - a Klicken Sie auf die Felder, um bestimmte Pool-IDs auszuwählen.
  - b Wählen Sie in der angezeigten Liste der Pools einen Pool aus, der ausgeschlossen werden soll, und klicken Sie über der Liste auf die Schaltfläche mit dem roten X.  
  
Wiederholen Sie diesen Schritt, bis alle Pools entfernt sind, die nicht verfügbar sein sollen. Falls Sie ein Element versehentlich aus der Liste entfernt haben, können Sie den Pool über das Dropdown-Feld **Neuer Wert** wieder in die Liste einfügen.
  - c Ändern Sie mithilfe der Pfeilschaltflächen die Reihenfolge, in der die Pools angezeigt werden.
  - d Klicken Sie auf **Übernehmen**.

7 Klicken Sie auf **Senden**, um den Arbeitsablauf auszuführen.

Die angegebenen Desktop- und Anwendungspools sind in den Self-Service-Arbeitsabläufen im Ordner vCAC61 verfügbar.

## Ausgabeparameter für vCAC61-Arbeitsabläufe konfigurieren

Für Arbeitsabläufe, die Ausgabeparameter zurückgeben, können Sie die Ausgabeparameter zum Dienst-Blueprint hinzufügen.

Arbeitsabläufe, die in vCloud Automation Center verfügbar gemacht werden, können mit dem Formular-Editor von vCloud Automation Center angepasst werden. Sie können Felder ausblenden oder neu anordnen und kosmetische Änderungen vornehmen, um die Formulare an den Dienstkatalog des Unternehmens anzupassen. Fügen Sie den Blueprint für den jeweiligen Arbeitsablauf hinzu und bearbeiten Sie ihn nach Bedarf. Sie können jedes Arbeitsablauffeld in ein Textfeld umwandeln oder vorgegebene Anzeigewerte hinzufügen, sodass die Benutzer aus einer Dropdown-Liste auswählen können.

### Voraussetzungen

- Stellen Sie sicher, dass Sie über Administratoranmeldeinformationen für den Orchestrator-Server verfügen. Das Konto muss Mitglied der Gruppe „vCenter Orchestrator Admin“ sind, die für die Authentifizierung über vCenter Single Sign-On konfiguriert ist.
- Stellen Sie sicher, dass eine Verbindung mit dem View Pod hergestellt wurde, indem Sie den Arbeitsablauf „Add View Pod in Configuration“ (View Pod in Konfiguration einschließen) ausführen. Siehe [Konfigurieren der Verbindung mit einem View Pod](#).
- Stellen Sie sicher, dass vCloud Automation Center für die Kommunikation mit dem vCenter Orchestrator-Server konfiguriert wurde, sodass die vCenter Orchestrator-Arbeitsabläufe verfügbar sind.

### Verfahren

- 1 Melden Sie sich als Administrator bei vCloud Automation Center an.
- 2 Wählen Sie **Advanced Services (Erweiterte Dienste) > Service Blueprints (Dienst-Blueprints)** aus.
- 3 Klicken Sie auf das Symbol **Add Blueprint (+)** (Blueprint hinzufügen).
- 4 Wählen Sie in der Arbeitsablaufbibliothek von vCenter Orchestrator einen Arbeitsablauf aus dem Ordner **Bibliothek > Horizon > Arbeitsabläufe > vCAC61** aus.
- 5 Klicken Sie auf **Weiter** und geben Sie den Namen und die Beschreibung des Arbeitsablaufs an, die im Dienstkatalog von vCloud Automation Center angezeigt werden sollen.
- 6 Klicken Sie auf **Weiter** und klicken Sie auf der Registerkarte **Blueprint-Formular** auf das Plussymbol (+).

- 7 Geben Sie im Dialogfeld „Neues Formular“ dem Formular den Titel **Anforderungsdetails** und wählen Sie in der Liste **BildschirmtypGesendete Anforderungsdetails** aus und klicken Sie auf **Senden**.

In der Liste „Felder“ auf der linken Seite des Formulars können Sie nach unten zu einem neuen Abschnitt namens **Ausgaben** blättern.

