Die Vorteile einer lokalen Cloud und Nutzung vertrauter Tools

Durch Dell EMC PowerEdge FC640-Server und VMware-Software ist Private-Cloud-Management eine lohnenswerte Alternative zur Verlagerung in die Public Cloud

Die Art der Cloud, für die Sie sich jetzt entscheiden, wird sich über Jahre auf die Verwaltung Ihres Rechenzentrums auswirken. Schauen wir uns also einige Gründe an, warum es geschäftlich sinnvoll ist, sich für eine lokale Cloud statt einer Public Cloud zu entscheiden. Erstens können Sie durch den Aufbau und die Implementierung Ihrer eigenen Private Cloud besser auf Bedenken hinsichtlich Sicherheit, Compliance und Leistung für wichtige Anwendungen eingehen. Zweitens muss es mit einer Dell EMC™ PowerEdge™ FX2-Architektur und vertrauten Tools nicht notwendigerweise immer der Fall sein, dass Public Clouds – wie von einigen Leuten angenommen – einfacher zu verwalten sind als lokale Clouds und zwangsweise zur Senkung der Verwaltungskosten beitragen. In der Tat können mit Vor-Ort-Bereitstellungen in bestimmten Fällen ebenfalls Einsparungen bei den Gesamtbetriebskosten (TCO) erzielt werden.

Wir haben festgestellt, dass zur Verwaltung einer lokalen Private-Cloud-Lösung auf Dell EMC PowerEdge FC640-Servern mit skalierbaren Prozessoren der Intel® Xeon® Produktreihe im Vergleich zu einer auf Amazon Web Services™ (AWS) ausgeführten Public Cloud zwar ein vergleichbarer Zeitaufwand, aber durchschnittlich um 34 Prozent weniger Schritte erforderlich waren. Darüber hinaus ist die VMware®-Software integriert, mit der Sie bereits vertraut sind.

Dell EMC PowerEdge FC640-Server mit neuester Technologie für Private Clouds

** im Vergleich zu einer AWS Public Cloud*

Nutzen der Vorteile einer lokalen Cloud

Schnelles Erledigen von Aufgaben

Vergleichbarer Zeitaufwand beim Cloudmanagement bei durchschnittlich **34 % weniger Schritten***

Nutzen der Vorteile einer lokalen Cloud

Die vom Wettbewerb geprägten Geschäftsumgebungen von heute machen eine Verlagerung in die Cloud unausweichlich. Die Wahl zwischen einer Public und einer Private Cloud ist in etwa vergleichbar damit, ob ein Auto gekauft oder geleast wird. Wenn Sie sich für eine Public Cloud entscheiden, beispielsweise die bereits erwähnte AWS-Option, begeben Sie sich in die Abhängigkeit von einem monatlichen oder jährlichen Vertrag und müssen abwägen, wie viel Datenspeicher und -zugriff Sie jetzt und in absehbarer Zukunft benötigen. Ähnlich wie beim Leasing eines Autos kann eine Überschreitung des im Rahmen des Abonnements verfügbaren Kontingents zusätzliche Kosten nach sich ziehen. Bei einer lokalen Private Cloud wie der angesprochenen Dell EMC PowerEdge FX2-Lösung zahlen Sie im Voraus und erhalten eine flexible, modulare Serverplattform, die Sie entsprechend den aktuellen Anforderungen aufteilen und vollständig zuweisen und bei einer Änderung dieser Anforderungen neu konfigurieren können. Der Aufbau und die Implementierung einer eigenen Private Cloud bieten außerdem eine Vielzahl weiterer Vorteile:

Sicherheit und Compliance

Die Sicherheit sensibler Daten zu gewährleisten ist ein ständiger Kampf. Wenn Sie sich für eine lokale Cloudlösung entscheiden, wissen Sie immer genau, wo sich Ihre Daten befinden, und behalten die Kontrolle über die Sicherheitsstrategien, die zum Schutz Ihres Unternehmens und seiner Kunden implementiert werden. Dies ist besonders wichtig, wenn Ihr Unternehmen medizinische oder Finanzdaten verarbeitet oder behördliche Auflagen erfüllen muss. Die Speicherung solcher Daten in einer Public Cloud kann mit dem Wachstum Ihres Unternehmens zunehmend komplex werden.

