Table of Contents

Hands-on Lab im Überblick – HOL-1810-01-SDC – Grundlagen der Virtualisierung

Was bedeutet Virtualisierung?

In dieser Lektion erhalten Sie eine Einführung, falls Sie noch nicht mit Virtualisierung vertraut sind.

Falls Sie mit Virtualisierung vertraut sind oder dieses Hand-on Lab bereits zuvor in Anspruch genommen haben, können Sie zum Abschnitt Anleitung für das Hands-on Lab springen.

Virtualisierung:

Die heutige x86-Computer-Hardware wurde zur Ausführung eines einzigen Betriebssystems und einer einzigen Anwendung konzipiert. Damit sind die meisten Maschinen bei Weitem nicht ausgelastet. Virtualisierung bietet Ihnen die Möglichkeit, mehrere virtuelle Maschinen auf einem physischen Computer auszuführen, wobei jede virtuelle Maschine die Ressourcen dieses Computers in mehreren Umgebungen nutzen kann. Verschiedene virtuelle Maschinen können unterschiedliche Betriebssysteme und mehrere Anwendungen auf ein und demselben physischen Computer ausführen.

Definition von „Virtualisierung“

Virtualisierung platziert einen zusätzlichen Software-Layer – einen Hypervisor – auf dem physischen Server. Der Hypervisor ermöglicht die Installation mehrerer Betriebssysteme und Anwendungen auf einem einzigen Server.

Trennung

Durch Isolierung des Betriebssystems von der Hardware entsteht eine virtualisierungsbasierte x86-Plattform. Die hypervisorbasierten Virtualisierungsprodukte und -lösungen von VMware stellen die grundlegende Technologie für x86-Virtualisierung bereit.

Partitionierung

In dieser Abbildung sehen Sie, wie sich die Auslastung durch Partitionierung verbessern lässt.

Isolation

Sie können eine VM isolieren, um Bugs und Fehler zu suchen und zu beheben, ohne dabei andere VMs und Betriebssysteme zu beeinträchtigen. Nach der Fehlerbehebung kann innerhalb weniger Minuten eine vollständige VM-Wiederherstellung durchgeführt werden.

Kapselung

Kapselung erleichtert das Management, da VMs als Dateien behandelt werden. So können sie kopiert, verschoben und wiederhergestellt werden.

Hardwareunabhängigkeit

VMs sind nicht von der physischen Hardware oder einem Anbieter abhängig. Dadurch wird Ihre IT flexibler und skalierbarer.

Vorteile

Virtualisierung ermöglicht das Konsolidieren von Servern und eine sichere Trennung von Anwendungen. Dadurch wird Hochverfügbarkeit und Skalierbarkeit kritischer Anwendungen erreicht.

Vereinfachte Recovery

Virtualisierung erfordert weder eine Konfiguration der Hardware, eine Neuinstallation und Konfiguration des Betriebssystems noch Backup-Agents. Die Recovery einer ganzen VM erfolgt einfach durch Wiederherstellung.

Senkung der Storage-Kosten

Eine Technologie namens Thin Provisioning hilft Ihnen bei der Optimierung des Speicherplatzes und der Storage-Kosten. Mit dieser Technologie erhalten VMs genau dann Storage, wenn sie diesen benötigen.

Kostenvermeidung

Anleitung für das Hands-on Lab

In diesem einführenden Hands-on Lab werden die grundlegenden Funktionen von vSphere und vCenter erläutert. Es stellt einen ausgezeichneten Einstieg in die Grundlagen der Virtualisierung dar.

In diesem Hands-on Lab werden Schritt für Schritt die grundlegenden Funktionen vSphere und vCenter, einschließlich Storage und Netzwerk, erläutert. Es ist in drei Module aufgeteilt. Die Module können in beliebiger Reihenfolge absolviert werden.

- Modul 1 – Einführung in das Management mit vCenter Server (60 Minuten)
- Modul 2 – Einführung in vSphere-Netzwerke und -Sicherheit (60 Minuten)
- Modul 3 – Einführung in vSphere-Storage (60 Minuten)

Jedes Modul dauert etwa 60 bis 90 Minuten, je nach Erfahrung allerdings auch kürzer oder länger.

Außerdem sind Videos in diesen Modulen enthalten. Wenn Sie die Videos ansehen, wird das Tragen von Kopfhörern empfohlen. Der Zeitpunkt jedes Videos ist im Titel vermerkt. In einigen Fällen werden Videos für Aufgaben verwendet, die wir nicht in der Hands-on Lab-Umgebung zeigen können, während andere Videos zusätzliche Informationen enthalten. In einigen dieser Videos ist möglicherweise eine ältere Edition von vSphere zu sehen. Die einzelnen Schritte und Konzepte bleiben jedoch im Grunde unverändert.

Hands-on Lab-Dozenten: Doug Baer, Bill Call, Dave Rollins

Eine Kopie dieser Anleitung kann im PDF-Format heruntergeladen werden:

http://docs.hol.vmware.com/HOL-2017/hol-1810-01-sdc_pdf_en.pdf

oder im HTML-Format angesehen werden:

http://docs.hol.vmware.com/HOL-2017/hol-1810-01-sdc_html_en/

Dieses Hands-on Lab wurde unter Umständen lokalisiert. Informationen, ob dieses Hands-on Lab in Ihrer Sprache lokalisiert wurde und wie Sie Ihre Spracheinstellungen entsprechend ändern, erhalten Sie in dieser PDF-Datei:

http://docs.hol.vmware.com/announcements/nee-localization.pdf

Position der Hauptkonsole

1. Der ROT umrahmte Bereich ist die Hauptkonsole. Das Hands-on Lab-Handbuch befindet sich in der Registerkarte rechts neben der Hauptkonsole.
2. In bestimmten Hands-on Labs gibt es möglicherweise zusätzliche Konsolen auf eigenen Registerkarten oben links. Falls Sie eine andere Konsole öffnen müssen, erhalten Sie entsprechende Anweisungen.
3. Für die Bearbeitung des Hands-on Lab haben Sie 90 Minuten Zeit. Das Hands-on Lab kann nicht gespeichert werden. Sie müssen die Aufgaben während dieser einen Hands-on Lab-Sitzung erledigen. Sie können allerdings die Zeit verlängern, indem Sie auf die Schaltfläche **EXTEND** klicken. Wenn Sie sich auf einem VMware-Event befinden, können Sie Ihre Zeit für das Hands-on Lab zweimal um bis zu 30 Minuten verlängern. Jeder Klick verlängert das Hands-on Lab um 15 Minuten. Außerhalb von VMware-Events können Sie Ihre Zeit für das Hands-on Lab um bis zu 9 Stunden und 30 Minuten verlängern. Jeder Klick verlängert das Hands-on Lab um eine Stunde.

Alternativen zur Tastatureingabe

Im Verlauf des Moduls geben Sie Text in die Hauptkonsole ein. Als Alternative zur direkten Eingabe gibt es zwei hilfreiche Methoden, die die Eingabe komplexer Daten erleichtern.

Inhalte aus dem Hands-on Lab-Handbuch anklicken und in das aktive Konsolenfenster ziehen

Sie können Text und Befehle in der Befehlszeile (CLI) anklicken und direkt aus dem Hands-on Lab-Handbuch in das aktive Fenster der Hauptkonsole ziehen.

Zugriff auf die internationale Online-Tastatur

Darüber hinaus können Sie die internationale Online-Tastatur in der Hauptkonsole verwenden.

1. Klicken Sie auf das Tastatursymbol in der Windows-Schnellstartleiste.

Einmal in das aktive Konsolenfenster klicken

In diesem Beispiel verwenden Sie die Online-Tastatur, um das in E-Mail-Adressen verwendete „@“-Symbol einzugeben. Auf US-Tastaturen wird das @-Symbol über die Umschalttaste 2 eingegeben.

1. Klicken Sie einmal in das aktive Konsolenfenster.
2. Klicken Sie auf die **Umschalttaste**.

Auf die @-Taste klicken

1. Klicken Sie auf die „@“-**Taste**.

Wie Sie sehen, wurde ein @-Symbol in das aktive Konsolenfenster eingegeben.

Blicken Sie auf den unteren rechten Teil des Bildschirms

Überprüfen Sie, ob das Hands-on Lab alle Startroutinen abgeschlossen hat und gestartet werden kann. Falls etwas anderes als „Ready“ angezeigt wird, warten Sie einige Minuten. Falls der Status Ihres Hands-on Lab nach fünf Minuten nicht auf „Ready“ gewechselt hat, bitten Sie um Hilfe.

Aktivierungsaufforderung oder Wasserzeichen

Wenn Sie Ihr Hands-on Lab erstmals starten, sehen Sie möglicherweise ein Wasserzeichen auf dem Desktop, das angibt, dass Windows nicht aktiviert wurde.

Ein großer Vorteil von Virtualisierung ist, dass virtuelle Maschinen verschoben und auf jeder Plattform ausgeführt werden können. Die Hands-on Labs machen sich diesen Vorteil zunutze. So können wir die Hands-on Labs von mehreren Rechenzentren aus ausführen. Allerdings können sich die Prozessoren dieser Rechenzentren unterscheiden. Dies veranlasst Microsoft zu einer Aktivierungsprüfung über das Internet.

Wir können Ihnen versichern, dass VMware und die Hands-on Labs den Lizenzierungsanforderungen von Microsoft entsprechen. Bei dem Hands-on Lab, das Sie nutzen, handelt es sich um einen gekapselten Pod, der nicht vollen Zugriff auf das Internet hat. Dies ist jedoch für die Windows-Aktivierungsprüfung erforderlich. Ohne vollen Zugriff auf das Internet schlägt dieser automatisierte Prozess fehl und es wird ein Wasserzeichen angezeigt.

Hierbei handelt es sich um ein kosmetisches Problem, das Ihr Hands-on Lab nicht beeinträchtigt.

Modul 1 – Einführung in das Management mit vCenter Server (60 Minuten)

Was ist vSphere?

VMware vSphere ist die weltweit führende Virtualisierungsplattform. Während Virtualisierung und die vSphere-Plattform gewachsen sind, standen Unternehmen vor immer neuen Herausforderungen. Mit vSphere können virtuelle Maschinen (VMs) zwar schnell bereitgestellt werden. Jedoch wurden Management, Kapazitätsplanung und Lebenszyklusmanagement dieser VMs immer schwieriger. VMware vSphere with Operations Management (vSOM) ist eine neue Lösung, mit der Anwender betriebliche Einblicke in eine vSphere-Infrastruktur gewinnen und gleichzeitig die Kapazität optimieren können. Selbst wenn vSphere-Umgebungen wachsen, müssen Anwender in der Lage sein, diese proaktiv zu verwalten. Hierzu werden Informationen hinsichtlich Überwachung, Performance und Kapazität auf einen Blick benötigt. Eine solch detaillierte Analyse hilft Anwendern, die Virtualisierungsplattform optimal zu nutzen, indem sie ungenutzte Kapazität zurückgewinnen, virtuelle Maschinen richtig dimensionieren, die Auslastung optimieren und so außerdem zur Verbesserung der Konsolidierungsraten beitragen. Diese neue VMware-Lösung vereint vSphere und vRealize Operations Standard.

Video: Einführung in VMware vSphere with Operations Management (5:48)

In diesem Video erfahren Sie, wie Sie vSphere with Operations Management für das Management einer effizienteren Umgebung mit höherer Verfügbarkeit nutzen können.

Installation und Konfiguration von ESXi

Aufgrund der Umgebung, in der Hands-on Labs ausgeführt werden, und der damit verbundenen hohen E/A-Last, kann keine Software installiert werden. Die weiterführenden Schritte entnehmen Sie deshalb bitte den nachfolgenden Videos.

Video: Installation und Konfiguration von vSphere (4:36)

Im folgenden Video wird der Installations- und Konfigurationsprozess von vSphere erläutert.

Video: Übersicht über das DCUI (4:58)

In diesem Video wird das Direct Console User Interface (DCUI) erläutert.

vCenter 6 – Übersicht

vCenter Server vereinheitlicht Ressourcen von einzelnen Hosts, sodass diese Ressourcen von virtuellen Maschinen im gesamten Rechenzentrum gemeinsam genutzt werden können. Dies wird durch das Verwalten der Zuweisung virtueller Maschinen zu den Hosts sowie der Zuweisung von Ressourcen zu den virtuellen Maschinen in einem bestimmten Host erreicht. Dem liegen wiederum vom Systemadministrator festgelegte Richtlinien zugrunde.

vSphere 6 – Komponenten

Die oben stehende Abbildung zeigt, wie sich vCenter in den vSphere-Stack einfügt. Mit der Installation von vCenter erhalten Sie einen zentralen Managementpunkt. vCenter Server ermöglicht die Nutzung von erweiterten vSphere-Funktionen wie vSphere Distributed Resource Scheduler (DRS), vSphere High Availability (HA), vSphere vMotion und vSphere Storage vMotion.

Bei der anderen Komponente handelt es sich um vSphere Web Client. vSphere Web Client ist die Oberfläche für vCenter Server- und Multi-Host-Umgebungen. Die Komponente bietet darüber hinaus Konsolenzugriff auf virtuelle Maschinen. Mit vSphere Web Client können alle administrativen Aufgaben in einer in den Browser integrierten Oberfläche durchgeführt werden.

vCenter 6 – Komponenten

Seit vSphere 5.1 gibt es zwei Bereitstellungsmethoden für vCenter. Die erste Methode ist eine Windows-Installation. Mit der Windows-Methode können Sie vCenter Single Sign-On, Inventory Service und vCenter Server auf derselben Hostmaschine (wie bei vCenter Simple Install) oder auf unterschiedlichen virtuellen Maschinen installieren.

Die andere Methode ist eine virtuelle Appliance. Bei der vCenter Server Appliance (vCSA) handelt es sich um eine einzige vorkonfigurierte Linux-basierte virtuelle Maschine, die für vCenter Server und zugehörige Services optimiert wurde.

Platform Services Controller (PSC)

Platform Services Controller (PSC) enthält gemeinsame Services, die in der ganzen Suite verwendet werden. Dazu zählen Single Sign-On (SSO), Lizenzierung und VMware Certificate Authority (VMCA). Auf den folgenden Seiten erhalten Sie weitere Informationen zu SSO und VMCA.

PSC ist die erste Komponente, die installiert oder für die ein Upgrade durchgeführt wird. Beim Upgrade wird eine SSO-Instanz zu einem PSC. Es gibt zwei Bereitstellungsmodelle: eingebettet und zentralisiert.

- Eingebettet bedeutet, dass PSC und vCenter Server auf einer gemeinsamen virtuellen Maschine installiert werden. – Eingebettet wird für Standorte mit einer einzigen SSO-Lösung wie einem einzigen vCenter empfohlen.
- Zentralisiert bedeutet, dass PSC und vCenter Server auf unterschiedlichen virtuellen Maschinen installiert werden. – Zentralisiert wird für Standorte mit mindestens zwei SSO-Lösungen wie mehreren vCenter Servers, vRealize Automation usw. empfohlen. Bei der Bereitstellung in einem zentralisierten Modell wird empfohlen, den PSC hochverfügbar zu machen, damit kein Single Point of Failure entsteht. Neben der Nutzung von vSphere HA kann ein Lastausgleich vor zwei oder mehreren PSCs platziert werden, um eine hochverfügbare PSC-Architektur zu schaffen.

PSC und vCenter Servers können beliebig miteinander kombiniert werden. Dies bedeutet, dass Appliance-PSCs zusammen mit Windows-PSCs sowie Windows- und appliancebasierten vCenter Servers bereitgestellt werden können. Bei jeder Kombination wird die integrierte Replikation des PSC verwendet.

Anwendungsbeispiel:

- Der PSC entfernt Services aus vCenter und zentralisiert diese über die vCloud Suite hinweg.
- Dadurch steht Kunden eine zentrale Stelle für die Verwaltung aller vSphere-Rollen und -Berechtigungen samt Lizenzierungen zur Verfügung.
- Durch Reduzierung der Komplexität einer vCenter Server-Installation kann vSphere 6 schneller installiert oder ein Upgrade dafür durchgeführt werden.
- Es gibt lediglich zwei Installationsoptionen:
    - Bei einem eingebetteten PSC werden alle Komponenten auf einer einzigen virtuellen Maschine installiert.
    - Bei einem zentralisierten PSC müssen PSC und vCenter Server getrennt installiert werden.

- Unabhängig vom Installationsmodell werden alle vCenter Server-Services auf dem vCenter Server installiert, wodurch die Komplexität der Planung und Installation von vCenter Server reduziert wird.

vCenter Single Sign-On

Mit vSphere 5.1 wurde vCenter Single Sign-On (SSO) als Teil der vCenter Server-Managementinfrastruktur eingeführt. Diese Änderung beeinflusst die Installation, das Upgrade und den Betrieb von vCenter Server. Die Authentifizierung durch vCenter Single Sign-On macht die Cloud-Infrastrukturplattform von VMware sicherer, da die vSphere-Softwarekomponenten über einen sicheren Tokenaustauschmechanismus miteinander kommunizieren können und die einzelnen Komponenten nicht mehr jeden Anwender separat über einen Verzeichnisdienst wie Active Directory authentifizieren müssen.

vCenter Single Sign-On – Übliche Bereitstellung

Seit Version 5.1 enthält vSphere einen vCenter Single Sign-On-Service als Teil der vCenter Server-Managementinfrastruktur.

Die Authentifizierung mit vCenter Single Sign-On macht vSphere sicherer, da die vSphere-Softwarekomponenten über einen sicheren Tokenaustauschmechanismus miteinander kommunizieren und sich alle anderen Anwender auch mit vCenter Single Sign-On authentifizieren.

vCenter Single Sign-On ist seit vSphere 6.0 entweder als eingebettete Bereitstellung oder als Teil des Platform Services Controller enthalten. Der Platform Services Controller enthält alle Services, die für die Kommunikation zwischen vSphere-Komponenten benötigt werden, einschließlich vCenter Single Sign-On, VMware Certificate Authority, VMware Lookup Service und Lizenzierungsservice. In der oberen Abbildung befindet sich SSO beispielsweise innerhalb des Platform Services Controller als Teil dieser Multi-vCenter-Topologie. In dieser Topologie können sowohl Windows als auch vCSA genutzt werden.

vCenter Single Sign-On – Einzelnes vCenter

Bei einer Topologie mit einem einzigen vCenter kann der PSC (mit allen zugehörigen Services) auf einer gemeinsamen Maschine ausgeführt werden. Dies wird auch als eingebettete Bereitstellung bezeichnet. Bei dieser gemeinsamen Maschine kann es sich um einen physischen Windows-Server, eine Windows-VM oder die vCSA handeln.

Während vCenter Server, wie oben dargestellt, eine Datenbank erfordert, ist dies für SSO nicht erforderlich.

Weitere Informationen zu Single Sign-On

Im zweiten Modul dieses Hands-on Lab, „Einführung in vSphere-Netzwerke und -Sicherheit“, wird SSO genauer beschrieben.

Weitere Informationen zu den Anforderungen und Überlegungen einer SSO-Architektur in vCenter 6 finden Sie außerdem im vCenter 6-Bereitstellungsleitfaden:

http://www.vmware.com/files/pdf/techpaper/vmware-vcenter-server6-deployment-guide.pdf

Verwenden von vSphere Web Client

In diesem Hands-on Lab werden vSphere 6 Web Client und dessen Funktionen vorgestellt.

vSphere Web Client ist die primäre Methode zur Systemadministration und Anwenderinteraktion mit der von VMware vSphere® erstellten virtuellen Rechenzentrumsumgebung. vSphere verwaltet eine Reihe von Objekten, aus denen das virtuelle Rechenzentrum besteht, wie Hosts, Cluster, virtuelle Maschinen, Datenspeicher und Netzwerkressourcen.

vSphere Web Client ist eine webbrowserbasierte Anwendung für das Management, die Überwachung und die Administration der Objekte, aus denen das virtualisierte Rechenzentrum besteht. Mit vSphere Web Client kann die vSphere-Umgebung auf folgende Weise überwacht und geändert werden:

■ Anzeige von Informationen zu Systemzustand, Status und Performance von vSphere-Objekten

■ Erteilen von Management- und Administrationsbefehlen an vSphere-Objekte

■ Erstellung, Konfiguration, Provisioning oder Löschen von vSphere-Objekten

Sie können vSphere auf unterschiedliche Weisen erweitern, um eine passende Lösung für Ihre spezielle IT-Infrastruktur zu schaffen. Sie können vSphere Web Client um zusätzliche GUI-Funktionen erweitern, um diese neuen Funktionen für das Management und die Überwachung Ihrer speziellen vSphere-Umgebung zu unterstützen.

Hauptbereiche des Webclient

vSphere Web Client besteht aus sechs Hauptbereichen, die auch als Fenster bezeichnet werden.

1. Der Navigationsbaum oder Navigator
2. Der Hauptbereich für Inhalte
3. Die Suchleiste
4. Die Liste „Work in Progress“
5. Die Liste „Alarms“
6. und die Liste „Recent Tasks“

Das Layout dieser Fenster kann angepasst werden. Klicken Sie auf das Stecknadelsymbol in den Fenstern „Navigator“, „Recent Tasks“, „Work in Progress“ oder „Alarms“, um diese zu minimieren. So entsteht mehr Platz für den Hauptbereich, wenn Sie mit einem kleinen Monitor oder geringer Auflösung arbeiten. Außerdem können Sie die Positionen dieser Fenster ändern, indem Sie die Titelleiste des Fensters an den Bildschirmrand ziehen.

Hinweis: Da dieses Hands-on Lab auf eine geringe Bildschirmauflösung beschränkt ist, sind alle Fenster standardmäßig minimiert, um den Platz auf dem Bildschirm bestmöglich zu nutzen. Sie können jederzeit die gewünschten oder alle Fenster öffnen. Indem Sie auf die Stecknadel klicken, bleibt das jeweilige Fenster geöffnet.

Übersicht über die Hauptbereiche der Weboberfläche

Starten Sie den Chrome-Webbrowser. Dieser öffnet die Seite „Site A Web Client“.

1. Klicken Sie auf das Kontrollkästchen **Use Windows session authentication**.
2. Klicken Sie auf **Login**.

vCenter-Bestandsliste

Sie gelangen automatisch zu einer Ansicht, in der die mit vCenter verbundenen Hosts und Cluster angezeigt werden. Durch Auswählen von „Global Inventory Lists“ erhalten Sie eine Gesamtübersicht.

1. Klicken Sie entweder in der linken Baumstruktur oder im rechten Fenster auf **Global Inventory Lists**. Mit einem Klick auf „Global Inventory Lists“ gelangen Sie zur Bestandsliste, in der Sie alle mit vCenter Server-Systemen verbundenen Objekte wie Rechenzentren, Hosts, Cluster, Netzwerke, Storage und virtuelle Maschinen finden.

Untergeordnete Objekte, Rechenzentren und Hosts

1. Klicken Sie auf das Bestandselement **Virtual Machines**. Wenn Sie dieses Bestandselement auswählen, wird eine Liste mit den in dieser Umgebung befindlichen VMs angezeigt.

Virtuelle Maschinen: Zusammenfassung

1. Klicken Sie auf die virtuelle Maschine **w12-core**.
2. Klicken Sie bei dieser virtuellen Maschine auf die Registerkarte **Summary**. Auf dieser Seite werden alle Details der virtuellen Maschine angezeigt. Außerdem gibt es den Link „Edit Settings“, mit dem Sie die Einstellungen der virtuellen Maschine ändern können.

Bearbeiten der Einstellungen einer virtuellen Maschine

1. Klicken auf den Pfeil neben **VM Hardware**, um dieses Fenster einzublenden und die Hardware-Einstellungen der VM anzuzeigen.
2. Klicken Sie auf **Edit Settings**, um einen zweiten Netzwerkadapter zur virtuellen Maschine hinzuzufügen.

Hinzufügen eines zweiten Netzwerkadapters

Hinzufügen eines zusätzlichen Netzwerkadapters.

1. Klicken Sie auf die Dropdown-Liste für **New Device**.
2. Wählen Sie das Gerät **Network** aus.
3. Klicken Sie auf die Schaltfläche „Add“, um die neue Netzwerkkarte zur virtuellen Maschine hinzuzufügen.

Konfigurieren der zweiten Netzwerkkarte

1. Klicken Sie auf den Pfeil neben „New Network Card“, um die Einstellungen einzublenden. Beachten Sie, dass die MAC-Adresse zu diesem Zeitpunkt leer ist. Eine neue MAC-Adresse wird generiert, sobald diese NIC hinzugefügt wird oder Sie eine eigene MAC-Adresse (gemäß einiger Regeln) angeben können.
2. Klicken Sie auf **OK**, um das Gerät zur VM hinzuzufügen. Wenn Sie **OK** auswählen, wird eine neue Aufgabe erstellt.