- 8 Klicken Sie in der Liste „Felder“ unter **Ausgaben** auf ein Element und ziehen Sie es auf die Formularseite.

Wenn Sie z. B. ein Blueprint-Formular über einen Desktopzuordnungsarbeitsablauf erstellen, können Sie das Element **htmlAccessUrl** in der Liste „Felder“ unter **Ausgaben** auswählen und das Element **htmlAccessUrl** auf die Formularseite ziehen.

- 9 Klicken Sie auf **Weiter** und klicken Sie auf der Registerkarte **Bereitgestellte Ressource** auf **Hinzufügen**.

Der Blueprint wird auf der Seite „Service Blueprints“ (Dienst-Blueprints) mit dem Status „Draft“ (Entwurf) hinzugefügt.

- 10 Um den Blueprint zu veröffentlichen, wählen Sie in der Liste **Actions** (Aktionen) für den Blueprint die Option **Publish** (Veröffentlichen) aus.

Das Element wird jetzt auf der Registerkarte **Administrator (Administrator) > Catalog Management (Katalogverwaltung) > Catalog Items (Katalogelemente)** angezeigt.

#### Nächste Schritte

Konfigurieren Sie das Katalogelement für diesen Dienst. Wenn ein Benutzer eine Anforderung mithilfe dieses Katalogelements sendet, können Sie auf der Registerkarte **Anforderungen** die Details einer der Anforderungen für dieses Element anzeigen und auf der Registerkarte **Schritt** werden die Ausgabeparameter aufgelistet.

## Konfigurieren des Katalogelements für den Arbeitsablauf

Administratoren können Arbeitsabläufe in vCloud Automation Center so konfigurieren, dass sie im Katalog für delegierte Administratoren und Endbenutzer angezeigt werden.

#### Voraussetzungen

- Stellen Sie sicher, dass Sie über Administratoranmeldeinformationen für den Orchestrator-Server verfügen. Das Konto muss Mitglied der Gruppe „vCenter Orchestrator Admin“ sind, die für die Authentifizierung über vCenter Single Sign-On konfiguriert ist.
- Stellen Sie sicher, dass der Arbeitsablauf als Dienst-Blueprint veröffentlicht wurde. Siehe [Verknüpfen von vCAC60-Arbeitsabläufen mit bestimmten Pods und Pools in vCloud Automation Center](#) oder [vCAC61-Arbeitsabläufe mit einem vCAC-Benutzer verknüpfen](#).

#### Verfahren

- 1 Melden Sie sich als Administrator bei vCloud Automation Center an.
- 2 Wählen Sie **Administration (Verwaltung) > Catalog Management (Katalogverwaltung) > Catalog Items (Katalogelemente)** aus.

- 3 Wählen Sie neben dem Element in der Liste **Actions** (Aktionen) die Option **Configure** (Konfigurieren) aus.
- 4 Wählen Sie auf der Registerkarte **Katalogelement konfigurieren** in der Liste **Dienst** den Dienst für den delegierten Administrator oder für den Endbenutzer aus und klicken Sie auf **Aktualisieren**.

Der Arbeitsablauf kann jetzt vom delegierten Administrator bzw. vom Endbenutzer ausgeführt werden. Wenn sich der delegierte Administrator oder der Endbenutzer bei vCloud Automation Center anmeldet und die Registerkarte **Catalog** (Katalog) auswählt, wird der Dienst bzw. der Arbeitsablauf aufgeführt. Der Benutzer klickt auf die Schaltfläche **Request** (Anforderung), füllt das angezeigte Formular aus und klickt auf **Senden**, um den Arbeitsablauf auszuführen.

Benutzer können den Status einer Anforderung auf der Registerkarte **Request** (Anforderung) überprüfen.

Der primäre Administrator kann den Status überprüfen, indem er sich bei Orchestrator anmeldet, neben dem Arbeitsablauf auf die Erweiterungsschaltfläche klickt und anschließend die gewünschte Ausführung des Arbeitsablaufs auswählt.