Leistung und Kontinuität

Der Umstieg auf neue Technologien kann IT-Mitarbeiter vor große Herausforderungen stellen, da sie eventuell wieder geschult werden müssen. Wenn Sie sich für eine lokale Cloudlösung entscheiden, können Sie Ihre bestehende VMware vSphere®-Umgebung weiter nutzen und Ihre Cloud über die Cloudmanagementplattformen der VMware vRealize® Suite erstellen und steuern. Dadurch erleichtern Sie der IT, die bereits mit diesen Tools vertraut ist, die Aktualisierung, Sicherung und Optimierung wichtiger Anwendungen. Bestehende IT-Strategien und -Policies des Unternehmens können Sie ebenfalls beibehalten, wenn Sie sich für eine lokale Private-Cloud-Lösung mit Dell EMC PowerEdge FX2 entscheiden.

Anpassung und Verständnis

Sie wissen besser als jeder andere, welchen Kunden, Nutzern und Anwendungen Priorität eingeräumt werden muss. Es ist unrealistisch, von einem Public-Cloud-Service zu erwarten, dass er die erforderliche Granularität bietet, um die Verfügbarkeit für die Abläufe zu gewährleisten, die für Sie am wichtigsten sind. Wenn Sie sich für eine lokale Cloudlösung entscheiden, können Sie das Ressourcenmanagement an Ihre spezifischen Anforderungen anpassen und müssen sich nicht mit der Universallösung einer Public Cloud zufriedengeben.

Die Dell EMC PowerEdge FX2-Lösung

Bei Dell EMC PowerEdge FX2 handelt es sich um eine modulare Serverplattform, die Server, Speicher und Netzwerke in einem einzigen 2-HE-Gehäuse vereint.

Die neuen Dell EMC PowerEdge FC640-Server mit zwei Sockeln und halber Länge sind mit den neuen skalierbaren Prozessoren der Intel Xeon Produktreihe, bis zu 2 TB Arbeitsspeicher und verschiedenen Speichermedien ausgestattet, darunter SSDs mit Speicherkapazitäten von bis zu 240 GB.

Dell EMC PowerEdge FC640-Server bieten außerdem integrierte End-to-End-Sicherheit, wie z. B. Silicon Root of Trust (chipbasierte Sicherheit) für Firmwareaktualisierungen, zusätzlichen Schutz vor Hardwareangriffen, Policy-basierte USB-Kontrolle und sichere Verschlüsselungsoptionen für Laufwerke.

Weitere Informationen über die Dell EMC PowerEdge FX-Architektur finden Sie unter www.dell.com/en-us/work/shop/cty/pdp/spd/poweredge-fx.

Schnelles Erledigen von Cloudmanagementaufgaben

Ob Public oder Private Cloud, irgendjemand muss ihre Verwaltung übernehmen. Mit einer lokalen Dell EMC Private Cloud sind Sie mit Ihren IT-Mitarbeitern, die sich um Ihre bestehende PowerEdge- und VMware-Infrastruktur kümmern, bestens gerüstet.

Wir haben für beide Cloudoptionen die benötigte Zeit sowie die Schritte zur Durchführung acht häufiger Cloudmanagementaufgaben protokolliert. Wir haben eine Vielzahl von Aufgaben ausgesucht, die zusammen ein umfassendes Bild eines Cloudmanagement-Lebenszyklus vermitteln. Diese Aufgaben decken das Monitoring der Konfigurationsschritte ab, das von Administratoren häufig geändert wird, sowie die Wartung von Nutzerkonten, mit der sich die Administratoren fast täglich auseinandersetzen müssen.