Liste „Recent Tasks“

Nach dem Hinzufügen der zweiten NIC zur VM wird eine Aufgabe in der Liste „Recent Tasks“ angezeigt.

1. Falls das Fenster „Recent Tasks“ noch minimiert ist, klicken Sie auf die Schaltfläche „Recent Tasks“.
2. Optional können Sie auf das Stecknadelsymbol rechts im Fenster „Recent Tasks“ klicken, um das Fenster „Recent Tasks“ in der Oberfläche anzupinnen.

Liste „Recent Tasks“

Überprüfen Sie die Liste „Recent Tasks“. Sobald die Aufgabe abgeschlossen wurde, sollte ein zweiter Netzwerkadapter im Abschnitt „VM Hardware“ angezeigt werden. Beachten Sie, dass die Netzwerke nicht verbunden sind, da die VM ausgeschaltet ist.

Sie können das Fenster „Recent Tasks“ wahlweise ausblenden, indem Sie auf die Schaltfläche „Recent Tasks“ klicken, oder dauerhaft anpinnen, indem Sie auf die Stecknadel klicken.

Anzeigen des Fensters „Work In Progress“

Für einige der nächsten Übungen kann es hilfreich sein, das Fenster „Work In Progress“ einzublenden.

1. Klicken Sie auf die Schaltfläche **Work In Progress**.
2. Klicken Sie auf die **Stecknadel**, um das Fenster anzupinnen.

Erstellen einer virtuellen Maschine

Das Erstellen einer neuen VM ist in mehreren Bereichen der Oberfläche möglich. In diesem Beispiel wird die oberste Hierarchieebene verwendet: vCenter Server.

1. Bewegen Sie den Mauszeiger auf das Menü **Home** (die Schaltfläche muss nicht angeklickt werden).
2. Wählen Sie **VMs and Templates** aus.

Erstellen einer virtuellen Maschine

1. Erweitern Sie die Baumstruktur „vcsa-01a.corp.local“, um das Objekt **DataCenter Site A** anzuzeigen.
2. Klicken Sie auf **DataCenter Site A**.

Starten des Assistenten zum Erstellen neuer virtueller Maschinen

1. Falls Sie sich noch nicht in dieser Ansicht befinden, klicken Sie auf die Registerkarte **Getting Started**, um die Liste „Basic Tasks“ anzuzeigen. Diese enthält Aufgaben, die gestartet werden können.
2. Klicken Sie auf **Create a new virtual machine**, um den Assistenten zum Erstellen neuer virtueller Maschinen zu starten. Dieser Assistent erstellt eine neue virtuelle Maschine und platziert diese in der vSphere-Bestandsliste.

Assistent zum Erstellen virtueller Maschinen

1. Klicken Sie auf **Next**, da der Punkt **Create a New Virtual Machine** bereits hervorgehoben ist.

Benennen der virtuellen Maschine

1. Geben Sie **web-serv01** als Namen der neuen virtuellen Maschine ein.
2. Klicken Sie auf **Next**.

Platzierung der virtuellen Maschine

Erweitern Sie **Datacenter Site A**, um **Cluster Site A** anzuzeigen.

Da Distributed Resource Scheduler (DRS) aktiviert ist, müssen Sie lediglich einen Cluster auswählen. DRS legt selbst fest, welcher Host für die VM verwendet wird.

1. Klicken Sie auf **Cluster Site A**.
2. Klicken Sie auf **Next**.

Pausieren des Assistenten

Sie kennen das: Sie befinden sich gerade mitten in einer Aufgabe, nur um dann von einer anderen Anfrage unterbrochen zu werden. In vSphere Web Client ist das kein Problem. Sie können den Assistenten einfach „pausieren“, sich der anderen Aufgabe widmen und dann dort weitermachen, wo Sie aufgehört haben. Sie erhalten zum Beispiel einen Anruf von einem Anwender mit der Bitte, seine VM umgehend zu starten. Also pausieren Sie den Assistenten, um die VM des Anwenders zu starten.

1. Speichern Sie den Fortschritt des Assistenten, indem Sie auf **>>** in der oberen rechten Ecke des Webclient klicken. Hiermit wird der Zustand des Assistenten im Fenster „Work In Progress“ gespeichert und der Assistent wird geschlossen. Jetzt können Sie sich der dringenderen Aufgabe widmen und die VM des Anwenders starten.

Das Fenster „Work In Progress“

1. Zeigen Sie das Fenster „Work In Progress“ an, um zu überprüfen, ob Ihre Arbeit gespeichert wurde.
2. Nachdem Sie überprüft haben, ob Ihre Arbeit gespeichert wurde, klicken Sie auf die Stecknadel im Fenster „Work In Progress“, um dieses zu minimieren und mehr Platz auf Ihrem Bildschirm zu schaffen.

Starten von w12-core

1. Klicken Sie auf **Hosts and Clusters**.
2. Erweitern Sie „vcsa-01a.corp.local“, „Datacenter Site A“ und „Cluster Site A“, um die VM „w12-core“ anzuzeigen.
3. Klicken Sie mit der rechten Maustaste auf **w12-core**. Dies öffnet das Untermenü „Actions“.
4. Erweitern Sie das Menü, indem Sie den Mauszeiger auf **Power** bewegen.
5. Klicken Sie auf den Menüeintrag **Power On** .

Fortsetzen des Assistenten zum Erstellen neuer virtueller Maschinen

1. Klicken Sie auf die Schaltfläche **Work In Progress**, um das Fenster „Work In Progress“ anzuzeigen.

Fortsetzen des Assistenten zum Erstellen neuer virtueller Maschinen

1. Klicken Sie auf **New Virtual Machine**, um den Assistenten zum Zeitpunkt des Verlassens aufzurufen.

Auswählen des Datastore

1. Stellen Sie sicher, dass der Datastore **ds-site-a-nfs01** ausgewählt ist.
2. Klicken Sie auf **Next**.

Kompatibilität

1. Klicken Sie auf **Next**, um die Standardeinstellung **ESXi 6.5 and later** zu akzeptieren.

Gastbetriebssystem

In diesem Schritt wird das zu installierende Betriebssystem festgelegt. Nach Auswahl des Betriebssystems wird die unterstützte virtuelle Hardware und empfohlene Konfiguration zur Erstellung der virtuellen Maschine verwendet. Denken Sie daran, dass hierdurch keine virtuelle Maschine erstellt wird, auf der das gewünschte Betriebssystem installiert ist, sondern eine virtuelle Maschine, die für das von Ihnen ausgewählte Betriebssystem optimiert ist.

1. Wählen Sie **Linux** im Dropdown-Menü unter **Guest OS Family** aus.
2. Wählen Sie **VMware Photon OS (64-bit)** unter **Guest OS Version** aus.
3. Klicken Sie auf **Next**, um fortzufahren.

Ändern der Größe der virtuellen Festplatte

1. Ändern Sie den Arbeitsspeicher von 2048 in **1024**. Dies ist eine Test-VM. Deshalb benötigt sie lediglich 1 GB Arbeitsspeicher und 40 MB Festplattenspeicher.
2. Ändern Sie die Festplattengröße von GB in **MB**.
3. Ändern Sie die Festplattengröße von 16.384 in **40** MB.
4. Ändern Sie das Netzwerk in **VM Network (vds-site-a)**.
5. Wählen Sie **Next** aus.

Abschließen des Vorgangs

Überprüfen Sie Ihre Einstellungen und klicken Sie auf **Finish**, um diese neue virtuelle Maschine zu erstellen.

Neu erstellte virtuelle Maschine

Herzlichen Glückwunsch, Sie haben Ihre erste virtuelle Maschine erstellt!

Wie bereist erwähnt, haben Sie gerade die virtuelle Maschine erstellt. Jetzt müssen Sie noch das ISO-Image eines Betriebssystems mounten und das Betriebssystem auf der virtuellen Maschine installieren. Aufgrund der Performance-Probleme, die beim Installieren eines Betriebssystems in der Hands-on Lab-Infrastruktur entstehen würden, können wir die tatsächliche Installation nicht zeigen. Im weiteren Verlauf dieses Kurses erfahren Sie, wie Sie ein ISO-Image an eine virtuelle Maschine anbinden, um eine Datei davon zu kopieren. Dies ist vergleichbar mit dem Prozess zum Installieren eines Betriebssystems auf einer virtuellen Maschine.

Einschalten der neuen virtuellen Maschine

1. Klicken Sie mit der rechten Maustaste auf **web-serv01**.
2. Bewegen Sie den Mauszeiger auf den Menüeintrag **Power**.
3. Klicken Sie auf **Power On**.

Zusätzlich zum Rechtsklickmenü gibt es oben im Webclient ein Menü „Actions“, in dem diese Befehle ebenfalls ausgeführt werden können.

Öffnen der VM-Konsole

Klicken Sie nach dem Einschalten der virtuellen Maschine auf das **Konsolenbild**, um das Konsolenfenster der virtuellen Maschine aufzurufen.

Interaktion mit der Konsole

In Chrome sollte eine neue Registerkarte geöffnet werden, auf der die Konsole der virtuellen Maschine angezeigt wird.

Da kein Betriebssystem installiert wurde, wird die virtuelle Maschine versuchen, aus dem Netzwerk zu booten, und schließlich fehlschlagen. Falls ein bootfähiges ISO-Image in die virtuelle Maschine eingebunden wäre, beispielsweise die ISO eines Betriebssystems, würde die virtuelle Maschine von diesem booten und mit dem Installationsprozess beginnen. Die Installation kann dann über diese Konsole gesteuert werden.

Klicken Sie auf das **X**, um die Registerkarte zu schließen und zu vSphere Web Client zurückzukehren.

Einbinden eines ISO-Image in eine virtuelle Maschine

Ein wichtiger Schritt nach der Erstellung einer virtuellen Maschine und der Installation des Betriebssystems ist die Installation von VMware Tools. VMware Tools ist eine Suite von Dienstprogrammen, die die Performance des Betriebssystems der virtuellen Maschine und das Management der virtuellen Maschine verbessern. Üblicherweise werden Sie nach dem Erstellen der virtuellen Maschine informiert, dass VMware Tools nicht installiert ist. Dabei wird ein Link angezeigt, mit dem Sie diese Aktion ausführen

können (siehe Abbildung 1). Klicken Sie jedoch **nicht auf diesen Link**, da kein Betriebssystem installiert ist.

VMware Tools kann auch manuell mithilfe eines ISO-Image installiert werden, das gemeinsam mit vSphere installiert wird. Nachfolgend wird schrittweise erklärt, wie Sie VMware Tools in der virtuellen Maschine mounten und auf den Desktop der virtuellen Maschine kopieren.

Klicken Sie auf **w12-core**.

Bearbeiten der Einstellungen von „w12-core“

Wählen Sie **Edit Settings...** im Menü **Actions** aus.

Datastore ISO File

Wählen Sie **Datastore ISO File** aus dem Dropdown-Menü **CD/DVD drive 1** aus. Hiermit wird ein Dateiexplorer geöffnet, um die Datei auszuwählen.

Erweitern der Verzeichnisse

1. Erweitern Sie die Verzeichnisse unter **vmimges** und klicken Sie anschließend auf **tools-isoimages**.
2. Wählen Sie **windows.iso** im Fenster „Content“ aus.
3. Klicken Sie auf **OK**.

Verbinden des Laufwerks

Als Letztes wird das ISO-Image mit der virtuellen Maschine verknüpft bzw. verbunden.

1. Klicken Sie auf das Kontrollkästchen **Connected** neben **CD/DVD drive 1**.
2. Klicken Sie auf **OK**.

Öffnen einer Konsole zu „w12-core“

Klicken Sie auf das Konsolenbild von „w12-core“, um ein Konsolenfenster zu öffnen und mit der virtuellen Maschine zu interagieren. Daraufhin wird eine neue Registerkarte in Chrome geöffnet.

Öffnen des Windows-Explorer

Klicken Sie in der Taskleiste auf das **Ordnersymbol**, um den Windows-Explorer zu öffnen.

DVD-Laufwerk

1. Scrollen Sie nach unten, bis **DVD Drive (D:)** zu sehen ist. Dies ist das ISO-Image, das vorher in der virtuellen Maschine gemountet wurde. Klicken Sie darauf.

Im rechten Fenster werden die auf dem ISO-Image befindlichen Dateien angezeigt.

Kopieren von setup64.exe

Klicken Sie auf **setup64.exe** und halten Sie dabei die linke Maustaste gedrückt. Ziehen Sie die Datei auf den Desktop, um sie zu kopieren.

Das Kopieren sollte nur wenige Sekunden dauern.

Schließen des Konsolenfensters

Klicken Sie auf das **X**, um das Konsolenfenster zu schließen.

Bearbeiten der Einstellungen von „w12-core“

Sobald Sie das ISO-Image auf der virtuellen Maschine nicht mehr benötigen, müssen Sie es unmounten.

Wählen Sie im Menü **Actions** die Option **Edit Settings...** aus.

Deaktivieren von „Connected“

1. Durch Deaktivieren des Kontrollkästchens **Connected** unmounten Sie das ISO-Image von der virtuellen Maschine.

2. Klicken Sie auf **OK**.

Sie können bei der Installation eines Betriebssystems ebenso verfahren. Mounten Sie das ISO-Image des Betriebssystems auf der virtuellen Maschine (stellen Sie sicher, dass die Option „Connect when powered on“ ausgewählt ist) und schalten Sie die virtuelle Maschine ein. Sie werden feststellen, dass der Installationsprozess wesentlich schneller ist als mit einer echten CD/DVD auf physischer Hardware.

Es handelt sich hierbei nicht immer um die schnellste Möglichkeit, virtuelle Maschinen zu erstellen. In der nächsten Lektion werden andere Möglichkeiten wie Cloning und die Erstellung virtueller Maschinen aus einer Vorlage besprochen.

Klonen von virtuellen Maschinen und Verwenden von Vorlagen

VMware bietet verschiedene Möglichkeiten zum Bereitstellen von vSphere-VMs.

Eine Möglichkeit besteht darin, eine einzige virtuelle Maschine zu erstellen, ein Betriebssystem darauf zu installieren und diese virtuelle Maschine als Basis-Image zu verwenden, aus dem andere virtuelle Maschinen geklont werden. Das Klonen einer virtuelle Maschine kann Zeit sparen, wenn Sie viele ähnliche virtuelle Maschinen bereitstellen. Sie können auf einer einzigen virtuellen Maschine Software erstellen, konfigurieren und installieren. Anschließend können Sie diese mehrfach klonen, anstatt jede virtuelle Maschine einzeln zu erstellen und zu konfigurieren.

Eine weitere Provisioning-Methode ist das Klonen einer virtuellen Maschine als Vorlage. Eine Vorlage ist eine Masterkopie einer virtuellen Maschine, die zur Erstellung und Bereitstellung neuer virtueller Maschinen verwendet werden kann. Die Erstellung einer Vorlage kann hilfreich sein, wenn Sie mehrere virtuelle Maschinen mit denselben Grundeinstellungen bereitstellen müssen, jedes System jedoch individuell anpassen möchten. Ein wesentlicher Vorteil der Verwendung von Vorlagen ist die Zeitersparnis. Falls Sie eine virtuelle Maschine häufig klonen, sollten Sie diese virtuelle Maschine zu einer Vorlage machen und Ihre virtuellen Maschinen aus dieser Vorlage bereitstellen.

In dieser Lektion klonen Sie eine bestehende virtuelle Maschine in eine Vorlage und stellen eine neue virtuelle Maschine aus dieser Vorlage bereit.

Navigieren zum Managementfenster „VMs and Templates“

1. Wählen Sie **VMs and Templates** im Menü „Home“ aus.

Öffnen der Bestandsliste

1. Klicken Sie auf die Pfeile, um die Bestandsliste zu erweitern.

Hier sehen Sie, dass mehrere virtuelle Maschinen in der vSphere-Umgebung vorhanden sind. Im nächsten Schritt wird die virtuelle Maschine „TinyLinux-01“ in eine Vorlage geklont.

Starten des Assistenten zum Klonen einer virtuellen Maschine in eine Vorlage

1. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine **TinyLinux-01**.

2. Wählen Sie **Clone** aus.
3. Wählen Sie **Clone to Template** aus.

Auswählen eines Namens und Ordners

Belassen Sie den Standort für dieses Hands-on Lab auf **Datacenter Site A**.

1. Geben Sie im Assistenten zum Klonen einer virtuellen Maschine in eine Vorlage einen Namen für die Vorlage ein: **TinyLinux Template**.
2. Klicken Sie auf **Next**.

Auswählen einer Computing-Ressource

Wählen Sie eine Computing-Ressource aus:

1. Wählen Sie **Cluster Site A** aus.

2. Klicken Sie auf **Next**.

Auswählen des Storage

Es wird automatisch der Datastore mit dem größten freien Speicherplatz ausgewählt. Wählen Sie in diesem Fall **ds-site-a-nfs01** aus. Klicken Sie auf die Schaltfläche **Next**.

Überprüfen der Einstellungen für die VM-Vorlage

Überprüfen Sie die Einstellungen für die VM-Vorlage und klicken Sie auf die Schaltfläche **Finish**.

Überwachen des Aufgabenfortschritts

1. Klicken Sie auf die Schaltfläche **Recent Tasks**, um den Fortschritt der gerade von Ihnen erstellten Vorlage zu beobachten.
2. Sobald die Aufgabe abgeschlossen wurde, wird das neue Objekt **TinyLinux Template** im Bestandsfenster angezeigt.

Starten des Assistenten zur Bereitstellung aus einer Vorlage

1. Wählen Sie die Vorlage **TinyLinux Template** aus.

2. Wählen Sie die Registerkarte **Getting Started** aus.

3. Klicken Sie unter „Basic Tasks“ im Aktionsfenster auf **Deploy to a new virtual machine**.

Auswählen eines Namens und Ordners

1. Geben Sie **TinyLinux-02** als Namen der neuen virtuellen Maschine ein.

2. Belassen Sie den Standort auf dem Standardwert **Datacenter Site A**.

3. Klicken Sie auf die Schaltfläche **Next**.

Auswählen einer Computing-Ressource

1. Wählen Sie **Cluster Site A** aus.
2. Klicken Sie auf **Next**.

Auswählen des Storage

1. Belassen Sie den Datastore auf dem Standardwert **ds-iscsi01**, der den größten freien Speicherplatz besitzt.
2. Klicken Sie auf **Next**.

Auswählen der Klonoptionen

Lassen Sie die Kontrollkästchen für die Klonoptionen deaktiviert. Um das Modul nicht unnötig in die Länge zu ziehen, ist auf der Vorlage **TinyLinux-01** kein Betriebssystem installiert. Deshalb ist es nicht möglich, den Gast anzupassen.

Als Herausforderung können Sie eine Vorlage der VM „w12-core“ erstellen und dort die Optionen zur Gastanpassung durchgehen. Das Klonen der VM „w12-core“ dauert etwa 20 Minuten. Es kann etwas Zeit gespart werden, wenn Sie die VM in eine Vorlage konvertieren und anschließend eine neue VM aus dieser Vorlage mit Gastanpassung klonen.

1. Klicken Sie auf **Next**.

Abschließen des Vorgangs

Überprüfen Sie die Bereitstellungsoptionen und klicken Sie anschließend auf **Finish**.

Überwachen des Aufgabenfortschritts

1. Sie können auf die Schaltfläche **Recent Tasks** klicken, um zu beobachten, wie die VM aus der Vorlage erstellt wird.
2. Sobald die Aufgabe abgeschlossen wurde, wird die virtuelle Maschine **TinyLinux-02** im Bestandsfenster angezeigt.

Video: Weitere Informationen zu VM-Klonen und -Vorlagen (4:04)

Im folgenden Video erhalten Sie weitere Informationen zu VM-Klonen und -Vorlagen in vSphere:

Verwenden von Tagging und Suche zum schnellen Finden von Objekten

vSphere Web Client bietet einige mächtige Suchoptionen. In dieser Lektion werden die unterschiedlichen Suchoptionen erläutert, um Bestandsobjekte schnell zu finden. Mit einer neuen Funktion von vCenter Inventory Service können Anwender außerdem eigene Tags für Bestandsobjekte aus der Umgebung erstellen, um diese zu kategorisieren. Diese Tags sind durchsuchbare Metadaten, die den Zeitaufwand für die Suche nach Bestandsobjekten verringern. In dieser Lektion wird die Erstellung von Tags und die Nutzung von Tags bei einer Suche erläutert.

Suchoptionen

Es gibt verschiedene Suchoptionen: „New Search“, „Saved Searches“ und „Quick Search“. Als Erstes wird „New Search“ beschrieben.

1. Klicken Sie im Webclient auf das **Haussymbol**, um das Menü „Home“ anzuzeigen.
2. Klicken Sie auf **New Search**.

Suchen nach virtuellen Maschinen

1. Führen Sie eine einfache Suche durch, indem Sie **vm** in das Suchfeld eingeben.
2. Klicken Sie auf **Search**.
3. Die Suchergebnisse werden nach Objekttyp geordnet im Bestandsfenster angezeigt.
4. Von der Suche wurden außerdem nach Objekttyp geordnete Registerkarten erstellt. Sie sollten sich auf der Registerkarte „Virtual Machines“ befinden. Falls dies nicht der Fall ist, klicken Sie auf die Registerkarte „Virtual Machines“.

In der Umgebung vorhandene virtuelle Maschinen

1. Wenn Sie die Registerkarte **Virtual Machines** auswählen, wird eine Liste von in der Umgebung vorhandenen VMs angezeigt.
2. Als Nächstes suchen Sie nach einem bestimmten Tag. Klicken Sie auf den Link **Advanced Search**.

Erweiterte Suche

Mit der erweiterten Suche können Sie nach verwalteten Objekten suchen, die mehrere Kriterien erfüllen.

Beispielsweise können Sie nach virtuellen Maschinen mit einer gemeinsamen Zeichenfolge suchen. Die virtuellen Maschinen befinden sich auf Hosts, deren Namen einer zweiten gesuchten Zeichenfolge entsprechen. Suchen Sie nach virtuellen Maschinen, um den Status von VMware Tools zu prüfen.

1. Ändern Sie das hervorgehobene Feld in **Virtual Machine**.
2. Klicken Sie im Feld für die Eigenschaft auf **VMware Tools Version Status**.
3. Klicken Sie auf das Dropdown-Menü, um das Kriterium **Not installed** auszuwählen.
4. Klicken Sie auf die Schaltfläche **Search**.
5. Die Ergebnisse werden im Ergebnisbildschirm angezeigt.
6. Damit diese Suche erneut verwendet werden kann, müssen Sie diese speichern. Klicken Sie auf **Save...**.

Benennen der Suche

1. Geben Sie als Name der Suche **VMware Tools Not Installed** ein.
2. Klicken Sie auf **OK**.

Anzeigen von gespeicherten Suchen

1. Klicken Sie oben auf das **Haussymbol**.
2. Klicken Sie auf **Saved Searches**.

Speichern von Suchergebnissen

1. Klicken Sie auf die gespeicherte Suche **VMware Tools Not Installed**.
2. Im Ergebnisfenster wird eine Liste von VMs angezeigt, auf denen VMware Tools nicht installiert ist.

Schnellsuche

1. Geben Sie in der oberen rechten Ecke **vm** in das Schnellsuchfeld ein. In einem Pop-up-Fenster werden dem Filter entsprechende Objekte anzeigt.
2. Klicken Sie auf den zweiten Eintrag **VM Network** neben der Überschrift **Distributed Port Group**.

Liste virtueller Maschinen

Wählen Sie die Registerkarte **VMs** aus, um eine erweiterte Liste der virtuellen Maschinen anzuzeigen.

Tags, benutzerdefinierte Bezeichnungen

Mithilfe von Tags fügen Sie Bestandsobjekten Metadaten hinzu. Sie können Informationen zu Ihren Bestandsobjekten in Tags festhalten und diese Tags in Suchen verwenden.

1. Klicken Sie auf das Menü **Home**.
2. Wählen Sie **Tags and Custom Attributes** aus, um Tag-Kategorien und Tags zu erstellen.

Erstellen von Tag-Kategorien

Mithilfe von Kategorien werden Tags gruppiert und es wird festgelegt, wie Tags zu Objekten hinzugefügt werden können.

Jedes Tag darf nur einer Kategorie angehören. Sie müssen mindestens eine Kategorie erstellen, bevor Sie Tags erstellen.

1. Klicken Sie auf **New Category**.

Neue Kategorie

Associable Object Types: Verwenden Sie hier den Standardwert, sodass das neue Tag in dieser Kategorie allen Objekten zugewiesen werden kann. Mit den anderen Optionen können Sie ein bestimmtes Objekt festlegen, wie eine virtuelle Maschine oder Datastores.