# Mit nicht verwalteten Maschinen arbeiten

# 5

Für manuelle nicht verwaltete Pools in View kann die View-Verbindungsserver-Instanz keine Informationen von einer vCenter Server-Instanz erhalten. Die nicht verwalteten Maschinen müssen daher mit der View-Verbindungsserver-Instanz registriert werden, bevor sie zu einem Desktop-Pool hinzugefügt werden können.

Der Beitrag [Voraussetzungen für das Hinzufügen von nicht verwalteten Maschinen zu Pools](#) gilt für sämtliche Typen nicht verwalteter Maschinen. Die anderen Beiträge in diesem Kapitel gelten nur für physische Maschinen, die Sie zu einem View-Desktop-Pool hinzufügen.

---

**Hinweis** Der Arbeitsablauf „Nicht verwaltete Maschinen zu einem Pool hinzufügen“ ist mit dem Horizon vCenter Orchestrator-Plug-In 1.1 verfügbar.

---

Dieses Kapitel enthält die folgenden Themen:

- [Voraussetzungen für das Hinzufügen von nicht verwalteten Maschinen zu Pools](#)
- [Hinzufügen physischer Maschinen und nicht durch vSphere bereitgestellter virtueller Maschinen zu Pools](#)

## Voraussetzungen für das Hinzufügen von nicht verwalteten Maschinen zu Pools

Prüfen Sie anhand dieser Checkliste, ob Sie alle Aufgaben ausgeführt haben, die für den Arbeitsablauf zum Hinzufügen der Maschine zu einem manuellen, nicht verwalteten Pool erforderlich sind.

Es sind verschiedene Arbeitsabläufe verfügbar, mit denen ein delegierter Administrator physische und virtuelle Maschinen zu manuellen Desktop-Pools in View hinzufügen kann. Diese Arbeitsabläufe sind mit dem Horizon vCenter Orchestrator-Plug-In 1.1 verfügbar.

- Verwenden Sie den Arbeitsablauf „Add Unmanaged Machines to Pool“ (Nicht verwaltete Maschinen zu einem Pool hinzufügen) für nicht verwaltete Maschinen, die durch eine vCenter-Instanz verwaltet werden, wenn diese vCenter-Instanz nicht zu View hinzugefügt wurde.
- Verwenden Sie den im Ordner Workflows/Example verfügbaren Arbeitsablauf „Add Physical Machines to Pool“ (Physische Maschinen zu einem Pool hinzufügen), um physische Maschinen und

nicht mit vSphere bereitgestellte virtuelle Maschinen hinzuzufügen, z. B. solche, die Sie mit Citrix XenServer, Microsoft HyperV oder VMware Workstation erstellen. Alternativ können Sie den anderen Arbeitsablauf wie unter [Hinzufügen physischer Maschinen und nicht durch vSphere bereitgestellter virtueller Maschinen zu Pools](#) beschrieben ausführen.

Prüfen Sie vor dem Ausführen eines Arbeitsablaufs zum Hinzufügen nicht verwalteter Maschinen zu einem Pool, ob Sie die folgenden Aufgaben ausgeführt haben:

- Installieren Sie für virtuelle vSphere-Maschinen die aktuellste Version von VMware Tools auf der nicht verwalteten virtuellen Maschine.

Eine schrittweise Anleitung finden Sie in der Hilfe zu VMware vSphere.

- Installieren Sie View Agent 6.0 oder 6.0.1 auf der nicht verwalteten Maschine.

Eine schrittweise Anleitung finden Sie im Abschnitt „Installieren von View Agent auf einer nicht verwalteten Maschine“ in *Einrichten von Desktop- und Anwendungspools für View*.

- Wenn die nicht verwaltete Maschine ein Windows Server 2008 R2-Computer ist, aktivieren Sie die Verwendung des Servers als Remote-Desktop:

- a Melden Sie sich bei View Administrator an.

Die View Administrator-Oberfläche verwendet eine URL im folgenden Format: `https://connection-server/admin`.

- b Wechseln Sie zu **View-Konfiguration > Globale Einstellungen**.

- c Wählen Sie die Registerkarte **Allgemein** aus und klicken Sie auf **Bearbeiten**.

- d Wählen Sie das Kontrollkästchen **Windows Server 2008 R2-Desktops aktivieren** aus und klicken Sie auf **OK**.