FX2- und TCO-Einsparungen

Principled Technologies führte eine Studie durch, in der die TCO-Kosten eines auf Apache Spark basierenden Big Data-Analytik-Workload auf einer AWS-Public-Cloud-Lösung mit denen auf einer lokalen Dell EMC PowerEdge FX2-Lösung verglichen wurden. Wir haben festgestellt, dass mit einer lokalen Dell EMC FX2-Lösung **bis zu 42 Prozent an TCO-Kosten gespart werden können**. Obwohl in dieser Studie ein anderes Betriebssystem und eine andere Testumgebung verwendet wurden als in dem Ihnen vorliegenden Bericht, vermittelt sie dennoch einen Eindruck von den möglichen Kosteneinsparungen im Zusammenhang mit der Leistung. Klicken Sie hier, um den vollständigen Bericht „Run big data analytics on a powerful on-premises Dell EMC PowerEdge FX2 solution and save money over three years" zu lesen.[1]

Szenarien	Dell EMC und VMware		AWS	
	Zeit (m:s)	Schritte	Zeit (m:s)	Schritte
Erstellen eines neuen Nutzers	01:01	20	00:59	22
Bereitstellen einer angepassten VM	00:14	7	00:34	14
Konfigurieren des Monitorings von Vorgängen	00:10	3	00:12	6
Konfigurieren des Monitorings von Protokolldateien	00:07	3	00:10	7
Konfigurieren von angepassten Chargeback-Berichten	00:23	6	00:18	9
Konfigurieren des Capacity-Managements	00:08	3	00:08	4
Bereitstellen eines LAMP-Stacks	00:17	6	00:47	15
Erstellen eines Snapshot	00:15	9	00:12	8

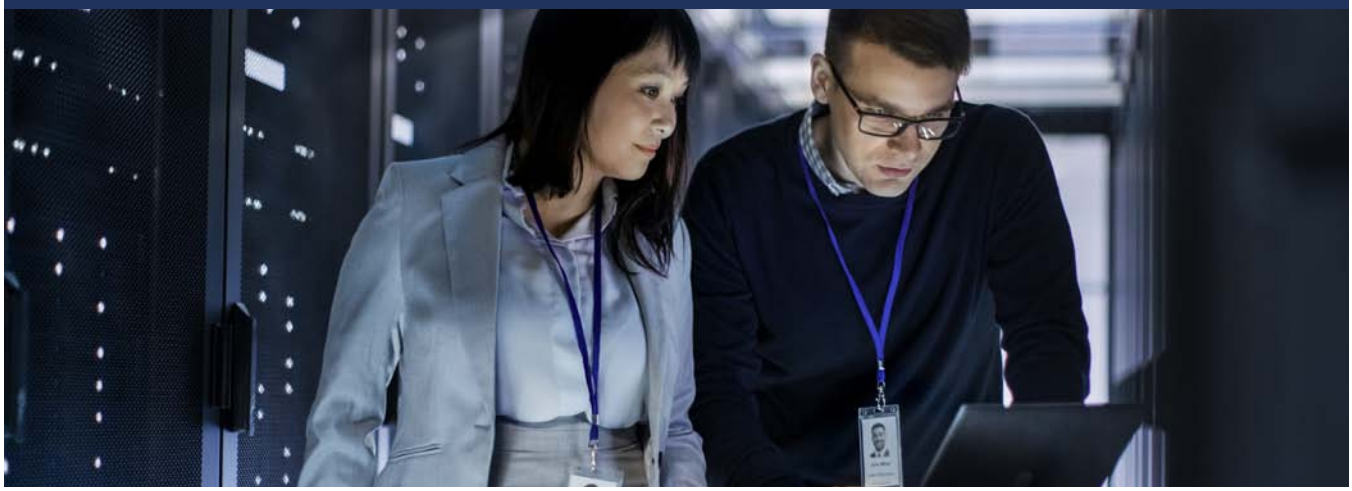
Sämtliche Ergebnisse finden Sie in Anhang D.