1. Geben Sie **web tier** in das Feld „Category Name“ ein.
2. Behalten Sie den Standardwert **One tag per object** bei.
3. Klicken Sie auf **OK**.

Erstellen eines neuen Tags

Klicken Sie auf **New Tag**, um ein neues Tag zu erstellen.

Erstellen von Tags und Kategoriezuweisung

1. Geben Sie **Web Server version 2** ein, um ein neues Tag zu erstellen.
2. Klicken Sie im Dropdown-Menü von „Category“ auf **web tier**.
3. Wählen Sie **OK** aus.

Zum Überprüfen der von Ihnen erstellten Kategorie und Tags wählen Sie die Registerkarte „Items“ aus. In dieser Ansicht können Sie die Kategorien und Tags überprüfen und bearbeiten. Außerdem können in dieser Ansicht neue Kategorien und Tags erstellt werden.

Auflisten erstellter Tags

1. Wenn Sie die Registerkarte **Tags** auswählen, wird eine Liste der erstellten Tags angezeigt. Darüber hinaus gibt es die Registerkarte „Categories“. Auf dieser werden die erstellten Kategorien angezeigt.

Zuweisen von Tags zu einer virtuellen Maschine

1. Klicken Sie auf das Menü **Home**.
2. Klicken Sie auf **VMs and Templates**.

Auswählen einer VM

1. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine **web-serv01**. Möglicherweise müssen Sie den Navigationsbaum links erweitern, um die VMs anzuzeigen.
2. Suchen Sie den Menüeintrag **Tags & Custom Attributes**.
3. Klicken Sie auf **Assign Tag**.

Zuweisen eines Tags

1. Klicken Sie auf das Tag **Web Server Version 2**.
2. Klicken Sie auf **Assign**. Es wird eine Aufgabe erstellt und das Tag zugewiesen.

Suchen mithilfe von Tags

1. Geben Sie im Schnellsuchfeld **we** ein.

2. Wählen Sie das Tag **Web Server Version 2** aus.

Suchergebnisse

1. Klicken Sie auf die Registerkarte **Objects**, um die Liste von Objekten anzuzeigen, denen das Tag **Web Server Version 2** zugewiesen wurde.

Verwenden von Filtern

Eine andere Möglichkeit, Objekte schnell zu finden, ist die neue Filterfunktion in vSphere Web Client.

1. Klicken Sie zunächst auf das Menü **Home**.
2. Klicken Sie auf **Hosts and Clusters**.

Auswählen von „Cluster Site A“

1. Wählen Sie im linken Navigationsfenster **Cluster Site A** aus.
2. Klicken Sie als Nächstes auf die Registerkarte **Hosts**.

Filteroptionen

1. Klicken Sie auf die Schaltfläche **Quick Filter** neben dem Feld **Filter**.

Host-Filteroptionen

Jetzt wird eine Liste von Filteroptionen für vSphere-Hosts angezeigt.

1. Klicken Sie auf das Kontrollkästchen **In Maintenance Mode** unter „Maintenance Mode“.

Hosts im Wartungsmodus

Eine Liste von Hosts im Wartungsmodus wird nun angezeigt. In diesem Fall ist sie leer.

Um einen Filter zu entfernen, deaktivieren Sie einfach das zugehörige Kontrollkästchen. Um alle Filter zu entfernen und von Neuem zu beginnen, klicken Sie auf das Filtersymbol mit dem roten „X“.

1. Klicken Sie auf das Filtersymbol mit dem roten „X“.

Weitere Filter

Sie können durch die anderen Registerkarten („VMs“, „Networks“, „Datastores“ usw.) klicken und weitere Filter anzeigen, die für die einzelnen Objekttypen verfügbar sind. Jeder Filter gilt wiederum für seine eigene Objektklasse.

Falls ein Tag für dieses Objekt erstellt wurde, kann dieses ebenfalls zur Filterung verwendet werden.

Verständnis von vSphere Availability und Distributed Resource Scheduler (DRS)

In dieser Lektion wird beschrieben, wie VMware vSphere Web Client zum Aktivieren und Konfigurieren von vSphere Availability und Dynamic Resource Scheduler (DRS) verwendet wird. HA schützt vor Ausfällen durch Automatisieren der Recovery bei einem Host-Ausfall. DRS gewährleistet die Performance durch den Ausgleich von VM-Workloads über die Hosts eines Clusters.

Was ist vSphere Availability?

vSphere Availability bietet Hochverfügbarkeit für virtuelle Maschinen, indem die virtuellen Maschinen und Hosts, auf denen sie sich befinden, in einem Cluster zusammengefasst werden. Die Hosts des Clusters werden überwacht und bei einem Ausfall werden die virtuellen Maschinen eines ausgefallenen Hosts auf alternativen Hosts neu gestartet.

Bei der Erstellung eines vSphere Availability-Clusters wird ein einzelner Host automatisch als Master-Host ausgewählt. Der Master-Host kommuniziert mit vCenter Server und überwacht den Zustand der geschützten virtuellen Maschinen und Slave-Hosts. Es gibt verschiedene Arten von Host-Ausfällen. Deshalb muss der Master-Host Ausfälle erkennen und entsprechend handeln. Der Master-Host muss zwischen einem ausgefallenen Host, einem netzwerkpartitionierten Host oder einem netzwerkisolierten Host unterscheiden. Der Master-Host nutzt einen Heartbeat für Netzwerk und Datastore, um die Art des Ausfalls zu bestimmen. Beachten Sie außerdem, dass es sich bei vSphere Availability um eine Host-Funktion handelt. Dies bedeutet, dass keine Abhängigkeit von vCenter besteht, um ein Failover von VMs auf andere Hosts des Clusters einzuleiten.

Hauptkomponenten von vSphere Availability

Die Master-Rolle

Die Slave-Rolle

Die Wahl des Masters

Aktivieren und Konfigurieren von vSphere Availability

1. Klicken Sie zunächst auf die Schaltfläche **Home**.

2. Wählen Sie **Hosts and Clusters** aus.

Einstellungen von vSphere Availability

1. Klicken Sie auf **Cluster Site A**.
2. Klicken Sie auf **Actions**, um das Dropdown-Menü aufzurufen.
3. Klicken Sie auf **Settings**.

Cluster-Einstellungen

1. Klicken Sie auf **vSphere Availability** unter **Services**, um die Einstellungen für Hochverfügbarkeit aufzurufen. Möglicherweise müssen Sie zum Anfang der Liste scrollen.
2. Klicken Sie auf **Edit**.

Aktivieren von vSphere HA

1. Aktivieren Sie das Kontrollkästchen **Turn ON vSphere HA**.
2. Klicken Sie auf **Failures and Responses**.

Hinweis: Wenn Sie „Turn on Proactive HA“ aktivieren, werden virtuelle Maschinen proaktiv von Hosts migriert, deren Hardwarezustand sich verschlechtert.

Ausfälle und Reaktionen

1. Wählen Sie **VM and Application Monitoring** in der Dropdown-Liste „VM Monitoring“ aus.
2. Klicken Sie auf **Admission Control**.

Wenn Sie „VM and Application Monitoring“ auswählen, wird eine VM neu gestartet, wenn innerhalb eines bestimmten Zeitraums (standardmäßig 30 Sekunden) kein Heartbeat empfangen wird.

Zugangssteuerung

1. Wählen Sie **Cluster resource percentage** im Dropdown-Menü „Define host failover capacity by“ aus.

Für den Failover wird ein bestimmter Prozentsatz an CPU- und Arbeitsspeicherressourcen reserviert. Im oben genannten Fall jeweils 25%.

2. Klicken Sie auf **Heartbeat Datastores**.

VM-Überwachung und Datastore-Heartbeating

Datastore-Heartbeating ist ein weiterer Schutz-Layer. Mithilfe von Datastore-Heartbeating kann vSphere HA Hosts überwachen, falls eine Partition des Managementnetzwerks auftritt, und weiterhin auf auftretende Ausfälle reagieren.

1. Wählen Sie **Automatically select datastores accessible from the host** aus.
2. Klicken Sie auf **OK**, um vSphere HA zu aktivieren.

Überwachen der Aufgabe

Die Konfiguration von vSphere HA dauert etwa ein bis zwei Minuten. Sie können den Fortschritt im Fenster „Recent Tasks“ beobachten.

Sobald die drei Aufgaben abgeschlossen wurden, können Sie mit dem nächsten Schritt fortfahren.

Prüfen der Aktivierung von HA mithilfe der Registerkarte „Summary“

1. Klicken Sie auf die Registerkarte **Summary**.
2. Lokalisieren und erweitern Sie das Fenster **vSphere Availability** im Datenbereich: Klicken Sie links auf den Namen des Fensters, um es zu erweitern.
3. Falls unter **vSphere Availability** nicht **Protected** angezeigt wird und die Aufgaben erfolgreich abgeschlossen wurden, müssen Sie möglicherweise auf die Aktualisierungsschaltfläche klicken.

Der blaue Balken zeigt die Ressourcenauslastung an, der hellgraue Balken die geschützte Kapazität und der gestrichelte Balken die Reservekapazität.

Aktivieren von Distributed Resource Scheduler (DRS)

1. Klicken Sie auf die Schaltfläche **Configure**, um mit dem Aktivierungsprozess von Distributed Resource Scheduler zu beginnen.
2. Klicken Sie auf **vSphere DRS**.
3. Klicken Sie auf die Schaltfläche **Edit**, um die DRS-Einstellungen zu bearbeiten.

Aktivieren von Distributed Resource Scheduler (DRS)

1. Überprüfen Sie, ob das Kontrollkästchen **Turn ON vSphere DRS** aktiviert ist. – Hinweis: Im Hands-on Lab ist dies bereits geschehen.
2. Klicken Sie auf das Dropdown-Menü und wählen Sie **Fully Automated** aus.
3. Klicken Sie auf **OK**.

Automatisierungsstufen

Im Diagramm ist dargestellt, wie die Platzierung und Migration mittels DRS von der Einstellung „Manual“, „Partially Automated“ oder „Fully Automated“ beeinflusst wird.

Überprüfen der Cluster-Balance mithilfe der Registerkarte „Summary“

1. Klicken Sie auf die Registerkarte **Summary**, um den aktuellen Status des Clusters anzuzeigen.
2. Die Registerkarte „Summary“ von „Cluster Site A“ zeigt die aktuelle Balance des Clusters. Im Abschnitt „DRS“ wird außerdem angezeigt, wie viele Empfehlungen oder Fehler im Cluster aufgetreten sind. (Möglicherweise müssen Sie nach unten scrollen, um das vSphere DRS-Widget anzuzeigen.)

Kontinuierliche Verfügbarkeit durch vSphere 6 Fault Tolerance

vSphere 6 HA bietet einen grundlegenden Schutz für Ihre virtuellen Maschinen, indem die virtuellen Maschinen bei einem Hostausfall neu gestartet werden. vSphere 6 Fault Tolerance bietet einen höheren Grad an Verfügbarkeit, da es Anwendern ermöglicht wird, jede virtuelle Maschine ohne Daten-, Transaktions- oder Verbindungsverlust vor Hostausfällen zu schützen.

Fault Tolerance bietet kontinuierliche Verfügbarkeit, indem sichergestellt wird, dass der Status der primären und sekundären VM identisch ist, wenn die virtuelle Maschine Anweisungen ausführt. Dies erfolgt mithilfe der VMware vLockstep-Technologie auf der ESXi-Hostplattform. vLockstep sorgt dafür, dass die primäre und sekundäre VM identische x86-Anweisungssequenzen ausführen. Die primäre VM erfasst alle Eingaben und Ereignisse (vom Prozessor bis hin zu den virtuellen E/A-Geräten) und wiederholt diese auf der sekundären VM. Die sekundäre VM führt dieselbe Serie von Anweisungen wie die primäre VM aus, während der Workload lediglich von einem einzelnen VM-Image (der primären VM) ausgeführt wird.

Falls der Host, auf dem die primäre VM ausgeführt wird, ausfällt, erfolgt ein sofortiger und transparenter Failover. Der intakte ESXi-Host wird nahtlos zum Host der primären VM, ohne dass dabei Netzwerkverbindungen oder laufende Transaktionen unterbrochen werden. Durch den transparenten Failover gehen keine Daten verloren und alle Netzwerkverbindungen bleiben erhalten. Nach einem transparenten Failover wird eine neue sekundäre VM gestartet, um die Redundanz wiederherzustellen. Der gesamte Prozess verläuft transparent und vollkommen automatisiert – selbst wenn vCenter Server nicht verfügbar ist.

VMware vSphere Fault Tolerance

Vorteile von Fault Tolerance:

- Schutz unternehmenskritischer Hochleistungsanwendungen unabhängig vom Betriebssystem
- Kontinuierliche Verfügbarkeit – ohne Ausfallzeiten, kein Datenverlust aufgrund von Infrastrukturausfällen
- Vollständig automatisierte Reaktion

Anwendungsbereiche

Jeder nicht latenzsensible Workload mit bis zu 4 vCPUs und 64GB Arbeitsspeicher (VOIP und Hochfrequenzhandel wären z.B. keine guten Kandidaten für FT). Hinweis: Seit vSphere 6.0 gibt es die Möglichkeit, VMs mit mehr als 1 vCPU mittels FT zu schützen. In vSphere 5.5 und älteren Versionen konnten nur VMs mit 1 vCPU mit FT geschützt

werden. Mit den Standard und Enterprise Editions von vSphere v6.5 können VMs mit bis zu 2 vCPUs, mit der Enterprise Plus Edition VMs mit bis zu 4 vCPUs geschützt werden.

Durch die Nutzung von FT werden mehr VMs pro Anwendung benötigt. Der Overhead hängt von einer Reihe von Faktoren ab wie der Anwendung, der Anzahl von vCPUs, der Anzahl von FT-geschützten VMs auf einem Host, Hostprozessortyp usw. Weitere Informationen erhalten Sie unter Performance Best Practices for VMware vSphere.

Die neue Version von Fault Tolerance erweitert den Anwendungsbereich von FT auf etwa 90% aller Workloads.

Bei FT wird eine neue Technologie namens Fast Checkpointing eingesetzt. Hierbei handelt es sich im Grunde um eine stark modifizierte Version von xvMotion, die niemals beendet wird und viel mehr Checkpoints pro Sekunde ausführt. Beachten Sie außerdem, dass FT in älteren Versionen als 6.0 Shared Storage erforderte, wobei sich sowohl die primäre als auch die sekundäre Kopie der FT-geschützten VM dieselben VMDK-Dateien teilten. In vSphere 6.0 verwenden die primäre und sekundäre VM jedoch eigene VMDKs, um einen zusätzlichen Schutz der FT-geschützten VM zu erreichen.

Die FT-Protokollierung (Datenverkehr zwischen den Hosts, auf denen die primäre und sekundäre VM ausgeführt werden) ist sehr bandbreitenintensiv. Deshalb wird eine dedizierte 10-Gbit-NIC pro Host empfohlen. Dies ist zwar keine Voraussetzung, wird jedoch ausdrücklich empfohlen, da eine FT-geschützte VM mehr Bandbreite verbraucht. Langsamere NICs auf den ESXi-Hosts beeinträchtigen die Performance auf der sekundären VM.

Video: Schutz virtueller Maschinen mit FT (2:51)

In diesem Video wird gezeigt, wie virtuelle Maschinen mit VMware Fault Tolerance (FT) geschützt werden. Aufgrund von Ressourcenkonflikten innerhalb der Umgebung des Hands-on Lab, kann dies nicht live demonstriert werden.

Überwachung von Ereignissen und Erstellung von Alarmen

vSphere enthält ein vom Anwender konfigurierbares Subsystem für Ereignisse und Alarme. Dieses Subsystem verfolgt Ereignisse in vSphere und speichert diese Daten in Protokolldateien und in der vCenter Server-Datenbank. Mit diesem Subsystem können Sie außerdem festlegen, unter welchen Bedingungen Alarme ausgelöst werden. Bei veränderten Systembedingungen kann sich der Schweregrad eines Alarms von weniger schwerwiegenden auf dringendere Stufen ändern. Bei Bedarf werden zudem automatisierte Aktionen ausgelöst. Diese Funktion ist hilfreich, wenn Sie informiert werden oder sofort eingreifen möchten, sobald bestimmte Ereignisse oder Bedingungen für ein bestimmtes Bestandslistenobjekt oder eine Objektgruppe auftreten.

Ereignisse sind Aufzeichnungen von Anwenderaktivitäten oder Systemaktivitäten, die in Bezug auf Objekte in vCenter Server oder auf einem Host erfolgen. Zu Aktionen, die als Ereignisse aufgezeichnet werden, zählen unter anderem folgende Beispiele:

■ Ablaufen eines Lizenzschlüssels

■ Einschalten einer virtuellen Maschine

■ Anmelden eines Anwenders auf einer virtuellen Maschine

■ Unterbrechen einer Host-Verbindung

Ereignisdaten umfassen Details zum Ereignis, beispielsweise von wem es ausgelöst wurde, wann es aufgetreten ist und um welchen Ereignistyp es sich handelt.

Alarme sind Benachrichtigungen, die als Reaktion auf ein Ereignis, auf Bedingungen oder auf den Status eines Bestandslistenobjekts hin ausgelöst werden. Die Definition eines Alarms besteht aus folgenden Elementen:

■ Name und Beschreibung: bietet eine identifizierende Bezeichnung und Beschreibung

■ Alarmtyp: definiert den Typ eines zu überwachenden Objekts

■ Auslöser: definiert das Ereignis, die Bedingung oder den Status für das Auslösen eines Alarms sowie den Schweregrad der Benachrichtigung

■ Toleranzschwelle (Reporting): bietet zusätzliche Einschränkungen bezüglich der Schwellenwerte von Bedingungs- und Statusauslösern, die überschritten werden müssen, bevor ein Alarm ausgelöst wird

■ Aktionen: definiert Operationen, die als Reaktion auf ausgelöste Alarme durchgeführt werden. VMware bietet vordefinierte Aktionen für bestimmte Typen von Bestandslistenobjekten.

Alarme besitzen folgende Schweregrade:

■ Normal: grün

■ Warnung: gelb

■ Alarm: rot

Alarmdefinitionen sind mit dem in der Bestandsliste ausgewählten Objekt verknüpft. Ein Alarm überwacht den in seiner Definition festgelegten Typ von Bestandsobjekten.

Sie möchten beispielsweise die CPU-Auslastung aller virtuellen Maschinen eines bestimmten Host-Clusters überwachen. Sie können den Cluster im Bestand auswählen und einen Alarm für virtuelle Maschinen hinzufügen. Ist dieser Alarm aktiviert, werden alle auf dem Cluster ausgeführten virtuellen Maschinen überwacht. Der Alarm wird ausgelöst, sobald eine der VMs die im Alarm definierten Kriterien erfüllt. Wenn Sie nur eine bestimmte virtuelle Maschine im Cluster überwachen möchten, wählen Sie diese virtuelle Maschine in der Bestandsliste aus und fügen ihr einen Alarm hinzu. Wenn Sie dieselben Alarme zu einer Gruppe von Objekten hinzufügen möchten, platzieren Sie diese Objekte einfach in einem Ordner und legen Sie den Alarm für den Ordner fest.

In dieser Lektion erfahren Sie, wie Sie einen Alarm erstellen und aufgetretene Ereignisse prüfen.

Video: Konfigurieren von Alarmen und Benachrichtigungen in VMware vSphere (5:20)

In diesem Video wird gezeigt, wie Sie vCenter Server-Alarme und -Warnmeldungen mithilfe von VMware vSphere Web Client konfigurieren und E-Mail-Benachrichtigungen aktivieren.

Prüfen der Standardwarnmeldungen

1. Klicken Sie auf das **Haussymbol**.
2. Klicken Sie auf den Menüeintrag **Events**.

Ereigniskonsole

1. Wählen Sie die Spalte **Type** aus, um nach Schweregrad zu sortieren.
2. Wählen Sie ein Ereignis aus, um die Details des Ereignisses anzuzeigen.

Einrichten von Benachrichtigungen

1. Klicken Sie auf das Menü **Home**.
2. Klicken Sie auf den Menüeintrag **Hosts and Clusters**.

Einrichten von Benachrichtigungen

1. Wählen Sie das vCenter **vcsa-01a.corp.local** aus.
2. Klicken Sie auf die Registerkarte **Monitor**.
3. Klicken Sie auf die Registerkarte **Alarm Definitions**. Es werden die Standard-Alarmdefinitionen angezeigt.
4. Klicken Sie auf einen Alarm. Alarme können auf verschiedenen Ebenen definiert werden. Der hervorgehobene Alarm wurde auf oberster Ebene definiert. Alarme, die auf oberster Ebene definiert werden, werden von den untergeordneten Objekten geerbt.

Definieren eines Alarms

1. Verwenden Sie den Filter, um den Alarm „Host CPU usage“ zu suchen. Geben Sie hierzu **cpu** in das Suchfeld ein und drücken Sie die **Eingabetaste**.
2. Wählen Sie den Alarm **Host CPU usage** aus.
3. Klicken Sie auf die Schaltfläche **Edit**.

Host-CPU-Auslastung – Bearbeiten

1. Klicken Sie auf den Abschnitt **Triggers** des Alarms.
2. Wählen Sie eine Auslastung von **80%** für fünf Minuten aus, um den Alarm auszulösen.
3. Klicken Sie auf **Next**.

Definieren von Aktionen

1. Klicken Sie auf **+**, um eine neue Aktion hinzuzufügen.

2. Scrollen Sie in der Liste und klicken Sie auf **Enter maintenance mode**.
3. Setzen Sie **Alert State Change** auf **Once**.
4. Setzen Sie **Alert State Change** auf **Once**.
5. Klicken Sie auf **Finish**.

Erstellen eines neuen Alarms

Klicken Sie auf das Menü **Actions** und wählen Sie **Alarms > New Alarm Definition** aus.

Definieren eines neuen Alarms

Sie erstellen einen Alarm, der eine VM migriert, falls der Status „CPU Ready“ einen Durchschnittswert von 8000 ms über die Dauer von fünf Minuten überschreitet.

1. Geben Sie **Virtual Machine CPU Ready** ein.
2. Klicken Sie auf **Next**, um den Abschnitt „Triggers“ aufzurufen.

Definieren der CPU-Bereitschaftszeit

1. Klicken Sie auf **+**, um eine neue Auslöseraktion hinzuzufügen.
2. Scrollen Sie in der Liste nach unten und wählen Sie **VM CPU Ready Time** aus. Behalten Sie die Standardbedingungen bei.
3. Klicken Sie auf **Next**.

Definieren der durchzuführenden Aktion

1. Klicken Sie auf **+**, um eine neue Aktion hinzuzufügen.
2. Klicken Sie auf die Aktion **Migrate VM**.
3. Klicken Sie in der Spalte „Configuration“ auf **Resource Pool; Host; Priority**. Sobald Sie darauf klicken, ändert sich das Feld in **Click to Configure.** Klicken Sie auf diesen Link, um die Einstellungen des Ressourcenpools für die VM-Migration zu konfigurieren.

Assistent für Migrationsaktionen

Hier können Sie einen Host auswählen, auf den die virtuelle Maschine migriert werden soll.

1. Wählen Sie **esxi-01a-corp.local** aus.
2. Klicken Sie auf **Resource Pool**.

Ressourcenpool

1. Wählen Sie **Resources** aus.
2. Klicken Sie auf **Finish**.

Bestätigen der Einstellungen

Bestätigen Sie Ihre Einstellungen und klicken Sie auf **Finish**, um den Alarm zu erstellen.

Neuer Alarm erstellt

Der neu erstellte Alarm ist jetzt sichtbar.

Konfiguration von Quoten und Ressourcen

Quoten bestimmen die relative Wichtigkeit einer virtuellen Maschine (oder eines Ressourcenpools). Falls eine virtuelle Maschine über doppelt so viele Quoten einer Ressource wie eine andere virtuelle Maschine verfügt, ist sie berechtigt, doppelt so viele Ressourcen zu verbrauchen, falls sich diese beiden virtuellen Maschinen in einem Ressourcenkonflikt befinden. Diese Lektion beginnt mit einem Video, in dem das Arbeiten mit Quoten und Ressourcen erläutert wird. Im weiteren Verlauf dieses Moduls wird beschrieben, wie Änderungen an den Ressourcen einer VM vorgenommen werden.

Für Quoten werden üblicherweise die Werte „High“, „Normal“ oder „Low“ festgelegt.

Video: Konfiguration von Quoten und Reservierungen (4:00)

In diesem Video wird gezeigt, wie Sie mit VMware vSphere Web Client Quoten, Reservierungen und Limits konfigurieren, um Computing- und Arbeitsspeicherressourcen effektiv unter virtuellen Maschinen zu verteilen.