- Konfigurieren Sie für virtuelle vSphere-Maschinen die vCenter Server-Instanz mit der Option **Eine einzelne Sitzung gemeinsam verwenden** für die Verwaltung von Benutzeranmeldungen:

- a Melden Sie sich bei der Konfigurationskonsole von vCenter Orchestrator an.

Die Konfigurationskonsole verwendet eine URL im folgenden Format: `https://vco-server:8283`.

- b Wechseln Sie zu **vCenter Server** und klicken Sie für die vCenter Server-Instanz auf **Bearbeiten**.

- c Wählen Sie unter **Specify which strategy will be used for managing the users logins** (Legen Sie fest, mit welcher Strategie Benutzeranmeldungen verwaltet werden) die Option **Share a unique session** (Eine einzelne Sitzung gemeinsam verwenden) aus und klicken Sie auf **Apply changes** (Änderungen übernehmen).

- d Starten Sie den Serverdienst von vCenter Orchestrator neu.

- Fügen Sie Gastanmeldedaten hinzu, indem Sie den Arbeitsablauf „Add Guest Credentials“ (Anmeldedaten des Gasts hinzufügen) des Horizon vCenter Orchestrator-Plug-Ins ausführen.

Dieser Arbeitsablauf befindet sich im Ordner Configuration/Horizon Registration Configuration. Die Anmeldedaten des Gasts müssen eine Anmeldung als Administrator oder Domänenadministrator bei der virtuellen Maschine ermöglichen.

- Führen Sie den Arbeitsablauf „Manage Delegated Administrator Configuration for Registration“ (Konfiguration des delegierten Administrators für die Registrierung verwalten) aus, der sich im Ordner Configuration/Horizon Registration Configuration befindet, damit der delegierte Administrator berechtigt ist, die Gastanmeldedaten zu verwenden, und Zugriff auf die Ordner „datacenter“ und „virtual machine“ erhält.

Für den Arbeitsablauf „Add Unmanaged Machines to Pool“ (Nicht verwaltete Maschinen zu einem Pool hinzufügen) für virtuelle vSphere-Maschinen gelten einige wichtige Einschränkungen. Siehe [Add Unmanaged Machines to Pool \(Nicht verwaltete Maschinen zu einem Pool hinzufügen\)](#).

Für physische Computer und nicht durch vSphere bereitgestellte virtuelle Maschinen sind zusätzliche Konfigurationsschritte erforderlich. Siehe [Konfiguration einer physischen Maschine für einen nicht verwalteten Pool](#) und [Konfiguration von vCenter Orchestrator für die Verwendung der Kerberos-Authentifizierung mit physischen Maschinen](#). Sie können dann den Arbeitsablauf „Add Physical Machines to Pool“ (Physische Maschinen zu einem Pool hinzufügen) ausführen, der sich im Ordner workflows/Example befindet. Sie können aber auch die in [Ausführen von Arbeitsabläufen zum Hinzufügen physischer Maschinen als PowerShell-Hosts](#) vorgestellten Arbeitsabläufe „Register Machines to Pool“ (Maschinen in einem Pool registrieren) und „PowerShell“ ausführen.

## Hinzufügen physischer Maschinen und nicht durch vSphere bereitgestellter virtueller Maschinen zu Pools

Um physische Maschinen und nicht durch vSphere bereitgestellte virtuelle Maschinen, wie die mit Citrix XenServer, Microsoft HyperV oder VMware Workstation erstellten, zu manuellen nicht verwalteten Desktop-Pools hinzuzufügen, sind einige Konfigurationsaufgaben erforderlich.

Wenn Sie die unter [Voraussetzungen für das Hinzufügen von nicht verwalteten Maschinen zu Pools](#) aufgeführten Voraussetzungen erfüllen, müssen Sie folgende Aufgaben ausführen:

- 1 Windows Remote Management aktivieren, Remote-Ausführungsrichtlinien festlegen, Orchestrator-Server als vertrauenswürdigen Host hinzufügen und die Kommunikation mit dem PowerShell-Plug-In aktivieren. Anleitungen finden Sie unter [Konfiguration einer physischen Maschine für einen nicht verwalteten Pool](#).
- 2 Den Orchestrator-Server für die Kerberos-Authentifizierung konfigurieren. Anweisungen finden Sie unter [Konfiguration von vCenter Orchestrator für die Verwendung der Kerberos-Authentifizierung mit physischen Maschinen](#).
- 3 Sie können entweder den Arbeitsablauf „Physische Maschinen zu einem Pool hinzufügen“ ausführen, der sich im Ordner workflows/Example befindet. Oder Sie führen die in [Ausführen von Arbeitsabläufen zum Hinzufügen physischer Maschinen als PowerShell-Hosts](#) vorgestellten Arbeitsabläufe „Maschinen in einem Pool registrieren“ und „PowerShell“ aus.



## Konfiguration einer physischen Maschine für einen nicht verwalteten Pool

Bevor Sie einen physischen Computer zu einem manuellen nicht verwalteten Desktop-Pool hinzufügen, müssen Sie sich beim Computer als Administrator anmelden und einige Konfigurationsaufgaben durchführen.

### Voraussetzungen

- Stellen Sie sicher, dass Sie sich beim Computer mit Administratoranmeldedaten anmelden. Falls der Computer mit einer Domäne verknüpft ist, benötigen Sie Anmeldedaten als Domänenadministrator.
- Machen Sie sich mit dem Verfahren für die Konfiguration von WinRM für die Verwendung von HTTP vertraut. Sehen Sie hierzu in der Dokumentation der vCenter Plug-Ins [Configure WinRM to Use HTTP](#) (WinRM für die Verwendung von HTTP konfigurieren).

### Verfahren

- 1 Melden Sie sich als Administrator an und legen Sie fest, dass der Windows Remote Management-Dienst automatisch gestartet wird:
  - a Wechseln Sie zu den Diensten.  
Wechseln Sie beispielsweise auf einem Windows 7-Computer zu **Start > Verwaltung > Dienste**.
  - b Klicken Sie mit der rechten Maustaste auf den Dienst **Windows Remote Management (WS-Management)** und wählen Sie **Eigenschaften** aus.
  - c Wählen Sie für den Starttyp **Automatisch** aus, klicken Sie auf **Start** und nach dem Start des Dienstes auf **OK**.
- 2 Starten Sie die PowerShell als Administrator und konfigurieren Sie die Remote-Ausführungsrichtlinien mit den folgenden Befehlen:
  - a Prüfen Sie mit dem folgenden Befehl, ob für die Richtlinie RemoteSigned festgelegt ist.

```
Get-ExecutionPolicy
```

- b Wenn für die Richtlinie Eingeschränkt festgelegt ist, verwenden Sie folgenden Befehl:

```
Set-ExecutionPolicy RemoteSigned
```

Wählen Sie „Y“, wenn Sie dazu aufgefordert werden.

- c Aktivieren Sie mit dem folgenden Befehl die Remote-Ausführung für WinRM

```
Enable-PSRemoting
```

Wählen Sie „Y“, wenn Sie dazu aufgefordert werden.

- d Fügen Sie mit einem Befehl vCenter Orchestrator-Hosts als vertrauenswürdige Server hinzu.

Option	Befehl
Alle Maschinen als vertrauenswürdige Hosts hinzufügen	Set-Item wsman:\localhost\client\trustedhosts * oder set-item wsman:\localhost\Client\TrustedHosts -value *
Alle Domänenmaschinen als vertrauenswürdige Hosts hinzufügen	set-item wsman:\localhost\Client\TrustedHosts *.domain.com
Eine einzelne Maschine hinzufügen (benutzen Sie den FQDN der Maschine)	set-item wsman:\localhost\Client\TrustedHosts -value hostname.domain.com
Eine einzelne Maschine über die IP-Adresse hinzufügen	set-item wsman:\localhost\Client\TrustedHosts -value xxx.xxx.xxx.xxx

Wählen Sie „Y“, wenn Sie dazu aufgefordert werden.