Quoten, Limits und Reservierungen

Überprüfen der CPU-Einstellungen

1. Klicken Sie auf die virtuelle Maschine **w12-core**.
2. Klicken Sie auf die Registerkarte **Configure**.
3. Klicken Sie auf die Einstellung **VM Hardware**.
4. Erweitern Sie den Abschnitt „CPU“. Die aktuellen Einstellungen für Quoten, Reservierungen und Limits werden angezeigt.
5. Erweitern Sie den Abschnitt „Memory“. In diesem Abschnitt werden die Quoten, Reservierungen und Limits des Arbeitsspeichers angezeigt.
6. Klicken Sie auf die Schaltfläche **Edit**, um die Freigaben der VM zu bearbeiten.

Funktionsweise von Quoten

Im oberen Beispiel sind zwei VMs zu sehen: eine Entwicklungs-VM und eine Produktions-VM. Links im Diagramm können Sie sehen, dass die CPU-Quoten gleich sind. Es soll sichergestellt werden, dass die Produktions-VM den Großteil der CPU-Ressourcen erhält, wenn in der Umgebung ein Konflikt um diese Ressourcen entsteht. Dies erreichen Sie, indem Sie die Quoten der Produktions-VM von 1000 in 2000 ändern. Rechts im Diagramm sind die neuen Einstellungen zu sehen.

Ändern der Ressourcenzuweisung von CPU-Quoten

1. Erweitern Sie den Abschnitt „CPU“ in den Einstellungen.
2. Klicken Sie im Dropdown-Menü von „Shares“ auf **High**, um die Einstellung der CPU-Quoten zu ändern.
3. Klicken Sie auf **OK**.

Überprüfen der Einstellungen

In der Registerkarte „Settings“ werden die neuen Quoteneinstellungen angezeigt.

Einstellungen für Limits und Reservierungen

Limits und Reservierungen werden auf dieselbe Weise festgelegt. Wenn Sie auf „Edit Settings“ einer VM klicken, können Sie dort Limits und Reservierungen festlegen. Limits hindern eine VM daran, mehr Ressourcen als das festgelegte Limit zu nutzen. Reservierungen garantieren eine Mindestmenge an Ressourcen, die der virtuellen Maschine zur Verfügung stehen. Testen Sie verschiedene Einstellungen für Limits und Reservierungen. Beachten Sie, dass die VM möglicherweise nicht startet, wenn Sie mehr Arbeitsspeicher- oder CPU-Ressourcen reservieren, als vorhanden sind.

vSphere-Funktionen für Überwachung und Performance

VMware stellt verschiedene Tools bereit, mit deren Hilfe Sie Ihre virtuelle Umgebung überwachen und die Ursache potenzieller und aktueller Probleme herausfinden können. In dieser Lektion werden die Performance-Diagramme und -Grafiken in vSphere Web Client beschrieben.

Eine ausführlichere Einführung in Überwachung und Performance erhalten sie in den Hands-on Labs für vRealize Operations. vRealize Operations bietet einen dynamischeren, proaktiveren Ansatz hinsichtlich der Überwachung Ihrer virtuellen Infrastruktur.

Auswählen von „esx-01a“

1. Wählen Sie **esx-01a.corp.local** aus.
2. Klicken Sie auf die Registerkarte **Monitor**.
3. Klicken Sie auf die Registerkarte **Performance**.

CPU-Diagramm

Klicken Sie auf eine beliebige Stelle des Diagramms „CPU (%)“, um dieses zu aktivieren.

CPU-Auslastung des Hosts

1. Wählen Sie **Realtime** im Dropdown-Menü „Time Range“ aus.

Hier wird die CPU-Auslastung von esx-01a.corp.local in Echtzeit in Prozent angezeigt. Das Diagramm wird standardmäßig alle 20 Sekunden aktualisiert. Die Menge der angezeigten Daten hängt davon ab, wie lange das Hands-on Lab bereits aktiv ist.

CPU-Auslastung von virtuellen Maschinen

Klicken Sie jetzt auf das Dropdown-Menü **View** und wählen Sie **Virtual Machines** aus.

Aktivieren des Diagramms

Klicken Sie auf eine beliebige Stelle im Diagramm „CPU Usage (Top 10)“, um das Diagramm zu aktivieren.

Kombinierte CPU-Auslastung

In diesem Diagramm wird die CPU-Auslastung jeder virtuellen Maschine in Echtzeit angezeigt. Die einzelnen VMs werden im Diagramm durch verschiedene Farben dargestellt. Unten sehen Sie, welche VM von welcher Farbe dargestellt wird. Kombiniert erhalten Sie einen Überblick über die gesamte CPU-Auslastung des Hosts.

Weitere Diagramme

Es gibt weitere Diagramme, mit denen sich die Auslastung von Arbeitsspeicher, Netzwerk (Mbit/s) und Festplatte (KBit/s) des Hosts und der virtuellen Maschinen anzeigen lässt.

1. Blenden Sie das Fenster „Navigator“ aus, um mehr Platz für die Diagramme zu schaffen.
2. Scrollen Sie nach unten, um die weiteren Diagramme anzuzeigen.

Erweiterte Diagramme

Mit den bereits besprochenen Diagrammen erhalten Sie eine Übersicht über die vier Hauptkomponenten CPU, Arbeitsspeicher, Festplatte und Storage. Mit den erweiterten Diagrammen erhalten Sie detailliertere Informationen über diese Komponenten.

Bevor Sie diese Diagramme betrachten, müssen Sie CPU-Aktivität auf esx-01a.corp.local erzeugen, indem Sie alle VMs auf den Host migrieren und diese neu starten. Damit einige der VMs nicht zurück auf esx-02a.corp.local migriert werden, muss DRS deaktiviert werden.

1. Wählen Sie **Cluster Site A** aus.
2. Klicken Sie auf die Registerkarte **Configure**.
3. Klicken Sie auf die Schaltfläche **Edit**.

Deaktivieren von DRS

Deaktivieren Sie das Kontrollkästchen **Turn on vSphere DRS** und klicken Sie auf **OK**.

esx-02a.corp.local

1. Wählen Sie **esx-02a.corp.local** aus.
2. Klicken Sie auf die Registerkarte **VMs**.

Abhängig davon, welche anderen Module Sie absolviert haben, werden möglicherweise weitere VMs angezeigt.

Migrieren der VMs

Klicken Sie mit der rechten Maustaste auf **w12-core** und wählen Sie **Migrate...** aus.

Falls sich weitere VMs auf esx-02a.corp.local befinden, halten Sie die Strg-Taste gedrückt und klicken Sie jede VM an, um anschließend alle gleichzeitig mit der rechten Maustaste zu migrieren.

Akzeptieren Sie im VM-Migrationsassistenten bei jedem Schritt die Standardauswahl.

Einschalten von „TinyLinux-02“

1. Wählen Sie **TinyLinux-02** aus.
2. Klicken Sie auf das grüne **Einschaltsymbol**.

Auswählen der neu zu startenden VMs

Um Aktivität auf esx-01a.corp.local zu erzeugen, müssen die VMs neu gestartet werden.

1. Wählen Sie **esx-01a.corp.local** aus.
2. Klicken Sie auf die Registerkarte **VMs**.
3. Klicken Sie auf die **erste VM** in der Liste, halten Sie die **Umschalttaste** gedrückt und wählen Sie die **letzte VM** in der Liste aus.
4. Klicken Sie auf die **Neustartschaltfläche**.

Bestätigen des Neustarts

Klicken Sie auf **Yes**, um fortzufahren.

Sie werden merken, dass nur vier der fünf VMs neu gestartet werden. Dies liegt daran, dass auf web-serv01 weder ein Betriebssystem noch VMware Tools installiert ist.

Manuelles Starten der TinyLinux-VMs

Falls **TinyLinux-01** und **TinyLinux-02** nicht neu gestartet und stattdessen ausgeschaltet wurden, wählen Sie beide aus und klicken Sie auf das grüne Einschaltsymbol.

Überwachung der Performance

1. Klicken Sie auf die Registerkarte **Monitor**.
2. Klicken Sie auf die Registerkarte **Advanced**.

Diagrammoptionen

1. Klicken Sie auf den Link **Chart Options**.

Hiermit werden Optionen zum Anpassen des Diagramms angezeigt.

Stapeldiagramm pro VM

Wählen Sie **Stacked Graph per VM** im Dropdown-Menü „Chart Type“ aus.

Auswählen von Objekten

Klicken Sie unter dem Kästchen „Select objects for this chart“ auf die Schaltfläche **All**, um alle VMs und esx-01a.corp.local auszuwählen.

Klicken Sie auf die Schaltfläche **OK**, um das neu angepasste Diagramm anzuzeigen.

CPU-Auslastung in Echtzeit

Hier wird die CPU-Auslastung von jeder virtuellen Maschine und von esx-01a.corp.local angezeigt.

Legende des Performance-Diagramms

Wenn Sie nach unten scrollen, wird die Legende des Performance-Diagramms angezeigt. Sie können auf jede virtuelle Maschine oder auf esx-01a.corp.local klicken, um diese im Diagramm hervorzuheben.

Exportieren eines Diagrammbilds

1. Mit der Schaltfläche **Export** können Sie das Diagramm in verschiedenen Formaten exportieren: entweder als Grafik oder als CSV-Datei.
2. Klicken Sie auf den Link **Chart Options**.

Diagrammkennzahlen

Auf der linken Seite sehen Sie eine Liste der verfügbaren Diagrammkennzahlen, die angezeigt werden können. Die Zähler werden abhängig von der von Ihnen ausgewählten Kennzahl aktualisiert.

1. Wählen Sie **Memory** unter „Chart Metrics“ aus.

Sie werden feststellen, dass der Zählerabschnitt aktualisiert wird. Jetzt sind zusätzliche Zähler für dieses Diagramm verfügbar.

2. Klicken Sie auf **OK**.

Arbeitsspeicher in Echtzeit

In diesem Diagramm werden die Arbeitsspeicherzähler im Bezug auf den Arbeitsspeicher von esx-01a.corp.local angezeigt. Wenn Sie die Legende des Performance-Diagramms nach unten scrollen, sehen Sie, welche Zähler die einzelnen Linien darstellen.

Sie können jetzt weitere Diagrammoptionen testen und/oder mit dem nächsten Schritt fortfahren.

Aktivieren von DRS

Wenn Sie mit dem Ansehen der Diagramme fertig sind, muss DRS wieder aktiviert werden.

1. Wählen Sie **Cluster Site A** aus.
2. Klicken Sie auf die Registerkarte **Configure**.
3. Klicken Sie auf **vSphere DRS**.
4. Klicken Sie auf die Schaltfläche **Edit**.

Aktivieren von vSphere DRS

Aktivieren Sie das Kontrollkästchen **Turn ON vSphere DRS**, um DRS zu aktivieren, und klicken Sie auf „OK“.

Weitere Informationen

Weitere Informationen zu Performance-Diagrammen erhalten Sie im Leitfaden zu vSphere-Funktionen für Überwachung und Performance.

Schlussbemerkung

Hiermit ist Modul 1 – Einführung in das Management mit vCenter Server – abgeschlossen. Wir hoffen, dass Ihnen das Hands-on Lab weitergeholfen hat. Wir freuen uns, wenn Sie am Ende an der Umfrage teilnehmen.

Falls Sie noch Zeit haben, finden Sie nachfolgend die weiteren Module dieses Hands-on Lab mit der geschätzten Dauer, um das jeweilige Modul abzuschließen. Klicken Sie auf das Modul, um zum entsprechenden Abschnitt in diesem Handbuch zu springen.

- Modul 2 – Einführung in vSphere-Netzwerke und -Sicherheit (60 Minuten)
- Modul 3 – Einführung in vSphere-Storage (60 Minuten)

Modul 2 – Einführung in vSphere-Netzwerke und -Sicherheit (60 Minuten)

Einleitung

vSphere unterstützt zwei virtuelle Switches, den vSphere Standard Switch und den vSphere Distributed Switch.

vSphere Standard Switch

Der vSphere Standard Switch wird auf jedem ESXi-Host erstellt, der mit dem physischen Netzwerk verbunden werden muss. Jeder Switch muss auf jedem ESXi-Host einzeln erstellt und konfiguriert werden. Dies kann ein zeitaufwendiger Prozess sein. Durch Automatisierung mit Host Profiles lässt sich der Prozess etwas beschleunigen.
 Außerdem muss jeder vSphere Standard Switch auf Ebene des ESXi-Hosts verwaltet werden.

Bei der Verwendung von vSphere Standard Switches und einigen der Hochverfügbarkeitsfunktionen von vCenter ist darauf zu achten, dass die vSphere Standard Switches über alle ESXi-Hosts hinweg gleich benannt werden. Außerdem muss beachtet werden, dass Funktionen wie Network I/O Control, LLDP, Network Health Check sowie Backup und Wiederherstellung der Konfiguration nicht unterstützt werden.

vSphere Distributed Switch

Der vSphere Distributed Switch bietet gegenüber dem vSphere Standard Switch mehr Funktionen und ein einfacheres Management. Ein vSphere Distributed Switch (vDS) wird auf vCenter Server-Ebene konfiguriert und verwaltet, wo ESXi-Hosts mit einem zentralen Switch anstatt einzelner lokaler Switches verbunden sind.

Wenn sich die Konfiguration ändert, etwa durch Notwendigkeit neuer Portgruppen, muss die Änderung nur an einem Ort vorgenommen werden. Der vDS unterstützt außerdem erweiterte Netzwerkfunktionen wie Paketüberwachung und -analyse, Network I/O Control und 802.1p-Tagging.

Konfigurieren eines vSphere Standard Switch

In dieser Lektion wird der Erstellungs- und Konfigurationsprozess des vSphere Standard Switch beschrieben.

Hinzufügen einer VM-Portgruppe mit vSphere Web Client

Wenn Sie nicht bereits angemeldet sind, starten Sie den Chrome-Browser auf dem Desktop und melden Sie sich bei vSphere Web Client an.

1. Klicken Sie auf das Kontrollkästchen **Use Windows session authentication**.
2. Klicken Sie auf **Login**.

Auswählen von „Hosts and Clusters“

Wählen Sie im Menü **Home** die Option **Hosts and Clusters** aus.

Hinzufügen von Netzwerken

Erweitern Sie **Datacenter Site A** unter vcsa-01a.corp.local und anschließend **Cluster Site A**.

Klicken Sie im Navigator mit der rechten Maustaste auf **esx-02a.corp.local** und wählen Sie **Add Networking** aus.

Verbindungstyp

Wenn Sie nach dem Verbindungstyp gefragt werden, wählen Sie **Virtual Machine Port Group for a Standard Switch** aus und klicken Sie auf „Next“.

Zielgerät

Wenn Sie nach einem Zielgerät gefragt werden, wählen Sie **New Standard Switch** aus und klicken Sie auf „Next“.

Erstellen eines Standard Switch

Wählen Sie **Unused Adapters** aus und klicken Sie auf das grüne **+**.

Hinzufügen eines physischen Adapters

Wählen Sie **vmnic3** unter „Network Adapters“ aus und klicken Sie auf **OK**.

Hinzufügen eines physischen Adapters

Klicken Sie auf **Next**, um fortzufahren.

Verbindungseinstellungen

Belassen Sie im Schritt „Connection settings“ des Assistenten die Bezeichnung von „Network label“ bei **VM Network**.

Ändern Sie auch nicht den Wert von „VLAN ID“. Lassen Sie diesen auf **None (0)**.

Abschließen des Assistenten

Überprüfen Sie die Einstellungen der Portgruppe unter „Ready to complete“ und klicken Sie auf „Finish“.

(Optional) Video: Konfiguration eines vSphere Standard Switch (VSS) (4:22)

In diesem Video wird gezeigt, wie VMware vSphere Web Client zum Konfigurieren von vSphere-Hosts mithilfe des vSphere Standard Switch (VSS) verwendet wird.

Bearbeiten eines Standard Switch in vSphere Web Client

In dieser Lektion wird der in der vorherigen Lektion erstellte Standard Switch modifiziert.

Die Einstellungen des vSphere Standard Switch legen die switchweiten Standardwerte und Switch-Eigenschaften wie die Uplink-Konfiguration fest.

Auswählen von esxi-02a.corp.local

Navigieren Sie im Objektnavigator von vSphere Web Client zu **esxi-02a.corp.local**.

Auflisten der virtuellen Maschinen

Klicken Sie auf die Registerkarte **Configure** . Wählen Sie **Virtual switches** unter **Networking** aus.

Auswählen von vSwitch0

Wählen Sie den Switch **vSwitch0** in der Liste aus.

Bearbeiten von vSwitch0

Klicken Sie auf das Stiftsymbol, um den virtuellen Switch zu **bearbeiten.**.

Ändern der MTU-Einstellung eines vSphere Standard Switch (Aktivieren von Jumbo-Frames)

Wenn Sie in Ihrer Umgebung Jumbo-Frames verwenden und diese auch auf einem vSphere Standard Switch nutzen möchten, können Sie hier die MTU-Einstellung ändern.

Sie können die Größe der Maximum Transmission Unit (MTU) auf einem vSphere Standard Switch ändern, um die Menge der in einem einzelnen Paket übertragenen Nutzdaten zu vergrößern, d.h. Jumbo-Frames zu aktivieren. **Halten Sie Rücksprache mit Ihrem Netzwerkteam, bevor Sie hier Änderungen vornehmen.** Um von dem Vorteil dieser Einstellung zu profitieren und Performance-Probleme zu vermeiden, müssen die MTU-Einstellungen aller virtuellen und physischen Switches sowie Endgeräte wie Hosts und Storage-Arrays kompatibel sein.

Außerdem werden hier die Optionen „Security“, „Traffic shaping“ und „Teaming and Failover“ angezeigt. Hier werden die Standardeinstellungen für den virtuellen Switch vorgenommen. Wie Sie später sehen werden, können diese Standardwerte bei Bedarf auf Ebene der Portgruppe überschrieben werden.

Klicken Sie auf **Cancel**, um fortzufahren.

Ändern der Geschwindigkeit eines Uplink-Adapters in vSphere Web Client

Ein Uplink-Adapter kann zu einem Engpass für den Netzwerkverkehr werden, falls die Geschwindigkeit des Uplink-Adapters nicht mit der Geschwindigkeit des Netzwerkverkehrs kompatibel ist. Sie können die Verbindungsgeschwindigkeit und Duplexeinstellung eines Uplink-Adapters ändern und an die Portgeschwindigkeit des angebundenen physischen Switch anpassen.

Auswahl physischer Adapter

Klicken Sie auf **Physical adapters**.

Bearbeiten von vmnic3

Um die konfigurierte Geschwindigkeit und den Duplexwert eines physischen Netzwerkadapters zu ändern, wählen Sie **vmnic3** in der Liste aus und klicken Sie auf **Edit** (das Stiftsymbol).

Konfigurieren von Geschwindigkeit und Duplex

Die konfigurierte Geschwindigkeit und Duplexeinstellung können hier auf geeignete Werte festgelegt werden. Aufgrund der Einschränkungen des Hands-on Lab kann nur „10000 Mb, Full Duplex“ ausgewählt werden.

Klicken Sie auf **Cancel**, um fortzufahren.

Hinzufügen von Uplink-Adaptern in vSphere Web Client

Einem einzelnen vSphere Standard Switch können mehrere Adapter zugewiesen werden, um den Durchsatz zu steigern und Redundanz für Linkausfälle zu schaffen. Dies wird als „NIC-Teaming“ bezeichnet.

Auswählen von virtuellen Switches

Wählen Sie **Virtual switches** aus.

Klicken Sie auf **vSwitch0** und dann auf das Symbol zum Verwalten physischer Adapter, um die Konfiguration zu bearbeiten.

Hinzufügen eines Adapters

Fügen Sie einen Adapter hinzu, indem Sie auf das grüne **+** klicken.

Auswählen eines Adapters

Wählen Sie **vmnic2** in der Liste aus und wählen Sie **Active Adapters** aus dem Dropdown-Menü „Failover order group“ aus. Klicken Sie auf **OK**.

Anzeigen von Adaptern

Der ausgewählte Adapter wird als „Active Adapter“ unter der Liste „Assigned Adapters“ angezeigt. Klicken Sie auf **OK**, um die Änderung zu speichern.

Bearbeiten der Portgruppe eines Standard Switch

Sobald der vSwitch konfiguriert und dessen Standardwerte festgelegt wurden, kann die Portgruppe konfiguriert werden. Bei der Portgruppe handelt es sich um das Konstrukt, das mit den NICs von virtuellen Maschinen verbunden ist und üblicherweise eine VLAN- oder physische Netzwerkpartition wie Produktion, Entwicklung, Desktop oder DMZ darstellt.

Bearbeiten einer Portgruppe

Wählen Sie **vSwitch0** aus. Wählen Sie anschließend die Portgruppe **VM Network** aus und klicken Sie auf „Edit“ (das Stiftsymbol).

Eigenschaften einer Portgruppe

Unter „Properties“ können Name oder VLAN-ID der Portgruppe geändert werden.

Im Rahmen dieses Hands-on Lab ist es nicht notwendig, diese Einstellungen zu ändern.

Sicherheit einer Portgruppe

Klicken Sie im linken Fenster auf **Security**. Wenn Sie das Kontrollkästchen „Override“ aktivieren, können Sie die Standardeinstellung des virtuellen Switch dieser speziellen Portgruppe überschreiben.

In diesem Bereich können Sie Folgendes konfigurieren:

Promiscuous Mode

- Reject: Wird ein Gastadapter in den „Promiscuous Mode“ versetzt, hat dies keine Auswirkungen darauf, welche Frames vom Adapter empfangen werden.
- Accept: Wird ein Gastadapter in den „Promiscuous Mode“ versetzt, erkennt dieser alle Frames, die im Rahmen der erlaubten VLAN-Richtlinie der Portgruppe, mit der

dieser Adapter verbunden ist, vom vSphere Standard Switch weitergeleitet werden.

MAC Address Changes

- Reject: Wenn Sie „MAC Address Changes“ auf „Reject“ festlegen und das Gastbetriebssystem die MAC-Adresse des Adapters auf einen anderen Wert als in der .vmx-Konfigurationsdatei angegeben ändert, werden alle eingehenden Frames verworfen. Wenn das Gastbetriebssystem die MAC-Adresse zurück auf den in der .vmx-Konfigurationsdatei angegebenen Wert ändert, werden eingehende Frames wieder weitergeleitet.
- Accept: Eine Änderung der MAC-Adresse durch das Gastbetriebssystem hat folgenden Effekt: Frames, die an die geänderte MAC-Adresse gesendet werden, werden von der virtuellen Maschine empfangen.

Forged Transmits

- Reject: Ausgehende Frames mit einer MAC-Quelladresse, die sich von der aktuellen MAC-Adresse des Adapters unterscheidet, werden verworfen.
- Accept: Es findet keine Filterung statt und alle ausgehenden Frames werden weitergeleitet.

Hier müssen keine Änderungen vorgenommen werden und Sie können mit dem nächsten Schritt fortfahren.

Traffic Shaping

Klicken Sie im linken Fenster auf **Traffic shaping**. Aktivieren Sie anschließend das Kontrollkästchen neben „Override“. Wie in den Sicherheitseinstellungen kann die auf Switch-Ebene festgelegte Standardrichtlinie, die nur auf diese Portgruppe angewendet wird, überschrieben werden.

Eine Traffic Shaping-Richtlinie wird durch die durchschnittliche Bandbreite, Spitzenbandbreite und Burst-Größe definiert. Eine Traffic Shaping-Richtlinie kann für jede Portgruppe festgelegt werden.

ESXi steuert den ausgehenden Netzwerkverkehr auf Standard Switches. Traffic Shaping schränkt zwar die auf einem Port verfügbare Netzwerkbandbreite ein, kann jedoch auch so konfiguriert werden, dass kurze Datenspitzen mit höheren Geschwindigkeiten zugelassen werden.

Average Bandwidth

- Legt fest, wie viele Bits pro Sekunde einen Port im Durchschnitt durchlaufen dürfen. Diese Zahl ist die zugelassene Durchschnittslast.

Peak Bandwidth

- Die maximalen Bits pro Sekunde, die bei Lastspitzen von einem Port empfangen oder gesendet werden dürfen. Diese Zahl schränkt die Bandbreite eines Ports bei Lastspitzen ein.

Burst Size

- Maximale Bytes, die bei einem Burst erlaubt sind. Wenn dieser Parameter festgelegt ist, kann ein Port einen Burst-Bonus erhalten, wenn er nicht die gesamte ihm zugeteilte Bandbreite nutzt. Wenn der Port mehr Bandbreite benötigt als in der Durchschnittsbandbreite angegeben ist, darf der Port Daten vorübergehend mit einer höheren Geschwindigkeit übertragen, wenn ein Burst-Bonus verfügbar ist. Dieser Parameter schränkt die Anzahl an Bytes ein, die im Burst-Bonus angesammelt wurden, und überträgt Datenverkehr mit einer höheren Geschwindigkeit.