**Hinweis** Mit dem folgenden Befehl können Sie eine Liste der vertrauenswürdigen Hosts anzeigen:

```
Get-item wsman:\localhost\Client\TrustedHosts
```

- e Starten Sie den WinRM-Dienst mit dem folgenden Befehl neu:

```
Restart-Service WinRM
```

- 3 Testen Sie auf einer anderen Windows-Maschine die Verbindung zu der Maschine, die Sie gerade konfiguriert haben, indem Sie den folgenden Befehl ausführen:

```
Test-WSMan IP-oder-DNS-der-Maschine
```

Beispiel: Test-WSMan 12.34.56.78

Die Ausgabe sieht etwa wie folgt aus:

```
wsmid      : http://schemas.dmtf.org/wbem/wsman/identity/1/wsmanidentity.xsd
ProtocolVersion : http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
ProductVendor  : Microsoft Corporation
ProductVersion : OS: 0.0.0 SP: 0.0 Stack: 2.0
```

Wenn Sie folgenden Befehl verwenden, listet die Ausgabe den Inhalt von Laufwerk C auf:

```
Invoke-Command -ComputerName IP-or-DNS-of-machine -ScriptBlock { Get-ChildItem C:\ }
-credential domain\administrator
```

- 4 Öffnen Sie eine Eingabeaufforderung und konfigurieren Sie den physischen Computer (WinRM-Host) für die Kommunikation mit dem PowerShell-Plug-In über das HTTP-Protokoll.

Falls Sie PowerShell 2.0 benutzen, müssen Sie die Befehle wie folgt in einfachen Anführungszeichen eingeben:

```
winrm set winrm/config/service/auth '@{Basic="true"}'
winrm set winrm/config/service '@{AllowUnencrypted="true"}'

winrm set winrm/config/client/auth '@{Basic="true"}'
winrm set winrm/config/client '@{AllowUnencrypted="true"}'
```

Wenn es sich bei der WinRM-Hostmaschine um eine externe Domäne handelt, müssen Sie außerdem den folgenden Befehl ausführen, um die vertrauenswürdigen Hosts festzulegen:

```
winrm set winrm/config/client @{TrustedHosts="host1, host2, host3"}
```

Mit dem folgenden Befehl können Sie die Einstellungen nach Abschluss der Änderungen überprüfen:

```
winrm get winrm/config
```

- 5 Aktivieren und testen Sie die Kerberos-Authentifizierung für Maschinen, die einer Domäne angehören:
  - a Öffnen Sie eine Eingabeaufforderung und aktivieren Sie mit dem folgenden Befehl die Kerberos-Authentifizierung:

```
winrm set winrm/config/service/auth '@{Kerberos="true"}'
winrm set winrm/config/service '@{AllowUnencrypted="true"}'

winrm set winrm/config/client/auth '@{Kerberos="true"}'
winrm set winrm/config/client '@{AllowUnencrypted="true"}'
```

- b Testen Sie die Kerberos-Authentifizierung mit folgendem Befehl:

```
winrm id -r:machine.domain.com -auth:Kerberos -u:administrator@domain.com -p:'password'
```

- 6 Installieren Sie View Agent auf dem physischen Computer.

### Nächste Schritte

Konfigurieren Sie die Authentifizierung auf dem vCenter Orchestrator-Server. Siehe [Konfiguration von vCenter Orchestrator für die Verwendung der Kerberos-Authentifizierung mit physischen Maschinen](#).

## Konfiguration von vCenter Orchestrator für die Verwendung der Kerberos-Authentifizierung mit physischen Maschinen

Sie müssen eine Konfigurationsdatei auf Ihrem vCenter Orchestrator-Server bearbeiten, um den Domännennamen und Domänencontrollernamen anzugeben.

## Voraussetzungen

Sie benötigen das Stammkennwort, wenn Sie die virtuelle vCenter Orchestrator-Appliance verwenden, oder die Administratoranmeldedaten, falls vCenter Orchestrator auf einem Windows-Server installiert ist.

## Verfahren

- 1 Melden Sie sich als Root an (oder als Administrator, falls Sie einen Windows-Server haben).
- 2 Suchen Sie nach der Datei `krb5.conf` und benennen Sie diese in `krb5.conf.back` um.

Auf einer virtuellen Appliance befindet sich diese Datei, sofern vorhanden, im Ordner `etc/krb5.conf`.

- 3 Erstellen Sie eine Datei mit dem Namen `krb5.conf` im entsprechenden Verzeichnis.

Servertyp	Beschreibung
Virtuelle Appliance	<code>/usr/java/jre-vmware/lib/security/</code>
Windows-Server	<code>C:\Programme\Gemeinsame Dateien\VMware\VMware vCenter Server - Java Components\lib\security\</code>

- 4 Öffnen Sie die Datei `krb5.conf` in einem Texteditor und fügen Sie die folgenden Zeilen mit den entsprechenden Werten hinzu:

```
[libdefaults]
    default_realm = YOURDOMAIN.COM
    udp_preference_limit = 1
[realms]
    YOURDOMAIN.COM = {
        kdc = yourDC.yourdomain.com
        default_domain = yourdomain.com
    }
[domain_realms]
    . yourdomain.com= YOURDOMAIN.COM
    yourdomain.com= YOURDOMAIN.COM
```

- 5 Wenn Sie eine virtuelle Appliance verwenden, ändern Sie mit dem folgenden Befehl die Dateiberechtigungen, damit sie gelesen werden kann:

```
chmod 644 /usr/java/jre-vmware/lib/security/krb5.conf
```

- 6 Prüfen Sie, ob die Namen des PowerShell-Hosts (das ist die physische Maschine, die registriert werden muss) und des Domänencontroller-Hosts durch den vCenter Orchestrator-Server aufgelöst werden können.

Das DNS von vCenter Orchestrator muss mit dem DNS des Domänencontrollers übereinstimmen. Sie können aber auch die Maschinennamen oder IP-Adressen der physischen Maschinen und des Domänencontrollers auf dem vCenter Orchestrator-Server zur Datei `hosts` hinzufügen.

Auf einer virtuellen Appliance finden Sie diese Datei unter `/etc/hosts`.

- 7 Starten Sie den Serverdienst von vCenter Orchestrator neu.

## Nächste Schritte

Fügen Sie physische Maschinen als PowerShell-Hosts hinzu. Siehe [Ausführen von Arbeitsabläufen zum Hinzufügen physischer Maschinen als PowerShell-Hosts](#).

---

**Hinweis** Alternativ zum PowerShell-Arbeitsablauf können Sie auch den Arbeitsablauf „Physische Maschinen zu einem Pool hinzufügen“ verwenden, der sich im Ordner Workflows/Example befindet. Dieser Arbeitsablauf kombiniert die in [Ausführen von Arbeitsabläufen zum Hinzufügen physischer Maschinen als PowerShell-Hosts](#) vorgestellten Aktionen des Arbeitsablaufs „Maschinen in einem Pool registrieren“ und des PowerShell-Arbeitsablaufs. Bevor Sie den Arbeitsablauf „Physische Maschinen zu einem Pool hinzufügen“ starten, müssen Sie die in [Konfiguration einer physischen Maschine für einen nicht verwalteten Pool](#) und [Voraussetzungen für das Hinzufügen von nicht verwalteten Maschinen zu Pools](#) beschriebenen Aufgaben ausführen.

---

## Ausführen von Arbeitsabläufen zum Hinzufügen physischer Maschinen als PowerShell-Hosts

Sie müssen einige Arbeitsabläufe des PowerShell-Plug-Ins ausführen, um das Hinzufügen physischer Maschinen und nicht über vSphere bereitgestellter virtueller Maschinen mit dem Horizon vCenter Orchestrator-Plug-In zu Desktop-Pools abzuschließen.

---

**Hinweis** Alternativ zu den hier aufgeführten PowerShell-Arbeitsabläufen und dem Arbeitsablauf „Maschinen in einem Pool registrieren“ können Sie den Arbeitsablauf „Physische Maschinen zu einem Pool hinzufügen“ ausführen, der sich im Ordner Workflows/Example befindet.