Hier müssen keine Änderungen vorgenommen werden und Sie können mit dem nächsten Schritt fortfahren.

Teaming und Failover

Klicken Sie im linken Fenster auf **Teaming and failover**. Es besteht wiederum die Möglichkeit, die Standardeinstellungen des virtuellen Switch zu überschreiben.

Load Balancing: Die Richtlinie für den Lastausgleich legt fest, wie Datenverkehr zwischen den Netzwerkadaptern eines NIC-Teams verteilt wird. Virtuelle Switches in

vSphere gleichen nur den ausgehenden Datenverkehr aus. Der eingehende Datenverkehr wird durch die Richtlinie für den Lastausgleich auf dem physischen Switch gesteuert.

- Route based on the originating virtual port: Es wird ein Uplink basierend auf der virtuellen Port-ID des Switch ausgewählt. Nachdem der virtuelle Switch einen Uplink für eine virtuelle Maschine oder einen VMkernel-Adapter ausgewählt hat, leitet er Datenverkehr immer über denselben Uplink an diese virtuelle Maschine oder diesen VMkernel-Adapter weiter.
- Route based on IP hash: Es wird ein Uplink basierend auf einem Hash der Quell- und Ziel-IP-Adresse jedes Pakets gewählt. Bei Nicht-IP-Paketen verwendet der Switch die Daten dieser Felder zum Berechnen des Hash-Werts. Für IP-basiertes Teaming muss der physische Switch mit EtherChannel konfiguriert sein.
- Route based on source MAC hash: Es wird ein Uplink basierend auf einem Hash der Quell- Ethernet MAC-Adresse gewählt.
- Route based on physical NIC load: Ist bei verteilten Portgruppen oder verteilten Ports verfügbar. Es wird ein Uplink basierend auf der Last, die aktuell auf dem mit der Portgruppe oder dem Port verbundenen physischen Netzwerkadapter anliegt, ausgewählt. Wenn ein Uplink länger als 30 Sekunden zu mindestens 75 Prozent ausgelastet wird, verlagert der Host-Proxy-Switch einen Teil des VM-Datenverkehrs auf einen physischen Adapter mit freier Kapazität.
- Use explicit failover order: Aus der Liste der aktiven Adapter wird immer der erste Uplink verwendet, der die Failover-Erkennungskriterien erfüllt. Bei dieser Option findet kein tatsächlicher Lastausgleich statt.

Network Failure Detection: Hier wird die Methode ausgewählt, die der virtuelle Switch zur Failover-Erkennung nutzt.

- Link Status only: Diese Methode verlässt sich ausschließlich auf den Linkstatus, der vom Netzwerkadapter gemeldet wird. Mit dieser Option können Ausfälle wie abgesteckte Kabel oder ein Stromausfall am physischen Switch erkannt werden.
- Beacon Probing: Diese Option beinhaltet das Senden und Empfangen von Testsignalen auf allen NICs des Teams. Diese Testsignale werden zusammen mit dem Linkstatus genutzt, um Linkausfälle zu erkennen. ESXi sendet einmal pro Sekunde ein Testsignalpaket. Die NICs müssen sich in einer Aktiv/Aktiv- oder Aktiv/Standby-Konfiguration befinden, da keine Testsignale an die Reserve-NICs gesendet werden.

Notify Switches: Diese Option legt fest, ob der virtuelle Switch den physischen Switch über einen Ausfall in Kenntnis setzt.

Failover: Diese Option gibt an, ob ein physischer Adapter im Anschluss an die Wiederherstellung nach einem Ausfall wieder aktiviert wird.

- Wenn „Failback“ auf die Standardauswahl „Yes“ festgelegt ist, wird der Adapter sofort nach der Wiederherstellung wieder in den aktiven Betrieb genommen. Er ersetzt dann den Reserveadapter, der ggf. seinen Platz eingenommen hat.

- Wenn „Failback“ für einen Standardport auf „No“ festgelegt ist, bleibt ein ausgefallener Adapter nach der Wiederherstellung so lange inaktiv, bis ein momentan aktiver Adapter ausfällt und ersetzt werden muss.

Sie können außerdem die Standardeinstellung des virtuellen Switch für die Failover-Reihenfolge der physischen Adapter überschreiben.

Hier müssen keine Änderungen vorgenommen werden und Sie können mit dem nächsten Schritt fortfahren.

Abbrechen der Änderungen

Da keine Änderungen an der Portgruppe vorgenommen werden sollen, klicken Sie auf die Schaltfläche **Cancel**.

Schlussbemerkung

Beim vSphere Standard Switch handelt es sich um einen einfachen virtuellen Switch, der auf Hostebene konfiguriert und verwaltet wird. Dieser Switch bietet Zugriff, Datenverkehrsaggregation und Fehlertoleranz, indem mehrere physische Adapter an einen virtuellen Switch angebunden werden können.

Der VMware vSphere Distributed Switch erweitert die Funktionen des vSS und vereinfacht das Management in großen Bereitstellungen, indem er als einzelner Switch dargestellt wird, der mehrere verknüpfte Hosts umspannt. So müssen Änderungen nur ein Mal vorgenommen werden, da sie von allen Mitglieder-Hosts des Switch übernommen werden.

Hinzufügen und Konfigurieren eines vSphere Distributed Switch

In dieser Lektion wird das Hinzufügen und Konfigurieren eines Distributed Switch beschrieben.

Mit der Erstellung eines vSphere Distributed Switch in einem vSphere-Rechenzentrum kann der Netzwerkdatenverkehr aller zugehörigen Hosts des Rechenzentrums abgewickelt werden. Falls Ihr System viele Hosts und komplexe Portgruppenanforderungen besitzt, kann der Administrationsaufwand durch die Erstellung verteilter Portgruppen anstatt Standardportgruppen stark vermindert werden.

Hinzufügen eines vSphere Distributed Switch mittels vSphere Web Client

Klicken Sie im Navigator mit der rechten Maustaste auf „Datacenter Site A“ und wählen Sie „Distributed Switch“ --> „New Distributed Switch...“ aus.

Name und Standort

Behalten Sie den Standardnamen für den neuen Distributed Switch bei und klicken Sie auf **Next**.

Auswählen der Version

Stellen Sie sicher, dass „Distributed Switch: 6.5.0“ ausgewählt ist, und klicken Sie auf **Next**.

Beachten Sie, dass die Version des Distributed Switch festlegt, welche Versionen des ESXi-Hosts dem Switch beitreten können. Sobald ein Upgrade für alle Mitgliederhosts eines Distributed Switch durchgeführt wurde, kann auch für den Switch selbst ein Upgrade auf die passende Version durchgeführt werden. In diesem Hands-on Lab befinden sich alle ESXi-Hosts auf Version 6.5.0.

Bearbeiten der Einstellungen

Behalten Sie die Standardeinstellungen bei und klicken Sie auf **Next**.

Abschließen des Vorgangs

Überprüfen Sie die ausgewählten Einstellungen und klicken Sie auf „Finish“.

Hinweis: Die nächsten Schritte gelten für die Erstellung von verteilten Portgruppen und das Hinzufügen von Hosts.

(Optional) Video: VMware vSphere: Netzwerk – vSphere Distributed Switch (vDS) (15:15)

In diesem Video wird die Konfiguration des vSphere Distributed Switch gezeigt. vSphere Distributed Switches verfügen über alle Funktionen von vSphere Standard Switches sowie zahlreiche zusätzliche Funktionen.

Hinzufügen von Hosts zu einem vSphere Distributed Switch in vSphere Web Client

Nach der Erstellung eines vSphere Distributed Switch müssen zur Erstellung eines virtuellen Netzwerks Hosts und physische Adapter hinzugefügt werden.

Klicken Sie auf die Registerkarte **Networking**.

Hinzufügen von Hosts

Erweitern Sie „Datacenter Site A“, bis der von Ihnen erstellte Distributed Switch **DSwitch** angezeigt wird.

Klicken Sie mit der rechten Maustaste auf **DSwitch** und wählen Sie **Add and Manage Hosts** aus.

Auswählen der Aufgabe

Wählen Sie **Add hosts** aus und klicken Sie auf **Next**.

Auswählen von Hosts

Um Hosts zum Distributed Switch hinzuzufügen, klicken Sie auf das grüne **+**.

Auswählen der Hosts

Wählen Sie alle angezeigten ESXi-Hosts (**esx-01a.corp.local und esx-02a.corp.local**) aus und klicken Sie auf **OK**.

Auswählen von Hosts (Forts.)

Sie sollten jetzt die Hosts sehen, die zum Switch hinzugefügt werden. Klicken Sie auf **Next**.

Auswählen der Netzwerkadapteraufgaben

Behalten Sie die Standardwerte bei und klicken Sie auf **Next**, um fortzufahren.

Management physischer Netzwerkadapter

Im Rahmen des Prozesses zum Hinzufügen von Hosts muss jeweils mindestens ein Adapter jedes physischen Hosts dem Distributed Switch zugewiesen werden. Die zugewiesenen Adapter dürfen nicht mit einem anderen Switch auf dem Host geteilt werden.

Wählen Sie **vmnic3** unter „esx-01a.corp.local“ aus und klicken Sie auf **Assign uplink**.

Auswählen eines Uplink für vmnic3

Wählen Sie **Uplink 1** aus und klicken Sie auf **OK**.

Bestätigen des Hinzufügens

(Optional) Sie können vmnic3 vom Host „esx-02a.corp.local“ mit denselben Schritten wie bei „esx-01a.corp.local“ hinzufügen oder einfach auf **Next** klicken, um fortzufahren.

Warnmeldung

Wenn Sie nicht eine vmnic von jedem ESXi-Host hinzugefügt haben, erhalten Sie diese Warnmeldung.

In diesem Hands-on Lab können Sie einfach auf OK klicken, um fortzufahren.

Management virtueller Netzwerkadapter

In Ihrer Umgebung können Sie entscheiden, ob virtuelle Netzwerkadapter von einem vSphere Standard oder Distributed Switch auf den neuen Switch migriert werden sollen. In diesem Beispiel ist keine Migration erforderlich. Klicken Sie auf **Next**, um fortzufahren.

Analysieren der Auswirkungen

Es wird geprüft, ob die von Ihnen vorgenommenen Einstellungen andere netzwerkabhängige Services wie iSCSI beeinträchtigen. Klicken Sie auf **Next**, um fortzufahren.

Abschließen des Vorgangs

Überprüfen Sie die Änderungen, die Sie vornehmen möchten. Klicken Sie auf **Finish**, um die Änderungen zu übernehmen.

Management von Hosts auf einem vSphere Distributed Switch in vSphere Web Client

Sie können die Konfiguration von Hosts und physischen Adaptern auf einem vSphere Distributed Switch ändern, nachdem sie zum Distributed Switch hinzugefügt wurden.

Klicken Sie im Navigator mit der rechten Maustaste auf „DSwitch“ und wählen Sie „Add and Manage Hosts“ aus.

Auswählen der Aufgabe

Wählen Sie **Manage host networking** im Fenster „Select tasks“ aus und klicken Sie auf **Next**.

Auswählen von Hosts

Klicken Sie auf das grüne **+**, um die zu bearbeitenden Hosts auszuwählen.

Auswählen der Mitgliederhosts

Wählen Sie für die Aufgabe **esx-01a.corp.local** im Fenster „Select member hosts“ aus und klicken Sie auf **OK**.

Auswählen von Hosts (Forts.)

„esx-01a.corp.local“ sollte nun hinzugefügt worden sein. Klicken Sie auf **Next**.

Auswählen der Netzwerkadapteraufgaben

Behalten Sie die Standardeinstellungen bei und klicken Sie auf **Next**, um fortzufahren.

Management physischer Netzwerkadapter

Hier muss nichts geändert werden. Klicken Sie auf **Next**, um fortzufahren.

Management virtueller Netzwerkadapter

Als Nächstes wird ein VMkernel-Adapter zum Switch hinzugefügt. Klicken Sie auf **On this switch** und anschließend auf **New adapter**.

Auswählen des Zielgeräts

Klicken Sie auf die Schaltfläche **Browse**, um die verteilte Portgruppe und den Switch auszuwählen.

Auswählen des Netzwerks

Klicken Sie auf **DPortGroup** und **OK**.

Auswählen des Zielgeräts (Forts.)

Sie sehen, dass „DPortGroup“ hinzugefügt wurde. Klicken Sie auf **Next**.

Porteigenschaften

Übernehmen Sie die Standardwerte und klicken Sie auf **Next**.

IPv4-Einstellungen

Klicken Sie auf **Next**, um fortzufahren.

Abschließen des Vorgangs

Überprüfen Sie die Einstellungen und klicken Sie auf **Finish**.

Neuer VMkernel-Port hinzugefügt

Sie sehen den neuen virtuellen Netzwerkadapter, den Sie hinzugefügt haben. Klicken Sie auf **Next**, um fortzufahren.

Analysieren der Auswirkungen

Der Assistent überprüft erneut, ob die von Ihnen vorgenommenen Einstellungen andere abhängige Netzwerkservices beeinträchtigen. Klicken Sie auf „Next“, um fortzufahren.

Abschließen des Vorgangs

Klicken Sie auf **Finish**.

Bearbeiten der allgemeinen und erweiterten vSphere Distributed Switch-Einstellungen in vSphere Web Client

Die allgemeinen Einstellungen eines vSphere Distributed Switch umfassen den Namen des Distributed Switch und die Anzahl der Uplink-Ports auf dem Distributed Switch. Die erweiterten Einstellungen eines vSphere Distributed Switch umfassen die Konfiguration des Discovery-Protokolls und die maximale MTU für den Switch. Sowohl die allgemeinen als auch erweiterten Einstellungen können mittels vSphere Web Client konfiguriert werden.

1. Vergewissern Sie sich, dass **DSwitch** im Navigator ausgewählt ist.
2. Klicken Sie auf die Registerkarte **Configure**.

3. Klicken Sie unter **Settings** auf **Properties**.

Bearbeiten der Switch-Einstellungen

Klicken Sie auf **Edit**.

Allgemeine Einstellungen

Klicken Sie auf „General“, um die Einstellungen des vSphere Distributed Switch anzuzeigen. Hier können Sie Folgendes ändern:

Name: Sie können den Namen des Distributed Switch ändern.

Number of Uplinks: Sie können die Anzahl der mit dem Distributed Switch verbundenen Uplink-Ports vergrößern oder verkleinern. Hinweis: Mit der Schaltfläche „Edit uplink names“ können Sie die Uplinks außerdem sinnvoll benennen.

Number of Ports: Diese Einstellung kann nicht geändert werden. Die Anzahl der Ports wird standardmäßig dynamisch nach oben oder unten skaliert.

Network I/O Control: Über das Dropdown-Menü können Sie Network I/O Control auf dem Switch aktivieren oder deaktivieren.

Description: In diesem Feld können Sie eine sinnvolle Beschreibung des Switch angeben.

Erweiterte Einstellungen

Klicken Sie auf „Advanced“, um die Einstellungen des vSphere Distributed Switch anzuzeigen. Hier finden Sie die folgenden erweiterten Einstellungen für den Switch:

MTU (Bytes): Diese Option gibt die maximale MTU-Größe für den vSphere Distributed Switch an. Um Jumbo-Frames zu aktivieren, geben Sie einen Wert größer 1500 Byte ein. Halten Sie Rücksprache mit Ihrem Netzwerkteam, bevor Sie in Ihrer Umgebung Änderungen an dieser Einstellung vornehmen.

Multicast filtering mode

- Basic: Der Distributed Switch leitet den mit einer Multicast-Gruppe verbundenen Datenverkehr basierend auf einer MAC-Adresse, die aus den letzten 23 Bit der IPv4-Adresse der Gruppe generiert wird, weiter.
- IGMP/MLD snooping: Der Distributed Switch leitet Multicast-Datenverkehr an virtuelle Maschinen weiter. Dies erfolgt gemäß den IPv4- und IPv6-Adressen der abonnierten Multicast-Gruppen mittels Mitgliedschaftsnachrichten, die vom Internet Group Management Protocol (IGMP) und Multicast Listener Discovery-Protokoll definiert wurden.

Discovery Protocol

- Type: „Cisco Discovery Protocol“, „Link Layer Discovery Protocol“ oder „disabled“.
- Operation: „Listen“, „Advertise“ oder „Both“.

Administrator Contact: Hier geben Sie den Namen und andere Kontaktinformationen des für den Distributed Switch zuständigen Administrators ein.

Hier sind keine Änderungen notwendig. Klicken Sie auf **Cancel**.

Aktivieren oder Deaktivieren der vSphere Distributed Switch-Systemdiagnose in vSphere Web Client

Die Distributed Switch-Systemdiagnose überwacht Änderungen in vSphere Distributed Switch-Konfigurationen. Die vSphere Distributed Switch-Systemdiagnose muss aktiviert sein, damit Distributed Switch-Konfigurationen überprüft werden können.

Die Systemdiagnose für Distributed Switches steht ab ESXi 5.1 zur Verfügung. Systemdiagnoseinformationen können außerdem erst ab vSphere Web Client 5.1 angezeigt werden.

1. Klicken Sie auf die Registerkarte **Health check** unter „DSwitch“. Hier sehen Sie, dass „Health check“ für „VLAN and MTU“ sowie für „Teaming and failover“ deaktiviert ist.
2. Klicken Sie auf die Schaltfläche **Edit**.

Bearbeiten der Systemdiagnoseeinstellungen

Wählen Sie für beide **Enabled** aus und klicken Sie auf **OK**.

Verteilte Portgruppen

Eine verteilte Portgruppe gibt die Portkonfigurationsoptionen für die Mitgliederports auf einem vSphere Distributed Switch an. Verteilte Portgruppen legen fest, auf welche Weise die Verbindung mit einem Netzwerk erfolgt.

Klicken Sie im Navigator mit der rechten Maustaste auf **DSwitch** und wählen Sie **Distributed Port Group** --> **New Distributed Port Group** aus.

Auswählen des Namens und Standorts

Benennen Sie die neue Portgruppe **WebVMTrafic** und klicken Sie auf „Next“.

Konfigurieren der Einstellungen

Beim Erstellen einer verteilten Portgruppe gibt es folgende Optionen:

Port binding: Mit dieser Option legen Sie fest, wann Ports den mit dieser verteilten Portgruppe verbundenen virtuellen Maschinen zugewiesen werden.

- Static binding: Mit dieser Option wird ein Port einer virtuellen Maschine zugewiesen, wenn sich die virtuelle Maschine mit der verteilten Portgruppe verbindet.
- Dynamic binding: Mit dieser Option weisen Sie einer virtuellen Maschine einen Port zu, wenn diese das erste Mal eingeschaltet wird, nachdem sie mit der verteilten Portgruppe verbunden wurde. „Dynamic binding“ wird seit ESXi 5.0 nicht mehr unterstützt.
- Ephemeral: Keine Portbindung. Mit der Portbindung „Ephemeral“ können Sie eine virtuelle Maschine einer verteilten Portgruppe zuweisen, auch wenn diese mit dem Host verbunden ist.

Port allocation

- Elastic: Die Standardanzahl von Ports beträgt acht. Wenn alle Ports zugewiesen sind, werden acht weitere Ports erstellt. Dies ist die Standardoption.
- Fixed: Die Standardanzahl von Ports beträgt acht. Wenn alle Ports zugewiesen sind, werden keine weiteren Ports erstellt.

Number of ports: Hier geben Sie die Portanzahl der verteilten Portgruppe ein.

Network resource pool: Wenn Sie zur Steuerung des Netzwerkverkehrs einen Netzwerkpool erstellt haben, kann dieser hier ausgewählt werden.

VLAN: Im Dropdown-Menü „Type“ können Sie folgende VLAN-Optionen festlegen:

- None: Es wird kein VLAN verwendet.
- VLAN: Im Feld „VLAN ID“ kann eine Nummer zwischen 1 und 4094 eingegeben werden.
- VLAN Trunking: Hier wird ein VLAN-Trunk-Bereich eingegeben.
- Private VLAN: Hier wählen Sie einen Eintrag für ein privates VLAN aus. Wenn kein privates VLAN erstellt wurde, ist dieses Menü leer.

Advanced: Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Richtlinienkonfigurationen der neuen verteilten Portgruppe anpassen möchten.

Akzeptieren Sie die Standardeinstellungen und klicken Sie auf „Next“, um fortzufahren.

Abschließen des Vorgangs

Überprüfen Sie Ihre Einstellungen und klicken Sie auf **Finish**, um die verteilte Portgruppe zu erstellen.

Anzeigen der neuen verteilten Portgruppe

Wenn Sie **DSwitch** im Navigator erweitern, wird die neu erstellte verteilte Portgruppe **WebVMTraffic** angezeigt.

Verwenden des Host-Sperrmodus

Um die Sicherheit Ihrer ESXi-Hosts zu verbessern, können Sie diese in den Sperrmodus versetzen.

Wenn Sie den Sperrmodus aktivieren, besitzt ausschließlich der Anwender „vpxuser“ Authentifizierungsberechtigungen. Andere Anwender können Vorgänge auf dem Host nicht direkt ausführen. Durch den Sperrmodus müssen alle Vorgänge über vCenter Server ausgeführt werden.

Wenn der Sperrmodus für einen Host aktiviert wurde, können Sie keine vSphere CLI-Befehle in Bezug auf den Host über einen Administrationsserver, über ein Skript oder über von vSphere Management Assistant (vMA) ausführen. Möglicherweise können auch über externe Software- oder Managementtools keine Informationen vom ESXi-Host abgerufen oder geändert werden.

Der Sperrmodus ist nur auf ESXi-Hosts verfügbar, die zu vCenter Server hinzugefügt wurden. Sie können den Sperrmodus aktivieren, indem Sie einen Host mit dem Assistenten zum Hinzufügen von Hosts zu vCenter Server hinzufügen, indem Sie vSphere Web Client zum Verwalten eines Hosts verwenden oder indem Sie das Direct Console User Interface (DCUI) verwenden.

HINWEISE:

Anwendern mit DCUI-Zugriffsberechtigung ist es gestattet, sich auf dem Direct Console User Interface (DCUI) anzumelden, wenn der Sperrmodus aktiviert ist. Wenn Sie den Sperrmodus mithilfe des DCUI deaktivieren, wird allen Anwendern mit DCUI-Zugriffsberechtigung die Administratorrolle auf dem Host erteilt. Die DCUI-Zugriffsberechtigung wird in den erweiterten Einstellungen auf dem Host erteilt.

Wenn Sie den Sperrmodus mithilfe des Direct Console User Interface (DCUI) aktivieren oder deaktivieren, werden die Berechtigungen, die Anwendern und Gruppen auf dem Host zugewiesen sind, verworfen. Um diese Berechtigungen beizubehalten, müssen Sie den Sperrmodus mithilfe des mit vCenter Server verbundenen vSphere Client aktivieren oder deaktivieren.

Die Aktivierung oder Deaktivierung des Sperrmodus beeinflusst zwar, welche Anwendertypen auf Hostservices zugreifen dürfen, es beeinflusst jedoch nicht die Verfügbarkeit dieser Services. Anders ausgedrückt: Wenn die Services ESXi Shell, SSH oder Direct Console User Interface (DCUI) aktiviert sind, werden diese weiterhin ausgeführt, unabhängig davon, ob sich der Host im Sperrmodus befindet oder nicht.

Auswählen von „Hosts and Clusters“

Wählen Sie im Navigator die Registerkarte **Hosts and Clusters** aus.

Wählen Sie anschließend **esx-01a.corp.local** aus.

Sicherheitsprofil

Bevor Sie den Host-Sperrmodus konfigurieren, müssen Sie sich vergewissern, dass der SSH-Service auf „esx-01a.corp.local“ ausgeführt wird.

Klicken Sie zunächst auf die Registerkarte **Configure** unter „esx-01a“. Scrollen Sie nach unten zum Abschnitt **System**. Klicken Sie anschließend auf **Security Profile**.

Überprüfen, ob SSH aktiviert ist

Scrollen Sie nach unten bis zum Abschnitt **Services** .

Hier sehen Sie, dass **SSH service** aktiviert ist und auf esx-01a.corp.local **ausgeführt wird.**.

Öffnen einer SSH-Sitzung zu esx-01a

Prüfen Sie, ob Sie sich mithilfe einer SSH-Verbindung auf esx-01a anmelden können.

Klicken Sie in der Windows-Taskleiste auf das **PuTTY**-Symbol.

Verbinden mit esx-01a

Wählen Sie **esx-01a.corp.local** unter „Saved Sessions“ aus und klicken Sie auf die Schaltfläche **Open**.

Auf esx-01a angemeldet

Sie werden automatisch auf esx-01a.corp.local angemeldet, da eine Public-Key-Authentifizierung zwischen der Maschine mit der Hauptkonsole und dem ESXi-Host eingerichtet wurde.

Schließen der PuTTY-Sitzung

Schließen Sie die PuTTY-Sitzung, indem Sie **exit** eingeben und die Eingabetaste drücken. Nachdem Sie die Eingabetaste gedrückt haben, wird das PuTTY-Fenster geschlossen.

Aktivieren des Sperrmodus

Scrollen Sie im vSphere Web Client nach unten bis zum Abschnitt **Lockdown Mode**.

Klicken Sie auf die Schaltfläche **Edit**.

Sperrmodus

Klicken Sie auf das Optionsfeld „Normal“ und klicken Sie auf „Next“.

Hinweis: Es besteht die Möglichkeit, „Exception Users“ anzugeben.

Aktivierter Sperrmodus

Nachdem vSphere Web Client aktualisiert wurde, sehen Sie, dass der Sperrmodus aktiviert wurde.

PuTTY-Sitzung zu esx-01a

Befolgen Sie dieselben Schritte wie oben und öffnen Sie die **PuTTY**-Anwendung über die Windows-Taskleiste.

Klicken Sie unter „Saved Sessions“ auf **esx-01a.corp.local** und klicken Sie auf **Open**.

Abgelehnt!

Beim Verbindungsaufbau mit esx-01a.corp.local sollte eine Fehlermeldung angezeigt werden. Da der Sperrmodus auf dem Host konfiguriert wurde, lehnt dieser alle Remote-Verbindungen von Anwendern ab, die sich nicht auf der Liste „Exception User“ befinden.

Klicken Sie auf **OK** und schließen Sie PuTTY, indem Sie auf das **X** rechts oben in der Fensterecke klicken.

Deaktivieren des Sperrmodus

Sie befinden sich wieder in vSphere Web Client. Klicken Sie erneut auf die Schaltfläche **Edit** unter „Lockdown Mode“.

Aktivieren Sie das Kontrollkästchen „Disabled“. Klicken Sie auf „OK“.

Aktivieren Sie das Optionsfeld **Disabled** und klicken Sie auf **OK**, um fortzufahren.

Host-Sperrmodus deaktiviert

Damit sollte der Sperrmodus auf dem Host deaktiviert sein.

Der Host-Sperrmodus ist eine ausgezeichnete Möglichkeit, um Ihre vSphere-Hosts weiter abzusichern. Weitere Informationen erhalten Sie im folgenden Video.

Hiermit ist die Lektion zum Host-Sperrmodus abgeschlossen.

Video: Aktivieren des vSphere-Host-Sperrmodus in VMware vSphere (4:48)

In diesem Video wird gezeigt, wie VMware vSphere-Hosts mit dem Sperrmodus abgesichert werden können, um den direkten Zugriff auf die Hostkonsole zu beschränken und ein Management der Hosts über vCenter Server zu erzwingen.

Konfigurieren der Host-Services und -Firewall

Diese Lektion enthält ein kurzes Video über die Verwendung der VMware ESXi-Firewall.

Video: Konfigurieren der vSphere-Host-Firewall für VMware vSphere (4:34)

In diesem Video wird gezeigt, wie die VMware ESXi-Firewall auf dem vSphere-Host verwendet wird, um die eingehende und ausgehende Kommunikation zu unterbinden und die auf dem Host ausgeführten Services zu verwalten.

Rollen für Anwenderzugriff und Authentifizierung

VMware empfiehlt die Erstellung von Rollen, um den Zugriff entsprechend den Anforderungen Ihrer Umgebung zu steuern. Wenn Sie eine Rolle auf einem vCenter Server-System, das Teil einer vernetzten Gruppe im verknüpften Modus ist, erstellen oder bearbeiten, werden die von Ihnen vorgenommenen Änderungen von allen anderen vCenter Server-Systemen der Gruppe übernommen.

Der verknüpfte Modus vernetzt mehrere vCenter Server-Systeme unter Verwendung eines oder mehrerer Platform Services Controller miteinander. So können Sie alle verknüpften vCenter Servers anzeigen und durchsuchen sowie Rollen, Genehmigungen, Lizenzen, Richtlinien und Tags replizieren.

Erstellen einer Rolle in vSphere Web Client

In den folgenden Schritten wird eine Rolle in vSphere Web Client erstellt, der Rechte zugewiesen werden können.

Administration

Klicken Sie in vSphere Web Client auf das **Haussymbol** und wählen Sie **Administration** aus.

Rollen

Vergewissern Sie sich, dass die Registerkarte „Roles“ ausgewählt ist.

Erstellen einer Rolle

Klicken Sie auf das grüne **+**, um eine Rolle zu erstellen.

Rollenname

1. Nennen Sie die Rolle **HOL Role**.
2. Klicken Sie auf das Kontrollkästchen **All Privileges**.
3. Klicken Sie auf die Schaltfläche **OK**, um die neue Rolle zu erstellen.

Bearbeiten einer Rolle in vSphere Web Client

Beim Bearbeiten einer Rolle können Sie die ausgewählten Berechtigungen dieser Rolle bearbeiten. Wenn Sie fertig sind, werden diese Berechtigungen auf alle Anwender oder Gruppen angewendet, denen die bearbeitete Rolle zugewiesen wurde. Im verknüpften Modus werden alle von Ihnen vorgenommenen Änderungen von allen anderen vCenter Server-Systemen der Gruppe übernommen. Rollenzuweisungen zu bestimmten Anwendern und Objekten werden jedoch nicht von den miteinander verknüpften vCenter Server-Systemen geteilt.

Bearbeiten der Rolle „HOL Role“

1. Klicken Sie auf die Rolle **HOL Role**, um sie auszuwählen.
2. Klicken Sie auf die Schaltfläche **Edit**.

Entfernen von Berechtigungen

Falls Ihr Unternehmen separate Teams für das Management von Netzwerk und Storage einsetzt, benötigt die Rolle „HOL Role“ keinen Zugriff auf diese Bereiche.

Deaktivieren Sie die Kontrollkästchen für die Ansichten **Networking** und **Storage** und klicken Sie auf **OK**.

Klonen einer Rolle in vSphere Web Client

Sie können eine bestehende Rolle kopieren, umbenennen und bearbeiten. Wenn Sie eine Kopie erstellen, wird die neue Rolle nicht auf Anwender, Gruppen oder Objekte angewendet. Sie erbt lediglich die Einstellungen von der übergeordneten Rolle. Im verknüpften Modus werden Änderungen zwar von allen anderen vCenter Server-Systemen in der Gruppe übernommen, die Zuweisungen von Rollen zu bestimmten Anwendern und Objekten werden jedoch nicht von den verknüpften vCenter Server-Systemen geteilt.

Klonen einer Rolle

1. Klicken Sie auf die Rolle **HOL Role**, um sie auszuwählen.
2. Klicken Sie auf die Schaltfläche **Clone**.

Rollenname und Berechtigungen

1. Benennen Sie die geklonte Rolle **HOL Dev Role**. Da die Rolle geklont wurde, besitzt sie nicht die Berechtigungen für die von HOL Dev-Anwendern benötigten Netzwerk- und Storage-Sichten.

2. Aktivieren Sie das Kontrollkästchen **All Privileges**, um dieser Rolle wieder volle Administratorberechtigungen zu erteilen.
3. Klicken Sie auf **OK**, um das Klonen abzuschließen.

Neue Rolle geklont

Die von Ihnen aus einer bestehenden Rolle geklonte Rolle sollte jetzt angezeigt werden.

Umbenennen einer Rolle in vSphere Web Client

Wenn Sie die Privilegien einer Rolle ändern, möchten Sie diese möglicherweise umbenennen. Wenn Sie eine Rolle umbenennen, ändern sich die Zuweisungen dieser Rolle nicht. Im verknüpften Modus werden Änderungen an den Rollen zwar von allen anderen vCenter Server-Systemen in der Gruppe übernommen, die Zuweisungen von Rollen werden jedoch nicht von den verknüpften vCenter Server-Systemen geteilt.

Bearbeiten des Rollennamens

Klicken Sie auf die Rolle **HOL Role**, um sie auszuwählen, und klicken Sie auf die Schaltfläche **Edit**.

Neuer Name

1. Benennen Sie die Rolle in **HOL Admin Role** um.
2. Klicken Sie auf **OK**.

Entfernen einer Rolle in vSphere Web Client

Wenn Sie eine Rolle entfernen, die keinen Anwendern oder Gruppen zugewiesen ist, wird die Definition dieser Rolle aus der Liste von Rollen entfernt. Wenn Sie eine Rolle entfernen, die einem Anwender oder einer Gruppe zugewiesen ist, können Sie die Zuweisungen entfernen oder durch Zuweisung einer anderen Rolle ersetzen.

HINWEIS:

Bevor Sie eine Rolle von einem vCenter Server-System, das Teil einer vernetzten Gruppe im verknüpften Modus ist, entfernen, müssen Sie prüfen, ob die Rolle auf anderen vCenter Server-Systemen der Gruppe verwendet wird. Wenn Sie eine Rolle von einem vCenter Server-System entfernen, wird diese Rolle von allen anderen vCenter Server-Systemen der Gruppe entfernt, selbst wenn Sie Berechtigungen einer anderen Rolle auf dem aktuellen vCenter Server-System zuweisen.

Löschen einer Rolle

1. Klicken Sie auf die Rolle **HOL Admin Role**, um sie auszuwählen.
2. Klicken Sie auf die Schaltfläche **Delete**.

Bestätigen des Löschens

Klicken Sie auf **Yes**, um zu bestätigen, dass Sie diese Rolle löschen möchten.

Rolle gelöscht

Wie Sie sehen, wurde die Rolle „HOL Admin Role“ gelöscht.

Die Erstellung eigener und detaillierter Rollen für Anwender in Ihrer Organisation schafft ein höheres Maß an Sicherheit in Ihrer vSphere-Infrastruktur.

Hiermit ist die Lektion zu Rollen für Anwenderzugriff und Authentifizierung abgeschlossen.

Erläuterung von Single Sign-On

Die Authentifizierung und das Management von vCenter Server-Anwendern erfolgt mithilfe von vCenter Single Sign-On.

Die administrative Oberfläche von Single Sign-On ist Teil von vSphere Web Client. Zur Konfiguration von Single Sign-On und zum Management von Single Sign-On-Anwendern melden Sie sich als Anwender mit Single Sign-On-Administratorberechtigungen bei vSphere Web Client an. Hierbei handelt es sich unter Umständen nicht um denselben Anwender wie den vCenter Server-Administrator. Geben Sie die Anmeldeinformationen auf der Anmeldeseite von vSphere Web Client ein. Nach der Authentifizierung können Sie auf das Single Sign-On-Administrationstool zugreifen und Anwender erstellen sowie administrative Berechtigungen an andere Anwender vergeben.

In älteren vSphere-Versionen als 5.1 erfolgte die Anwenderauthentifizierung durch eine Validierung der vCenter Server-Anmeldeinformationen mit einer Active Directory-Domäne oder Liste lokaler Betriebssystembenutzer. Seit vSphere 5.1 erfolgt die Anwenderauthentifizierung mittels vCenter Single Sign-On. Der standardmäßige Single Sign-On-Administrator für vSphere 5.1 ist „admin@System-Domain“ und ab vSphere 5.5 „administrator@vsphere.local“. Das Kennwort für dieses Konto haben Sie bei der Installation festgelegt. Wenn Sie sich mit diesen Anmeldeinformationen bei vSphere Web Client anmelden, erhalten Sie Zugriff auf das Single Sign-On-Administrationstool. Anschließend können Sie Single Sign-On-Administratorprivilegien an einzelne Anwender, die mit dem Management des Single Sign-On-Servers betraut sind, weitergeben. Diese Anwender können sich von den Anwendern, die als Administratoren für vCenter Server fungieren, unterscheiden.

HINWEIS: Die Anmeldung bei vSphere Web Client mit den Anmeldeinformationen der Windows-Sitzung wird nur für Active Directory-Anwender der Domäne, zu der das Single Sign-On-System gehört, unterstützt.

Single Sign-On-Identitätsquellen

In den meisten Fällen wird vSphere SSO so bereitgestellt, dass eine externe Identitätsquelle für die primäre Authentifizierung verwendet wird. In dieser Hands-on Lab-Umgebung wurde SSO in Microsoft Active Directory integriert, damit sich Anwender der Domäne „corp.local“ mithilfe ihrer AD-Anmeldeinformationen bei vSphere anmelden können.

In diesem Abschnitt werden die Identitätsquellen beschrieben, mit denen Single Sign-On konfiguriert werden kann.

Abmelden als Administrator@CORP.LOCAL

Wenn Sie aktuell bei vSphere Web Client angemeldet sind, klicken Sie auf **Administrator@CORP.LOCAL** und wählen Sie **Logout** aus.

Anmelden als SSO-Administrator bei vSphere Web Client

Melden Sie sich mit einem Konto, das über das SSO-Administratorprivileg verfügt, bei vSphere Web Client an:

1. Username: **administrator@vsphere.local**
2. Password: **VMware1!**
3. Klicken Sie auf „Login“.

Navigieren zu „Administration“

1. Klicken Sie auf das **Haussymbol**.
2. Wählen Sie **Administration** aus.

Identitätsquellen für vSphere Single Sign-On

Wenn die Maschine mit dem Platform Services Controller (PSC), der die Single Sign-On-Komponente ausführt, zu einer Active Directory-Domäne hinzugefügt wird, wird die Identitätsquelle dieser Domäne automatisch zu SSO hinzugefügt.

Anwendern, die sich in den hier aufgeführten Domänen befinden, können Berechtigungen innerhalb vSphere erteilt werden.

1. Klicken Sie auf **Configuration** im Navigatorabschnitt „Single Sign-On“.
2. Klicken Sie auf die Registerkarte **Identity Sources**.
3. Sie stellen fest, dass die Domäne **corp.local** als Active Directory-Identitätsquelle aufgeführt wird.

4. Außerdem wird die Domäne **vsphere.local** mit einem nicht spezifizierten Typ aufgeführt. Hierbei handelt es sich um die interne SSO-Domäne.

Hinzufügen eines vCenter Single Sign On-Anwenders mithilfe von vSphere Web Client

Anwender, die in vSphere Web Client auf der Registerkarte „Users“ aufgeführt werden, sind vCenter Single Sign-On-intern. Hierbei handelt es sich nicht um dieselben Anwender wie auf dem lokalen Betriebssystem der Maschine, auf der Single Sign-On installiert ist (z.B Windows). Wenn Sie einen Single Sign-On-Anwender mit dem Single Sign-On-Administrationstool hinzufügen, wird dieser Anwender in der Single Sign-On-Datenbank gespeichert, die auf dem System ausgeführt wird, auf dem Single Sign-On installiert ist. Diese Anwender sind Teil der SSO-Domäne, standardmäßig „vsphere.local“ oder „System-Domain“ bei vSphere 5.1. Mit einer Installation von Single Sign-On ist genau eine Systemidentitätsquelle verknüpft.

Auflisten der aktuellen Anwender und Hinzufügen eines neuen Anwenders

1. Klicken Sie unter „Single Sign-On“ auf **Users and Groups**.
2. Klicken Sie auf der Registerkarte „Users“ auf das Symbol **New User**.

Eingeben der Eigenschaften des neuen Anwenders

Geben Sie einen Anwendernamen und ein Kennwort für den neuen Anwender ein. Beachten Sie, dass das Kennwort die Kennwortrichtlinien des Systems erfüllen muss. Die Richtlinie kann angezeigt werden, indem Sie den Mauszeiger auf das i-Symbol rechts neben dem Kennwortfeld bewegen.

Geben Sie Vor- und Nachname und anschließend eine E-Mail-Adresse ein.

Klicken Sie auf **OK**, um den Anwender zu erstellen.

HINWEIS: Der Name des Anwenders kann nach der Erstellung des Anwenders nicht mehr geändert werden. Vor- und Nachname sind optional.

Bearbeiten eines vCenter Single Sign-On-Anwenders mithilfe von vSphere Web Client

1. Klicken Sie unter „Single Sign-On“ auf **Users and Groups**.

Bearbeiten des Anwenders

Klicken Sie mit der rechten Maustaste auf den Anwender **holadmin** und wählen Sie **Edit User** aus.

Bearbeiten der Anwendereigenschaften

Nehmen Sie Änderungen am Anwender vor. Das Kennwort muss die Kennwortrichtlinien des Systems erfüllen.

Klicken Sie auf **OK**, um etwaige Änderungen zu speichern. Falls Sie Änderungen vorgenommen haben, müssen Sie das aktuelle Kennwort (VMware1!) eingeben, bevor Sie auf „OK“ klicken können. Wenn Sie Ihre Änderungen verwerfen möchten, klicken Sie auf **Cancel**.

Hinzufügen einer vCenter Single Sign-On-Gruppe mithilfe von vSphere Web Client

Bei Gruppen, die in vSphere Web Client auf der Registerkarte „Groups“ aufgeführt werden, handelt es sich um interne vCenter Single Sign-On-Gruppen. Mit einer Gruppe können Sie einen Container für eine Reihe von Gruppenmitgliedern erstellen. Diese werden als Berechtigte bezeichnet. Wenn Sie eine Single Sign-On-Gruppe mit dem Single Sign-On-Administrationstool hinzufügen, wird die Gruppe in der Single Sign-On-Datenbank gespeichert. Die Datenbank wird auf dem System ausgeführt, auf dem Single Sign-On installiert ist. Diese Gruppen sind Teil der Identitätsquellendomäne „vsphere.local“ (der Standarddomäne für vSphere 5.5 und höher) oder „System-Domain“ für vSphere 5.1.

Gruppenmitglieder können Anwender oder andere Gruppen sein. Eine Gruppe kann aus Mitgliedern von unterschiedlichen Identitätsquellen bestehen. Nachdem Sie eine Gruppe erstellt und Berechtigte hinzugefügt haben, können Sie der Gruppe Berechtigungen erteilen. Mitglieder der Gruppe erben die Gruppenberechtigungen.

Auflisten der aktuellen Anwender

1. Klicken Sie unter „Single Sign-On“ auf „Users and Groups“.

Auflisten der Gruppen

1. Wählen Sie die Registerkarte **Groups** aus.
2. Klicken Sie auf das Symbol „Add Group“ (das grüne **+**).

Erstellen der neuen Gruppe

Geben Sie einen Namen und eine Beschreibung für die Gruppe ein. Der Name der Gruppe kann nach der Erstellung der Gruppe nicht mehr geändert werden.

Klicken Sie auf **OK**, um die Gruppe zu erstellen.

Hinzufügen von Mitgliedern zu einer vCenter Single Sign-On-Gruppe in vSphere Web Client

Die Mitglieder einer vCenter Single Sign-On-Gruppe können Anwender oder andere Gruppen aus einer oder mehreren Identitätsquellen sein. Mitglieder einer Gruppe werden als Prinzipale bezeichnet. Gruppen, die in vSphere Web Client auf der Registerkarte „Groups“ aufgeführt werden, sind Single Sign-On-intern und Teil der Identitätsquelle „System-Domain“. Sie können Gruppenmitglieder aus anderen Domänen zu einer lokalen Gruppe hinzufügen. Außerdem können Sie Gruppen schachteln.

Hinzufügen von Mitgliedern zu Anwendern und Gruppen

1. Klicken Sie unter „Single Sign-On“ auf „Users and Groups“.

Hinzufügen von Mitgliedern zu Anwendern und Gruppen

1. Klicken Sie auf die Registerkarte **Groups**.
2. Klicken Sie auf die Gruppe **HOL Group**.
3. Klicken Sie im Abschnitt „Group Members“ auf das Symbol **Add Member**.

Hinzufügen des Anwenders „holadmin“ zur Gruppe „HOL Group“

1. Vergewissern Sie sich, dass die Domäne **vsphere.local** ausgewählt ist.
2. Geben Sie **HOL** in das Suchfeld ein und drücken Sie die Eingabetaste.
3. Wählen Sie in den Anwender „holadmin“ in der Liste aus.
4. Klicken Sie auf die Schaltfläche „Add“.
5. Klicken Sie auf „OK“, um das Hinzufügen des Anwenders zur Gruppe abzuschließen.

Zuweisen von globalen Berechtigungen

Nach der Konfiguration von Identitätsquellen, Anwendern und Gruppen müssen ihnen Berechtigungen für die Nutzung von vSphere zugewiesen werden.

Auflisten von globalen Berechtigungen

1. Klicken Sie unter „Access Control“ auf den Menüeintrag **Global Permissions**.
2. Klicken Sie auf die Registerkarte **Manage**.

Per SSO können einem Konto globale Berechtigungen zugewiesen werden, indem Sie hier den notwendigen Zugriff festlegen. In diesem Hands-on Lab führt die Liste die erteilten Standardberechtigungen auf, mit Ausnahme des Anwenders **CORP.LOCAL\ Administrator**, der Administratorberechtigungen für die gesamte vSphere-Infrastruktur besitzt.

Hinzufügen einer neuen globalen Berechtigung

Die Mitglieder der Gruppe „HOL Group“ werden mit dem Management aller virtuellen Maschinen der Umgebung betraut, deshalb werden die Berechtigungen hier konfiguriert.

1. Klicken Sie auf das grüne (+), um das Fenster „Add New Permission“ zu öffnen.
2. Klicken Sie auf die Schaltfläche **Add...**.

Lokalisieren der Gruppe „HOL Group“

1. Vergewissern Sie sich, dass die Domäne **vsphere.local** ausgewählt ist.
2. Geben Sie **hol** in das Suchfeld ein und drücken Sie die Eingabetaste, um die Liste zu filtern.
3. Wählen Sie die Gruppe **HOL Group** aus.
4. Klicken Sie auf die Schaltfläche **Add**.
5. Klicken Sie auf die Schaltfläche **OK**.

Konfigurieren der Berechtigungen

Ein Anwender erhält Berechtigungen für ein Objekt, indem eine Rolle mit dem Anwender verknüpft wird. Dies wurde in der vorherigen Lektion *Rollen für Anwenderzugriff und Authentifizierung* beschrieben.

1. Wählen Sie die Rolle **Virtual machine power user (sample)** aus der Liste „Assigned Role“ aus.
2. Stellen Sie sicher, dass das Kontrollkästchen **Propagate to children** aktiviert ist.
3. Klicken Sie auf **OK**.

Überprüfen der Änderung

Beachten Sie, dass der Gruppe „HOL Group“ der Zugriff „Virtual machine Power user“ auf alle untergeordneten Objekte in der Infrastruktur gewährt wurde.

Wenn Sie dies ausführlicher testen möchten, melden Sie sich aus dem Webclient ab und melden Sie sich als Anwender **holadmin@vsphere.local** mit dem Kennwort, das Sie bei der Erstellung des Kontos angegeben haben, an. Beachten Sie, dass der Zugriff auf

die Infrastruktur auf das grundlegende Management von virtuellen Maschinen beschränkt ist.

REFERENZ – Entsperren von vCenter Single Sign-On-Anwendern in vSphere Web Client

Das Konto eines vCenter Single Sign-On-Anwenders kann gesperrt werden, wenn die erlaubte Anzahl fehlgeschlagener Anmeldeversuche überschritten wird. Nachdem ein Anwenderkonto gesperrt wurde, kann sich der Anwender nicht beim Single Sign-On-System anmelden, bis das Konto entweder manuell oder nach einem bestimmten Zeitintervall entsperrt wird.

Die Bedingungen, unter welchen ein Anwenderkonto gesperrt wird, legen Sie in der Single Sign-On-Sperrrichtlinie fest. Gesperrte Anwenderkonten werden auf der Administrationsseite „Users and Groups“ angezeigt. Anwender mit geeigneten Privilegien können die Konten von Single Sign-On-Anwendern manuell entsperren, bevor die festgelegte Zeit abgelaufen ist. Um einen Single Sign-On-Anwender zu entsperren, müssen Sie ein Mitglied der Single Sign-On-Administratorgruppe sein.

Gesperrter Anwender

Standardmäßig wird ein Anwenderkonto nach drei fehlgeschlagenen Anmeldeversuchen gesperrt.

In diesem Hands-on Lab wurde diese Richtlinie deaktiviert, um oftmals durch länderspezifische Tastaturen verursachte Anmeldeprobleme zu vermeiden.

Dieser Abschnitt dient lediglich als Referenz.

Entsperren eines Anwenders

Melden Sie sich als Anwender mit SSO-Administratorprivilegien bei vSphere Web Client an und navigieren Sie zur Liste „Users“.