---

### Voraussetzungen

- Prüfen Sie, ob Sie das vCenter Orchestrator-Plug-In für Microsoft Windows PowerShell besitzen, das die für diesen Vorgang erforderlichen Arbeitsabläufe enthält.
- Stellen Sie sicher, dass Sie über Administratoranmeldeinformationen für den Orchestrator-Server verfügen. Das Konto muss Mitglied der Gruppe „vCenter Orchestrator Admin“ sind, die für die Authentifizierung über vCenter Single Sign-On konfiguriert ist.
- Führen Sie den Arbeitsablauf „Maschinen in einem Pool registrieren“ aus, um die DNS-Namen aller Maschinen in View in manuellen nicht verwalteten Desktop-Pools zu registrieren. Der Arbeitsablauf „Maschinen in einem Pool registrieren“ gibt ein Token (eines für jeden registrierten DNS) zurück, das in die Windows-Registrierung der Maschinen übertragen wird, sobald der in diesem Verfahren beschriebene PowerShell-Befehl ausgeführt wird.

### Verfahren

- 1 Melden Sie sich als Administrator beim Orchestrator-Client an.
- 2 Klicken Sie im Orchestrator-Client auf die Ansicht **Arbeitsabläufe**.
- 3 Wählen Sie in der hierarchischen Liste der Arbeitsabläufe **Bibliothek > PowerShell > - Konfiguration** aus und navigieren Sie zum Arbeitsablauf **PowerShell-Host hinzufügen**.

- 4 Klicken Sie mit der rechten Maustaste auf den Arbeitsablauf **PowerShell-Host hinzufügen** und wählen Sie **Arbeitsablauf starten** aus.
- 5 Geben Sie den Hostnamen und den vollqualifizierten Domännennamen der physischen Maschine ein und klicken Sie auf **Weiter**.

Falls die Maschine keiner Domäne angehört, können Sie die IP-Adresse verwenden. Wenn Sie keine Portnummer angeben, wird der Standardport verwendet.

- 6 Füllen Sie das angezeigte Formular aus und klicken Sie auf **Weiter**.

Option	Aktion
Remote-Hosttyp der PowerShell	Wählen Sie in der Dropdown-Liste <b>WinRM</b> aus.
Transportprotokoll	Wählen Sie in der Dropdown-Liste <b>HTTP</b> aus.
Authentifizierung	Wenn die Maschine der Domäne angehört, wählen Sie in der Dropdown-Liste <b>Kerberos</b> aus. Wenn die Maschine der Domäne nicht angehört, wählen Sie <b>Standard</b> aus.

- 7 Füllen Sie das angezeigte Formular aus.

Option	Aktion
Sitzungsmodus	Wählen Sie in der Dropdown-Liste <b>Gemeinsame Sitzung</b> aus.
Benutzername	Wenn die Maschine einer Domäne angehört, verwenden Sie das Format <b>administrator@domain.com</b> . Verwenden Sie den Benutzernamen des lokalen Administratorkontos, sofern die Maschine keiner Domäne angehört.

- 8 Klicken Sie auf **Senden**, um den Arbeitsablauf auszuführen.
- 9 Klicken Sie nach Abschluss des Arbeitsablaufs mit der rechten Maustaste auf den Arbeitsablauf **PowerShell-Skript starten**, der sich im Ordner PowerShell befindet, und wählen Sie **Arbeitsablauf starten** aus.
- 10 Wählen Sie den eben hinzugefügten Host aus und klicken Sie auf **Weiter**.
- 11 Geben Sie im Textbereich **Skript** den folgenden Befehl ein:

```
New-ItemProperty -Path "hklm:\SOFTWARE\VMware, Inc.\VMware VDM\Agent\Identity" -Name Bootstrap -
PropertyType String -Value "TokenReturnedByWorkflow" -Force
```

Verwenden Sie für *VomArbeitsablaufZurückgegebenesToken* das Token, das vom zuvor für die Registrierung der DNS-Namen ausgeführten Arbeitsablauf „Maschinen in einem Pool registrieren“ zurückgegeben wurde.

- 12 Klicken Sie auf **Senden**, um den Arbeitsablauf auszuführen.

Das View Agent-Token auf der Maschine wird nun mit der View-Verbindungsserver-Instanz gekoppelt.