1. Lokalisieren Sie das gesperrte Anwenderkonto: In der Spalte „Locked“ wird „Yes“ angezeigt.
2. Klicken Sie mit der rechten Maustaste auf den gesperrten Anwender und wählen Sie „Unlock“ aus.

Melden Sie sich vom Webclient ab.

Ändern des Kennworts in vSphere Web Client

Abhängig von Ihren vCenter Single Sign-On-Privilegien können Sie Ihr Single Sign-On-Anwenderprofil möglicherweise nicht anzeigen oder bearbeiten. Jedoch können alle

Anwender ihr Single Sign-On-Kennwort in vSphere Web Client ändern. Die im vCenter Single Sign-On-Konfigurationstool definierte Kennwortrichtlinie legt fest, wann ein Kennwort abläuft. **In vSphere 6 laufen Single Sign-On-Kennwörter standardmäßig nach 90 Tagen ab**. Diese Einstellung kann je nach Richtlinie Ihrer Organisation jedoch vom Systemadministrator geändert werden. Wenn Sie die Standardwerte verwenden, denken Sie daran, das Kennwort für das Konto „administrator@vsphere.local“ alle 90 Tage zu ändern, andernfalls wird es an Tag 91 gesperrt.

Ändern des Kennworts

Klicken Sie im oberen Navigationsfenster auf Ihren Anwendernamen, um das Menü zu öffnen.

Dialogfeld zum Ändern des Kennworts

Wählen Sie „Change Password“ aus und geben Sie Ihr aktuelles Kennwort ein.

Geben Sie ein neues Kennwort ein.

Geben Sie ein neues Kennwort ein und bestätigen Sie es.

Klicken Sie auf die Schaltfläche „OK“, um die Änderung vorzunehmen.

HINWEIS: Falls Sie das Kennwort ändern, müssen Sie das neue Kennwort für weitere Aktivitäten im Hands-on Lab verwenden.

Schlussbemerkung

Anwenderkonten werden üblicherweise nicht nativ in der SSO-Domäne verwaltet, sondern über eine externe Verzeichnisquelle wie Microsoft Active Directory oder OpenLDAP. Das Verständnis, wie Konten von SSO behandelt werden und wo Kontoberechtigungen vorgenommen werden, ist hilfreich für das Management einer vSphere-Implementierung.

Hinzufügen eines ESXi-Host zu Active Directory

In dieser Lektion wird das Hinzufügen eines ESXi-Hosts zu Active Directory beschrieben.

Konfigurieren eines Hosts zur Verwendung von Active Directory in vSphere Web Client

In dieser Lektion wird das Hinzufügen eines vSphere-Hosts zur Authentifizierung per Active Directory beschrieben.

Hosts und Cluster

Klicken Sie auf das **Haussymbol** und wählen Sie **Hosts and Clusters** aus.

esx-01a.corp.local

Klicken Sie auf **esx-01a.corp.local**.

TCP/IP-Konfiguration

Klicken Sie auf die Registerkarte **Konfiguration** und wählen Sie anschließend die Registerkarte **TCP/IP configuration** im Abschnitt „Networking“ aus.

Bearbeiten des System-Stacks „Default“

Klicken Sie auf **Default** unter „System stacks“ und klicken Sie auf die Schaltfläche **Edit**.

DNS-Konfiguration

Klicken Sie auf die Registerkarte **DNS configuration**.

Hier müssen Sie prüfen, ob der Hostname und die Informationen des DNS-Servers korrekt sind. Klicken Sie auf **OK**.

Hinzufügen eines Hosts zu einer Verzeichnisservice-Domäne in vSphere Web Client

Nachdem Sie die Netzwerkeinstellungen überprüft haben, können Sie einen Host zu Active Directory hinzufügen.

Klicken Sie auf **Authentication Services** im Abschnitt „System“. Möglicherweise müssen Sie nach unten scrollen.

Beitreten einer Domäne

Klicken Sie auf die Schaltfläche **Join Domain**.

Einstellungen zum Beitreten einer Domäne

Geben Sie „corp.local“ in das Feld „Domain“ ein.

Geben Sie im Abschnitt „Using Credentials“ Folgendes ein:

```
Username: administrator
Password: VMware1!
```

Klicken Sie auf „OK“.

Zu Active Directory hinzugefügt

Nach einigen Sekunden sollte der Bildschirm aktualisiert werden. Im Abschnitt „Authentication Services“ wird jetzt angezeigt, dass der Host mit der Active Directory-Domäne verbunden ist.

(Optional) Video: Hinzufügen von VMware vSphere-Hosts zu Active Directory (3:40)

In diesem Video wird das Hinzufügen eines VMware vSphere-Host zu einer Microsoft Active Directory(AD)-Domäne gezeigt, damit Administratoren ihre Active Directory-Anmeldeinformationen für den Zugriff auf und das Management von Hosts verwenden können.

Schlussbemerkung

Hiermit ist Modul 2 – Einführung in vSphere-Netzwerke und -Sicherheit – abgeschlossen. Wir hoffen, dass Ihnen das Hands-on Lab weitergeholfen hat. Wir freuen uns, wenn Sie am Ende an der Umfrage teilnehmen.

Falls Sie noch Zeit haben, finden Sie nachfolgend die weiteren Module dieses Hands-on Lab mit der geschätzten Dauer, um das jeweilige Modul abzuschließen. Klicken Sie auf die Schaltfläche „Inhalt“, um zum entsprechenden Modul in diesem Handbuch zu springen.

- Modul 1 – Einführung in das Management mit vCenter Server (60 Minuten)
- Modul 3 – Einführung in vSphere-Storage (60 Minuten)

Modul 3 – Einführung in vSphere-Storage (60 Minuten)

vSphere-Storage – Übersicht

Die folgende Lektion bietet eine Übersicht über die unterschiedlichen Storage-Typen, die in vSphere zur Verfügung stehen.

Der vSphere Hypervisor, ESXi, bietet Storage-Virtualisierung auf Hostebene, um den physischen Storage-Layer logisch von den virtuellen Maschinen zu abstrahieren.

In vSphere nutzt eine virtuelle Maschine zur Speicherung des Betriebssystems, der Programmdateien und anderer Daten, die mit ihrer Aktivität verbunden sind, eine virtuelle Festplatte. Bei einer virtuellen Festplatte handelt es sich um eine große physische Datei oder eine Reihe von Dateien, die wie jede andere Datei kopiert, verschoben, archiviert und gesichert werden kann. Virtuelle Maschinen können mit mehreren virtuellen Festplatten konfiguriert werden.

Für den Zugriff auf virtuelle Festplatten nutzt eine virtuelle Maschine SCSI-Controller. Zu diesen virtuellen Controllern zählen BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS und VMware Paravirtual. Diese Controller sind die einzigen Typen von SCSI-Controller, die für eine virtuelle Maschine sichtbar und zugänglich sind.

Eine virtuelle Festplatte befindet sich auf einem vSphere Virtual Machine File System (VMFS-)Datastore oder auf einem NFS-basierten Datastore, der auf physischem Storage bereitgestellt wurde. Aus Sicht der virtuellen Maschine wird jede virtuelle Festplatte als SCSI-Laufwerk, das an einen SCSI-Controller angeschlossen ist, angezeigt. Unabhängig davon, ob das eigentliche physische Storage-Gerät über parallele SCSI-, iSCSI-, Netzwerk-, Fibre Channel oder FCoE-Adapter auf dem Host angesprochen wird, ist es für das Gastbetriebssystem und die auf der virtuellen Maschine ausgeführten Anwendungen transparent.

Der Prozess des Storage-Managements in vSphere beginnt mit dem Speicherplatz, den Ihr Storage-Administrator vor der vSphere ESXi-Zuweisung auf unterschiedlichen Storage-Systemen freigibt. vSphere unterstützt zwei Storage-Typen: lokal und netzwerkbasiert. Die beiden Typen werden nachfolgend ausführlicher erläutert.

Lokaler Storage

Die Abbildung zeigt virtuelle Maschinen, die einen direkt mit einem einzigen ESXi-Host verbundenen lokalen VMFS-Storage nutzen.

Bei dem lokalen Storage kann es sich um interne Festplatten des ESXi-Hosts oder externe Storage-Systeme, die direkt über Protokolle wie SAS oder SATA mit dem Host verbunden sind, handeln.

Netzwerkbasierter Storage

Die Abbildung zeigt virtuelle Maschinen, die einen netzwerkbasierten VMFS-Storage nutzen, der mehreren ESXi-Hosts zur Verfügung gestellt wird.

Der netzwerkbasierte Storage besteht aus externen Storage-Systemen, die vom ESXi-Host für die Remote-Speicherung von virtuellen Maschinen verwendet werden. Üblicherweise greift der Host über ein Hochgeschwindigkeits-Storage-Netzwerk auf diese Systeme zu. Netzwerkbasierte Storage-Geräte werden üblicherweise von mehreren Objekten genutzt. Mehrere Hosts können gleichzeitig auf Datastores auf netzwerkbasierten Storage-Geräten zugreifen. Auf diese Weise werden weitere vSphere-Technologien möglich wie Hochverfügbarkeit durch Host-Clustering, Distributed Resource Scheduling, vMotion und virtuelle Maschinen mit Fehlertoleranz. ESXi unterstützt verschiedene netzwerkbasierte Storage-Technologien: Fiber Channel, iSCSI, NFS und Shared SAS.

Festplatten virtueller Maschinen

Die Abbildung oben zeigt virtuelle Maschinen, die unterschiedliche Typen von virtuellen Festplattenformaten auf einem gemeinsamen VMFS-Datastore nutzen.

Wenn Sie bestimmte Managementoperationen für virtuelle Maschinen durchführen, wie das Erstellen einer virtuellen Festplatte, das Klonen einer virtuellen Maschine in eine Vorlage oder das Migrieren einer virtuellen Maschine, können Sie eine Provisioning-Richtlinie für das Format der virtuellen Festplattendatei festlegen. Es gibt drei Typen von virtuellen Festplattenformaten:

Thin Provision

Nutzen Sie dieses Format, um Speicherplatz zu sparen. Bei Thin-Festplatten wird so viel Speicherplatz im Datastore bereitgestellt, wie die Festplatte auf Basis der von Ihnen angegebenen Größe benötigt. Allerdings nutzen Thin-Festplatten zunächst nur so viel Speicherplatz auf dem Datastore, wie sie für den erstmaligen Betrieb benötigen.

Thick Provision (Lazy Zeroed)

Hierbei wird eine virtuelle Festplatte in einem standardmäßigen Thick-Format erstellt. Der für die virtuelle Festplatte erforderliche Speicherplatz wird bei der Erstellung zugewiesen. Auf dem physischen Gerät verbliebene Daten werden beim Erstellen nicht gelöscht, sondern die Festplatte wird zu einem späteren Zeitpunkt während der ersten Schreibvorgänge der virtuellen Maschine mit Nullen beschrieben.

Wenn Sie Thick Provision (Lazy Zeroed) verwenden, verlieren Sie nicht die Möglichkeit, gelöschte Dateien oder alte Daten, die sich möglicherweise auf dem zugewiesenen Speicherplatz befinden, wiederherzustellen, da der Speicherplatz nicht genullt wird. Eine Festplatte, die mit Thick Provision (Lazy Zeroed) bereitgestellt wurde, kann nicht in eine Thin-Festplatte umgewandelt werden.

Thick-Provision (Eager Zeroed)

Hierbei handelt es sich um einen Typ einer virtuellen Thick-Festplatte, die Clustering-Funktionen wie Fehlertoleranz unterstützt. Der für die virtuelle Festplatte benötigte Speicherplatz wird bei der Erstellung zugewiesen. Im Gegensatz zum Thick Provision (Lazy Zeroed)-Format werden die Daten, die auf dem physischen Gerät verbleiben, beim Erstellen der virtuellen Festplatte mit Nullen überschrieben. Im Allgemeinen dauert die Erstellung von Festplatten in diesem Format wesentlich länger als die Erstellung anderer Festplattentypen.

Weitere Hands-on Labs zu vSphere Storage

In diesem Modul sind mehrere Lektionen enthalten, die das Konfigurieren und Verwenden von vSphere-Storage-Elementen beschreiben. Fahren Sie mit einem der folgenden Hands-on Labs fort, wenn Sie weitere Informationen erhalten und Praxiserfahrung sammeln möchten:

- Erstellen und Konfigurieren von vSphere-Datastores
- Management von VM-Festplatten
- Arbeiten mit VM-Snapshots
- Klonen von virtuellen Maschinen und Verwenden von Vorlagen
- vSphere Replication – Übersicht

Erstellen und Konfigurieren von vSphere-Datastores

In diesem Hands-on Lab wird die Erstellung und Konfiguration eines NFS- und eines iSCSI-vSphere-Datastores beschrieben. Darüber hinaus wird das Hinzufügen und Konfigurieren eines iSCSI-Softwareadapters beschrieben.

Anmelden bei vSphere Web Client

In diesem Schritt wird das Anmelden bei vSphere Web Client beschrieben.

Öffnen des Google Chrome-Webbrowsers

1. Wählen Sie **Google Chrome** auf dem Desktop der Hauptkonsole aus.

Eingeben der Anmeldeinformationen und Anmeldung

Hinweis: Wenn Sie „Use Windows session authentication“ auswählen, werden dieselben Anmeldeinformationen wie bei der Anmeldung mit dem Anwendernamen „CORP\Administrator“ und dem Kennwort „VMware1!“ weitergegeben.

1. Wählen Sie „Use Windows session authentication“ aus.

2. Wählen Sie „Login“ aus.

Navigieren zum Fenster für das Storage-Management

1. Wählen Sie die Registerkarte **Storage** aus.

Erweitern von „Datacenter Site A“

Aktuell wurden zwei Storage-Datastores konfiguriert: ein iSCSI-Datastore und ein NFS-Datastore.

1. Wählen Sie den Datastore **ds-iscsi01** aus.

2. Klicken Sie auf **Summary**, um eine Detailansicht des Datastores anzuzeigen.

Wiederholen Sie die Schritte für den Datastore **ds-site-a-nfs01**.

Erstellen eines vSphere-NFS-Datastores

In diesem Abschnitt erstellen Sie einen neuen vSphere-NFS-Datastore mithilfe eines bereits bereitgestellten NFS-Mounts.

Erstellen eines vSphere-NFS-Datastores

In diesem Abschnitt erstellen Sie einen neuen vSphere-NFS-Datastore mithilfe eines bereits bereitgestellten NFS-Mounts.

1. Wählen Sie **Datacenter Site A** aus.
2. Wählen Sie **Actions** aus.
3. Wählen Sie **Storage** aus.
4. Wählen Sie **New Datastore** aus.

Neuer Datastore: Typ

Klicken Sie auf die Schaltfläche **Next**, um im Assistenten mit dem nächsten Schritt **Type** fortzufahren.

5. Vergewissern Sie sich, dass „NFS“ ausgewählt ist, und klicken Sie auf **Next**.

Neuer Datastore: NFS-Version

5. Vergewissern Sie sich, dass NFS-Version **NFS 3** ausgewählt ist, und klicken Sie auf **Next**.

Neuer Datastore: Name und Konfiguration

7. Geben Sie den Namen **ds-site-a-nfs02** für den neuen Datastore ein.

8. Geben Sie **/mnt/NFS02** im Feld „Folder“ im Bereich „NFS Share Details“ ein.

9. Geben Sie **10.10.20.60** im Feld „Server“ im Bereich „NFS Share Details“ ein und klicken Sie auf „Next“.

Neuer Datastore: Hostzugriff

10. Aktivieren Sie das **Kontrollkästchen**, um alle Hosts auszuwählen, und klicken Sie auf **Next**.

Neuer Datastore: Abschließen des Vorgangs

12. Überprüfen Sie die Konfiguration des neuen Datastore und klicken Sie auf **Finish**.

Überwachen des Aufgabenfortschritts

13. Sie können den Fortschritt im Fenster „Recent Tasks“ beobachten.

14. Klicken Sie auf das Aktualisierungssymbol, um den Bildschirm zu aktualisieren.

Nach Abschluss des Vorgangs kann der neue Datastore **ds-site-a-nfs02** genutzt werden.

Überprüfen der Einstellungen des neuen Datastores

1. Wählen Sie den Datastore **ds-site-a-nfs02** in der Bestandsliste aus.
2. Wählen Sie **Summary** aus, um die Kapazitäts- und Konfigurationsdetails anzuzeigen.

Erstellen eines vSphere-iSCSI-Datastores

In diesem Abschnitt erstellen Sie einen neuen vSphere-iSCSI-Datastore mithilfe einer bereits bereitgestellten iSCSI-LUN.

1. Wählen Sie **Datacenter Site A** aus.
2. Wählen Sie **Actions** aus.
3. Wählen Sie **Storage** aus.
4. Wählen Sie **New Datastore** aus.

Neuer Datastore: Typ

Klicken Sie auf „Next“, um auf die Seite „Type“ des Assistenten zu gelangen.

5. Vergewissern Sie sich, dass „VMFS“ ausgewählt ist, und klicken Sie auf „Next“.

Neuer Datastore: Name und Konfiguration

6. Geben Sie den Namen **ds-iscsi02** für den neuen Datastore ein.

7. Wählen Sie einen Host aus, um die zugänglichen Festplatten/LUNs anzuzeigen, und wählen Sie **esx-01a.corp.local** im Dropdown-Menü aus.

Neuer Datastore: Name und Gerätekonfiguration

Hier sehen Sie die vorhandenen Datastores, die der vSphere-Umgebung zur Verfügung gestellt werden können.

8. Wählen Sie das Gerät mit **LUN-ID 12** aus. In diesem Fall sollte es das einzige sichtbare Gerät mit dem Präfix „FreeBSD“ sein.

Klicken Sie auf **Next**.

Neuer Datastore: VMFS-Version

Behalten Sie die Standardeinstellung **VMFS 5** bei und klicken Sie auf **Next**.

Neuer Datastore: Konfiguration der Partition

Sie können entweder die gesamte verfügbare Kapazität für diesen Datastore verwenden oder die Größe bei Bedarf ändern. Es genügt, die Standardeinstellungen auszuwählen.

Wählen Sie **Next** aus.

Neuer Datastore: Abschließen des Vorgangs

12. Überprüfen Sie die Konfiguration des neuen Datastores und klicken Sie auf „Finish“.

Neuer Datastore: Überwachen des Aufgabenfortschritts

13. Beobachten Sie den Fortschritt im Fenster „Recent Tasks“.

14. Nach Abschluss des Vorgangs kann der Datastore **ds-iscsi02** genutzt werden.

Neuer Datastore: Überprüfen der Einstellungen

1. Wählen Sie den Datastore **ds-iscsi02** in der Bestandsliste aus.
2. Wählen Sie **Summary** aus, um die Kapazitäts- und Konfigurationsdetails anzuzeigen.

Hinzufügen eines neuen ESXi-Hosts

In diesem Abschnitt fügen Sie einen neuen ESXi-Host, **esx-03a.corp.local**, zu der Umgebung an Standort A hinzu und stellen sicher, dass für diesen der geeignete Storage konfiguriert wurde, damit dieser zu einem produktiven Mitglied des Clusters werden kann.

Ansicht „Hosts and Clusters“

1. Klicken Sie auf das Symbol **Hosts and Clusters**, um zur Bestandslistenansicht zurückzukehren.
2. Wählen Sie **Cluster Site A** aus.
3. Klicken Sie auf **Summary**, um die aktuelle Konfiguration des Clusters anzuzeigen.

Wie Sie sehen, befinden sich zwei Hosts im Cluster und DRS ist im Modus „Partially Automated“ aktiviert. Wenn Sie Modul 1 – Einführung in das Management mit vCenter Server – abgeschlossen haben, befindet sich DRS möglicherweise im Modus „Fully Automated“ und der Cluster weist möglicherweise den Status „Imbalanced“ auf.

Start des Workflows zum Hinzufügen eines Hosts

1. Klicken Sie in der Bestandsliste auf **Cluster Site A**, um diesen auszuwählen.
2. Gehen Sie zum Menü **Actions**.
3. Wählen Sie **Add Host...** aus.

Eingeben des Hostnamens

4. Geben Sie den Namen des hinzuzufügenden Hosts ein: **esx-03a.corp.local**.
5. Klicken Sie auf „Next“.

Eingeben der Anmeldeinformationen

6. Geben Sie **root** als „Username“ ein.
7. Geben Sie **VMware1!** als „Password“ ein.
8. Klicken Sie auf „Next“.

Hostzusammenfassung

Da es sich um einen neuen Host handelt, ist die Bestandsliste leer.

10. Klicken Sie auf **Next**.

Zuweisen der HOL-Lizenz zum Host

11. Klicken Sie auf das Optionsfeld neben **FOR VMWARE...**.
12. Stellen Sie sicher, dass die Lizenz validiert wird.
13. Klicken Sie auf **Next**.

Konfigurieren des Sperrmodus

14. Behalten Sie die Standardeinstellung **Disabled** für den Sperrmodus bei und klicken Sie auf **Next**.

Anbinden eines Ressourcenpools

15. Da es sich um einen neuen Host mit leerer Bestandsliste handelt, behalten Sie die Standardeinstellungen bei und klicken auf **Next**.

Abschließen des Workflows zum Hinzufügen eines Hosts

16. Klicken Sie auf **Finish**, um den Host in vCenter zu importieren.

Überwachen des Fortschritts

Der Fortschritt der Aufgabe zum Hinzufügen eines Host kann im Fenster „Recent Tasks“ beobachtet werden.

Nach Abschluss wird der Host **esx-03a.corp.local** im Wartungsmodus in der Bestandsliste angezeigt. Dies ist beabsichtigt, da dem Host noch kein Storage zum Hosten von virtuellen Maschinen zur Verfügung gestellt wurde.

Mounten von NFS-Datastores auf dem neuen Host

Der Host **esx-03a.corp.local** wurde zwar importiert, besitzt jedoch noch keine Storage-Konfiguration. Wenn Sie in der Bestandsliste auf den Hostnamen klicken, wird die entsprechende Warnung angezeigt.

In diesem Abschnitt wird NFS-Storage zum neuen Host hinzugefügt.

Assistent zum Mounten eines NFS-Datastores auf dem neuen Host

In diesem Fall werden zwei NFS-Datastores vom Cluster „Cluster Site A“ verwendet. Das Hinzufügen eines vorhandenen NFS-Datastores zu einem neuen Host ist ein einfacher Prozess.

1. Klicken Sie auf das **Datastore-Symbol**, um zur Datastore-Ansicht zu wechseln.
2. Wählen Sie den Datastore **ds-site-a-nfs01** in der Bestandsliste aus.
3. Klicken Sie auf das Menü **Actions**.
4. Wählen Sie **Mount Datastore to Additional Hosts...** aus.

Mounten eines NFS-Datastores: Auswählen des Hosts

5. Aktivieren Sie das **Kontrollkästchen**, um alle Hosts in der Liste auszuwählen.

6. Klicken Sie auf **OK**.

Mounten eines NFS Datastores: Überwachen der Aufgabe

Der Fortschritt der Aufgabe zum Mounten kann im Fenster „Recent Tasks“ beobachtet werden.

Nachdem das Mounten abgeschlossen wurde, können Sie den Vorgang prüfen, indem Sie auf die Registerkarte **Hosts** klicken.

Hier werden alle Hosts in der Bestandsliste angezeigt, auf denen dieser Datastore gemountet wurde.

Als Übung können Sie die Schritte wiederholen, um den anderen NFS-Datastore **ds-site-a-nfs02** zum Host **esx-03a.corp.local** hinzuzufügen.

Hinzufügen eines iSCSI-Ziels zu einem ESXi-Host

iSCSI-Geräte werden als iSCSI-Ziel dargestellt. Sie können sich dies als Host für die iSCSI-Geräte vorstellen. Der ESXi-Host muss wissen, wo er nach den Geräten suchen muss. Deshalb wird in diesem Abschnitt beschrieben, wie Sie den ESXi-Host auf das iSCSI Ziel verweisen und wie die Erkennung der verfügbaren LUNs erfolgt.

Auswählen von „Hosts and Clusters“

Klicken Sie auf das Symbol **Hosts and Clusters** und klicken Sie auf **esx-03a.corp.local.**.

Klicken Sie anschließend auf die Registerkarte **Configure** .

Durchführen der dynamischen Erkennung

1. Wählen Sie **Storage Adapters** aus.
2. Wählen Sie den Adapter **vmhba65** im Abschnitt **iSCSI Software Adapters** aus (Sie müssen in der Liste möglicherweise nach unten scrollen).
3. Klicken Sie auf **Targets**.
4. Klicken Sie auf **Dynamic Discovery**. Wie Sie sehen, ist die Liste der iSCSI-Server aktuell leer.
5. Klicken Sie auf **Add**.

Hinzufügen eines Zielservers

6. Geben Sie die im Feld „iSCSI Server“ die Adresse **10.10.20.60** ein und wählen Sie „OK“ aus.

(Erneutes) Scannen des iSCSI-Storage-Adapters

Nachdem das neue Ziel hinzugefügt wurde, wird eine gelbe Nachricht angezeigt, die Sie darauf hinweist, mit dem Adapter eine Anfrage an das iSCSI-Ziel zu senden.

7. Klicken Sie auf den iSCSi-Adapter **vmhba65**, um diesen auszuwählen.
8. Klicken Sie auf das **Symbol zum erneuten Scannen des Adapters**.

Überprüfen der Sichtbarkeit von iSCSI-Geräten

9. Klicken Sie auf „Storage Devices“, nachdem der erneute Scan abgeschlossen wurde.
10. Jetzt sollten zwei verbundene iSCSI-Festplatten mit jeweils 45 GB Kapazität angezeigt werden.

Überprüfen der Verfügbarkeit des iSCSI-Datastores

11. Klicken Sie auf die Registerkarte **Datastores**.

Sie sehen, dass die beiden iSCSI-Datastores jetzt für den Host **esx-03a.corp.local** sichtbar sind.

(Optional) Scannen nach neuen Datastores

Der ESXi-Host aktualisiert regelmäßig seine Sicht auf den Storage und mountet gefundene VMFS-Datastores. Wenn Sie nicht auf einen Aktualisierungszyklus warten können, können Sie einen erneuten Scan der Umgebung manuell auslösen und so nach neuen Geräten und VMFS-Datastores suchen.

Scannen nach neuen Datastores

1. Klicken Sie auf die Registerkarte **Configure**

2. Wählen Sie dann **Storage Devices** unter „Storage“ aus.

3. Wählen Sie die Schaltfläche **Rescan** aus.

Bestätigen der Optionen für das erneute Scannen

Überprüfen Sie die Optionen zum erneuten Scannen des Storage und klicken Sie auf **OK**.

Abgeschlossener Scan

Der Fortschritt der Aufgabe zum erneuten Scannen kann im Fenster „Recent Tasks“ beobachtet werden. Nach dem erneuten Scannen sollten alle verfügbaren Geräte und VMFS-Datastores gemountet worden sein. Dies kann überprüft werden, indem Sie an die entsprechenden Stellen navigieren: das Fenster „Storage Devices“ für unformatierte Geräte und der Bereich „Related Objects > Datastores“ für VMFS-Datastores.

Aktivieren des neuen Hosts

Bis jetzt befand sich der Host **esx-03a.corp.local** im Wartungsmodus, da noch keine Datastores zugewiesen wurden. Jetzt, da die Datastores aller Cluster von „Cluster Site A“ für den Host sichtbar sind, kann der Host aktiviert werden.

Verlassen des Wartungsmodus

Es gibt verschiedene Wege, um den Wartungsmodus zu verlassen. Es ist hilfreich, diesen Prozess zu kennen, da mit ihm mehrere Hosts gleichzeitig aus dem Wartungsmodus geholt (oder in den Wartungsmodus versetzt) werden können.

1. Wählen Sie den Cluster **Cluster Site A** aus.
2. Klicken Sie auf **Hosts**.

3. Wählen Sie den Host **esx-03a.corp.local** in der Liste „Hosts“ aus.
4. Klicken Sie auf das **Symbol zum Verlassen des Wartungsmodus**.

Einsatzbereit

Nach ein bis zwei Minuten verlässt der Host den Wartungsmodus. Wenn Sie vSphere HA auf dem Cluster aktiviert haben, wird der HA-Agent konfiguriert und gestartet, bevor der Host den Status „Normal“ aufweist. Dieser Prozess wird relativ schnell abgeschlossen, daher ist es möglicherweise erforderlich, den Webclient zu aktualisieren, damit der aktuelle Status angezeigt wird.

Beachten Sie, dass die grundlegenden Netzwerkfunktionen für virtuelle Maschinen, vMotion und IP-Storage für dieses Hands-on Lab bereits im Voraus konfiguriert wurden. Das Hinzufügen des neuen Hosts zum verteilten Switch **vds-site-a** erfolgt üblicherweise, bevor der Host aus dem Wartungsmodus geholt wird. Dies ist für diese Übung jedoch nicht notwendig. Als Übung können Sie diesen Switch gerne zum VDS migrieren.

Dieser Host kann jetzt Workloads für den Cluster übernehmen.

Storage vMotion

Über 80% der Ausfallzeiten in Rechenzentren sind in der Regel auf geplante Ausfallzeiten zurückzuführen. Hardwarewartung, Server-Migration und Firmware-Updates erfordern die Außerbetriebnahme physischer Server. Zur Minimierung der Auswirkungen dieser Ausfälle sind Unternehmen gezwungen, Wartungen auf unpraktische und schwer einzuplanende Ausfallfenster zu verschieben.

Dank der Funktionen vMotion® und Storage vMotion in vSphere können Unternehmen geplante Ausfallzeiten reduzieren, da Workloads in einer VMware-Umgebung dynamisch ohne Serviceunterbrechung auf andere physische Server oder einen anderen zugrunde liegenden Storage verschoben werden können. Administratoren können Wartungsoperationen schneller und vollständig transparent durchführen, ohne unpraktische Wartungsfenster einplanen zu müssen. vSphere vMotion und Storage vMotion bieten Unternehmen folgende Vorteile:

■ Vermeidung von Ausfallzeiten bei gängigen Wartungsoperationen

■ Vermeidung geplanter Wartungsfenster

■ Durchführen von Wartungsarbeiten jederzeit ohne Unterbrechung für Anwender und Services

In dieser Lektion wird beschrieben, wie Sie virtuelle Maschinen mit vMotion auf andere Hosts innerhalb des Clusters verschieben.

Navigieren zu „Virtual Machines and Templates“

Vor Storage vMotion müssen Sie überprüfen, dass keine Ausfallzeit für die virtuelle Maschine entsteht, indem Sie sie dauerhaft anpingen. Zum Anpingen benötigen Sie die IP-Adresse der virtuellen Maschine „TinyLinux-01“.

1. Klicken Sie auf die Registerkarte **VMs and Templates**.
2. Wählen Sie **TinyLinux-01** aus.
3. Stellen Sie sicher, dass Sie sich auf der Registerkarte **Summary** befinden.
4. Notieren Sie die IP-Adresse von TinyLinux-01: **192.168.120.51**.

Öffnen einer Befehlsaufforderung

Klicken Sie in der Windows-Taskleiste auf das Symbol zum Öffnen einer Eingabeaufforderung.

Anpingen von TinyLinux-01

Geben Sie folgenden Befehl in die Eingabeaufforderung ein und drücken Sie die Eingabetaste:

```
ping -t 192.168.120.51
```

Ping-Ergebnis

Sie sollten jetzt sehen, dass TinyLinux-01 kontinuierlich angepingt wird.

Storage-Ansicht

1. Navigieren Sie zum Startbildschirm von vSphere Web Client, indem Sie auf das **Haussymbol** klicken.
2. Klicken Sie auf **Storage**.

Auflisten der virtuellen Maschinen in einem bestimmten Datastore

1. Navigieren Sie zum Datastore-Objekt **ds-iscsi01** im Rechenzentrum **Datacenter Site A**, das von vCenter **vcsa-01a.corp.local** verwaltet wird, und klicken Sie darauf.
2. Klicken Sie auf **VMs**.
3. Klicken Sie auf die Registerkarte **Virtual Machines**. Es wird eine Liste aller virtuellen Maschinen auf dem ausgewählten Datastore angezeigt.

Hinweis: Abhängig davon, welche Lektion Sie bereits abgeschlossen haben, weichen die verfügbaren Datastores und virtuellen Maschinen möglicherweise von denen in den Abbildungen ab.

Storage vMotion per Drag-and-Drop

Die VM **TinyLinux-01** befindet sich ursprünglich auf **ds-iscsi01** und muss auf **ds-site-a-nfs01** verschoben werden.

1. Klicken Sie auf die VM **TinyLinux-01** und halten Sie die linke Maustaste gedrückt, während Sie die VM auf das Datastore-Objekt **ds-site-a-nfs01** ziehen. Neben dem Mauszeiger wird ein grünes + angezeigt, wenn der Mauszeiger auf Objekte zeigt, die ein geeignetes Ziel für das zu verschiebende Objekt darstellen. Lassen Sie die Maustaste los, um die VM **TinyLinux-01** im Objekt **ds-site-a-nfs01** abzulegen. Zum Abschließen des Vorgangs öffnet sich der Migrationsassistent.

Migrieren des Datastores

1. Wählen Sie das Optionsfeld **Change storage only** aus. Beachten Sie, dass in vSphere 6.5 die Möglichkeit besteht, Computing, Netzwerk und Storage in einer einzigen vMotion-Operation zu ändern.
2. Klicken Sie auf **Next**.

Storage-Richtlinie

1. Beachten Sie, dass der Datastore **ds-site-a-nfs01** bereits ausgewählt ist, da die VM vor dem Starten des Assistenten dort abgelegt wurde.

2. Klicken Sie auf **Next**, um die Einstellungen für die Storage-Verschiebung zu akzeptieren.

Abschließen des Vorgangs

Überprüfen Sie Ihre Auswahl auf dem Bildschirm „Ready to complete“ und klicken Sie auf **Finish**, um die Verschiebung zu starten.

Sie können die Operation im Fenster „Recent Tasks“ beobachten oder mit dem nächsten Schritt fortfahren.

Überprüfen eines Paketverlusts

Kehren Sie zur Eingabeaufforderung zurück und prüfen Sie das Ping-Ergebnis. Sie können die Bildlaufleiste benutzen, um zu überprüfen, ob ein Paketverlust vorlag.

In einigen Fällen steigt die Antwortzeit möglicherweise auf 2 ms an, jedoch sollte kein Paketverlust vorliegen.

Beenden des Pings

Klicken Sie auf das **X**, um den Ping zu beenden und das Befehlsfenster zu schließen.

Überprüfen von Storage vMotion

Der Fortschritt von Storage vMotion kann im Fenster „Recent Tasks“ beobachtet werden.

1. Klicken Sie nach Abschluss des Vorgangs auf den Datastore **ds-site-a-nfs01**. Dort wird die virtuelle Maschine **TinyLinux-01** jetzt unter „Related Objects“ aufgelistet.

Der Storage der virtuellen Maschine wurde von iSCSI auf NFS-Storage migriert, ohne dass die virtuelle Maschine offline genommen werden musste.

Management von VM-Festplatten

Bei der Arbeit mit virtuellen Maschinen können Sie eine virtuelle Festplatte erstellen oder eine bestehende virtuelle Festplatte verwenden. Eine virtuelle Festplatte besteht aus einer oder mehreren Dateien auf dem Dateisystem, die für das Gastbetriebssystem als einzelne Festplatte sichtbar sind. Diese Festplatten können zwischen verschiedenen Hosts verschoben werden.

Das Hinzufügen einer virtuellen Festplatte erfolgt während der Erstellung einer virtuellen Maschine mit dem Assistenten zum Erstellen virtueller Maschinen. In dieser Lektion arbeiten Sie jedoch mit einer bereits bestehenden virtuellen Maschine aus der Bestandsliste.

In dieser Lektion wird das Hinzufügen einer neuen virtuellen Festplatte zu einer bestehenden virtuellen Maschine beschrieben. Darüber hinaus werden Sie die ursprüngliche Festplattenkapazität der virtuellen Maschine erweitern.

Navigieren zum Managementfenster „VMs and Templates“

1. Wählen Sie das **Haussymbol** in der Titelleiste aus.

2. Wählen Sie **VMs and Templates** aus.

Hier sehen Sie, dass mehrere virtuelle Maschinen in der vSphere-Umgebung vorhanden sind. Im nächsten Schritt fügen Sie der virtuellen Maschine ***w12-core*** eine neue virtuelle Festplatte hinzu.

Erstellen einer neuen virtuellen Festplatte

In diesem Schritt erstellen Sie eine neue virtuelle Festplattenressource für eine bereits vorhandene virtuelle Maschine.

Überprüfen des Storage von „w12-core“

1. Wählen Sie die virtuelle Maschine **w12-core** aus und klicken Sie auf die Registerkarte **Summary**.
2. Falls „w12-core“ nicht eingeschaltet ist, klicken Sie auf den **Einschaltknopf**.
3. Im Fenster „VM Hardware“ wird die ursprüngliche Festplattenkonfiguration angezeigt: eine Festplatte mit einer Kapazität von 24 GB.

Bearbeiten der VM-Einstellungen

1. Klicken Sie mit der rechten Maustaste auf **w12-core**.

2. Wählen Sie **Edit Settings** aus.

Auswählen der hinzuzufügenden neuen Festplatte

1. Wählen Sie das Pop-up-Menü **New Device** aus.

2. Klicken Sie auf **New Hard Disk**.

3. Klicken Sie auf **Add**, um den Vorgang abzuschließen.

Konfigurieren der Größen- und Provisioning-Einstellungen

1. Reduzieren Sie die Größe auf **5** GB.

2. Klicken Sie auf **OK**, um die neue virtuelle Festplatte zu erstellen.

Überwachen des Aufgabenfortschritts

Beobachten Sie den Fortschritt im Fenster „Recent Tasks“.

1. Nach Abschluss der Operation sollte „Hard disk 2“ mit einer Kapazität von 5 GB für die VM „w12-core“ verfügbar sein.

Erweitern einer bereits bestehenden virtuellen Festplatte

In diesem Abschnitt erweitern Sie eine bereits bestehende virtuelle Festplatte einer virtuellen Maschine.

1. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine **w12-core**.
2. Wählen Sie **Edit Settings** aus.

Einstellungen von „Hard disk 1“

1. Die Kapazität von „Hard disk 1“ wird im Einstellungsassistenten mit 24 GB angegeben.

Erweitern von „Hard disk 1“

1. Klicken Sie auf den Pfeil nach oben, um die Kapazität von „Hard disk 1“ auf **32** GB zu vergrößern.

2. Klicken Sie auf **OK**.

Überwachen des Aufgabenfortschritts

1. Beobachten Sie den Fortschritt im Fenster **Recent Tasks**.

1. Nach Abschluss der Operation sollte „Hard disk 1“ mit einer Kapazität von 32 GB für die VM „w12-core“ verfügbar sein.

Überprüfen der Konfiguration der virtuellen Festplatte

1. Wählen Sie **w12-core** in der Bestandsliste aus.
2. Beachten Sie die konfigurierten virtuellen Festplatten und zugehörige Kapazität.
3. Sie stellen fest, dass der Storage-Gesamtverbrauch der virtuellen Festplatten aufgrund von Thin Provisioning nur etwa die Hälfte der 32 GB beträgt. Wenn Sie Modul 1 abgeschlossen haben, beträgt die Storage-Auslastung 16,14 GB.

Arbeiten mit VM-Snapshots

Snapshots erfassen den Status und die Daten einer virtuellen Maschine zu dem Zeitpunkt, an dem Sie ihn erstellen. Snapshots sind hilfreich, wenn Sie wiederholt denselben VM-Zustand wiederherstellen müssen, aber nicht mehrere virtuelle Maschinen erstellen möchten. Sie können außerdem mehrere Snapshots einer virtuellen Maschine erstellen, um mehrere Wiederherstellungspunkte in einem linearen Prozess zu erstellen. Mit mehreren Snapshots können Sie viele Schritte für die verschiedensten Arbeitsprozesse speichern. Der Snapshot Manager in vSphere Web Client bietet mehrere Operationen für die Erstellung und das Management von VM-Snapshots und Snapshot-Baumstrukturen. Mit diesen Operationen können Sie Snapshots erstellen, jeden Snapshot einer Snapshot-Hierarchie wiederherstellen, Snapshots löschen und vieles mehr.

Der Snapshot einer virtuellen Maschine speichert folgende Informationen:

- **Einstellungen der virtuellen Maschine**: das Verzeichnis der virtuellen Maschine, das Festplatten enthält, die Sie nach Anfertigung des Snapshots hinzugefügt oder geändert haben
- **Betriebszustand**: Die virtuelle Maschine kann eingeschaltet, ausgeschaltet oder angehalten sein.
- **Festplattenstatus**: Status aller virtuellen Festplatten der virtuellen Maschine
- **Arbeitsspeicherzustand** (optional): der Inhalt des Arbeitsspeichers der virtuellen Maschine

In diesem Abschnitt erstellen Sie einen Snapshot einer virtuellen Maschine, nehmen Änderungen an Hardware und Konfigurationsstatus der virtuellen Maschine vor und stellen den Ursprungszustand der virtuellen Maschine mit dem vSphere Web Client Snapshot Manager wieder her.

Erstellen eines VM-Snapshots

In diesem Schritt erstellen Sie einen Snapshot einer virtuellen Maschine.

1. Klicken Sie mit der rechten Maustaste auf **w12-core**.
2. Wählen Sie **Snapshots** aus.
3. Klicken Sie auf **Take Snapshot**.

Eingeben eines Namens und einer Beschreibung für den VM-Snapshot

1. Geben Sie im Assistenten zum Erstellen eines VM-Snapshots einen Namen für den Snapshot ein: **Snapshot#1**.

2. Geben Sie eine Beschreibung für den Snapshot ein: **Snapshot taken prior to VM settings change**.

3. Klicken Sie auf **OK**.

Hinweis: Wenn Sie einen Snapshot von einer eingeschalteten virtuellen Maschine erstellen, besteht die Möglichkeit, den Arbeitsspeicherzustand der ausgeführten VM zu speichern.

Öffnen der Registerkarte „Snapshots“

Beobachten Sie den Fortschritt im Fenster „Recent Tasks“. Sobald die Snapshot-Aufgabe abgeschlossen wurde:

1. Klicken Sie auf die Registerkarte **Snapshots** .

2. Beachten Sie den Betriebszustand der VM in Bezug auf den Snapshot-Zeitverlauf.

Ändern der Einstellungen der virtuellen Maschine

In diesem Abschnitt ändern Sie die Arbeitsspeicherkonfiguration der virtuellen Maschine.

Um die Arbeitsspeicherkonfiguration von „w12-core“ zu ändern, muss die VM ausgeschaltet werden.

1. Wählen Sie **Power --> Power Off im Menü „Actions“ aus.** Wählen Sie **Yes** aus, um den Ausschaltvorgang zu bestätigen.

HINWEIS: Hierbei handelt es sich nicht um die richtige Methode, um die VM sanft herunterzufahren, sie ermöglicht jedoch ein schnelles Ausschalten der Maschine im Rahmen des Hands-on Lab.

Starten des Einstellungsassistenten

1. Wählen Sie die virtuelle Maschine **w12-core** aus.

2. Klicken Sie auf das Dropdown-Menü „Actions“ und wählen Sie **Edit Settings...** aus.

Ändern der Einstellungen der virtuellen Maschine

1. Wählen Sie das Dropdown-Menü für die Einstellung **Memory** aus.

2. Wählen Sie **4 GB** aus.

Überprüfen der neuen Einstellungen der virtuellen Maschine

1. Prüfen Sie die neue Arbeitsspeicherkonfiguration.

2. Klicken Sie auf **OK**, um fortzufahren.

Registerkarte „Summary“

1. Klicken Sie auf die Registerkarte **Summary** von „w12-core“, um die aktualisierte Arbeitsspeicherkonfiguration anzuzeigen.

Rückgängigmachen der VM-Einstellungen mittels Snapshot Manager

In diesem Abschnitt versetzen Sie die Konfiguration der virtuellen Maschine mit dem Snapshot Manager zurück in den Ursprungszustand.

1. Stellen Sie sicher, dass **w12-core VM** ausgewählt ist.

2. Klicken Sie auf die Registerkarte **Snapshots**.

Auswählen des gewünschten VM-Snapshots

1. Stellen Sie sicher, dass **Snapshot#1** ausgewählt ist.

2. Wählen Sie **Revert to** im Menü **All Actions** aus.

Bestätigen der Snapshot-Wiederherstellung

1. Klicken Sie auf „Yes“, um die Aktion zu bestätigen.

Überwachen des Aufgabenfortschritts

1. Beobachten Sie den Fortschritt im Fenster **Recent Tasks**.

2. Sie stellen fest, dass die Arbeitsspeicherkonfiguration auf **2048** MB zurückgesetzt wurde.

Löschen eines Snapshots

Klicken Sie auf die Registerkarte **Snapshots**.

Löschen von „Snapshot#1“

1. Wählen Sie **Delete All Snapshots** im Menü **All Actions** aus.

Klicken Sie auf **Yes**, um das Löschen aller Snapshots zu bestätigen.

Als Best Practice sollten nicht mehr benötigte Snapshots gelöscht werden. Im Laufe der Zeit kann das Snapshot-Delta relativ stark anwachsen. Dies kann zu Problemen bei der Konsolidierung der VM-Dateien und zu Performance-Problemen führen.

Video: Weitere Informationen zu VM-Snapshots (2:33)

Im folgenden Video erhalten Sie weitere Informationen zu Snapshots von virtuellen vSphere-Maschinen:

vSphere Datastore Cluster

Ein vSphere Datastore Cluster gleicht die E/A- und Storage-Kapazität einer Gruppe von vSphere-Datastores aus. Je nach Grad der gewünschten Automatisierung werden virtuelle Maschinen von Storage Dynamic Resource Scheduler platziert und migriert, um die Auslastung des Datastores über den Datastore Cluster hinweg auszugleichen.

In diesem Abschnitt erstellen Sei einen vSphere Datastore Cluster mithilfe von zwei iSCSI-Datastores.

Was ist vSphere Storage DRS? (5:08)

In diesem animierten Video wird gezeigt, wie VMware Storage DRS den Zeitaufwand und die Komplexität des Provisioning virtueller Maschinen reduziert, indem Datastores in einem einzigen Pool zusammengefasst werden. Dieser Pool wird als Datastore-Cluster bezeichnet und ermöglicht die schnelle Platzierung von virtuellen Maschinen und VM-Festplatten.

Navigieren zu „Storage“

1. Wählen Sie das **Haussymbol** aus.

2. Wählen Sie **Storage** aus.

Neuer Datastore Cluster

1. Klicken Sie mit der rechten Maustaste auf **Datacenter Site A**.

2. Wählen Sie **Storage-->New Datastore Cluster...** aus.

Neuer Datastore Cluster: Name und Standort

Geben Sie als Name **DatastoreCluster-01** ein und wählen Sie **Next** aus.

Neuer Datastore Cluster: Storage DRS-Automatisierung

Behalten Sie aufgrund der E/A-Eigenschaften der VMware Hands-on Labs-Umgebung die Standardeinstellungen bei und wählen Sie **Next** aus.

Sie können gerne die verschiedenen Einstellungen für Storage DRS-Automatisierung ansehen.

Neuer Datastore Cluster: Storage DRS-Laufzeiteinstellungen

Storage DRS bietet verschiedene Optionen, um die Sensibilität des Storage-Cluster-Ausgleichs anzupassen. Behalten Sie zunächst die Standardeinstellungen bei und wählen Sie **Next** aus.

Neuer Datastore Cluster: Auswählen von Clustern und Hosts

Da es keine eigenständigen Hosts gibt, wählen Sie **Cluster Site A** aus und klicken Sie anschließend auf die Schaltfläche **Next**.

Neuer Datastore Cluster: Auswählen der Datastores

Wählen Sie die Datastores **ds-iscsi02** und **ds-iscsi01** für den neuen Datastore Cluster aus.

Neuer Datastore Cluster: Abschließen des Vorgangs

Überprüfen Sie die Storage DRS-Einstellungen und klicken Sie auf die Schaltfläche **Finish**.

Neuer Datastore Cluster: Zusammenfassung

Prüfen Sie im Fenster **Recent Tasks** den Fortschritt der Operation.

Erstellen eines Datastore-Clusters mit Storage DRS (3:23)

In diesem Video werden die Erstellung und das Management eines Datastore-Clusters in einer vSphere-Umgebung beschrieben.

Schlussbemerkung

Mit der Nutzung von vSphere Datastore Clusters in Ihrer vSphere-Umgebung können Sie sicherstellen, dass Datastores gleichmäßig gefüllt sind und E/A-Operationen gleichmäßig über die gesamte Gruppe von Datastores innerhalb des Clusters verteilt werden.
Storage DRS kann die anfängliche Platzierung von neuen virtuellen Maschinen automatisieren und die Platzierung von virtuellen Maschinen für eine gleichmäßige Verteilung von E/A-Operationen über den Datastore-Cluster hinweg anpassen.

Conclusion

Thank you for participating in the VMware Hands-on Labs. Be sure to visit http://hol.vmware.com/ to continue your lab experience online.

Lab SKU: ManualExport-HOL-1810-01-SDC.zip

Version: 20171201-202557