Für die acht getesteten, gängigen Verwaltungsaufgaben war bei der Private-Cloud-Lösung von Dell EMC zwar eine vergleichbare Zeit wie bei der AWS Public Cloud erforderlich, aber es wurden durchschnittlich um 34 Prozent weniger Schritte benötigt. Diese Ergebnisse zeigen auch, dass die Wahl einer Public Cloud gegenüber einer lokalen Cloud nicht zwangsweise zu einer Senkung der Verwaltungskosten führt, da der Zeitaufwand im Wesentlichen identisch ist.

Informationen über skalierbare Intel Xeon Prozessoren

Skalierbare Intel Xeon Prozessoren sind Serverprozessoren der neuesten Generation von Intel mit vier Konfigurationen: Platinum, Gold, Silver und Bronze.

In unseren Tests der lokalen Private Cloud wurde der Dell EMC PowerEdge FC640 mit Intel Xeon Gold 5120-Prozessoren verwendet. Dieser Prozessor enthält 14 Cores, die mit einer Frequenz von 2,20 GHz und einer maximalen Turbofrequenz von 3,20 GHz ausgeführt werden. Weitere Informationen zu skalierbaren Intel Xeon Prozessoren finden Sie unter www.intel.com/content/www/us/en/processors/xeon/scalable/xeon-scalable-platform.html.



Fazit

Unsere Administratoren fanden heraus, dass es in manchen Fällen und Situationen geschäftlich sinnvoll ist, sich statt für eine Public-Cloud-Lösung von AWS für eine lokale Private-Cloud-Lösung zu entscheiden, die in einer Dell EMC PowerEdge FX2-Architektur auf FC640-Servern mit skalierbaren Prozessoren der Intel Xeon Produktreihe ausgeführt wird. Das liegt zum Teil daran, dass mit der VMware-Software eine Vielzahl gängiger Cloudverwaltungsaufgaben in einer lokalen Private Cloud im Vergleich zur Public-Cloud-Option von AWS innerhalb eines vergleichbaren Zeitraums aber mit durchschnittlich um 34 % weniger Schritten durchgeführt werden konnten. Ein weiterer wesentlicher Vorteil besteht darin, dass Rechenzentrumsadministratoren auch weiterhin die volle Kontrolle über die Implementierung ihrer Sicherheitsstrategien behalten und die Private-Cloud-Ressourcen aus Leistungsgründen anpassen können, ohne sich Gedanken über ein Überschreiten des im Rahmen des Abonnements verfügbaren Kontingents machen zu müssen. Dadurch kann Ihr Rechenzentrum problemlos an sich ständig ändernde Geschäftsanforderungen angepasst werden.

1 Principled Technologies: Run big data analytics on a powerful on-premises Dell EMC PowerEdge FX2 solution and save money over three years (Ersparnisse über einen 3-Jahres-Zeitraum bei der Ausführung von Big Data-Analytik auf einer leistungsstarken lokalen Dell EMC PowerEdge FX2-Lösung)

Die getesteten Hardware- und Softwarekonfigurationen wurden am 5. November 2017 finalisiert. Da oft Aktualisierungen für aktuelle und kürzlich veröffentlichte Hardware und Software herausgegeben werden, handelt es sich bei diesen Konfigurationen zum Zeitpunkt der Veröffentlichung dieses Berichts nicht immer um die neuesten verfügbaren Versionen. Am 30. November 2017 schlossen wir den praxisnahen Test ab.

Anhang A: Systemkonfigurationsinformationen

Informationen zur Serverkonfiguration	4 x Dell EMC PowerEdge FC640
BIOS-Name und -Version	Dell 1.0.1
Name und Version/Build-Nummer des Betriebssystems	VMware ESXi, 6.5.0, 5969303
Datum der zuletzt angewendeten Betriebssystemaktualisierungen/-patches	10/30/2017
Energiemanagement-Policy	Performance
Prozessor	
Anzahl der Prozessoren	2
Anbieter und Modell	Intel Xeon Gold 5120
Anzahl der Kerne (pro Prozessor)	14
Kernfrequenz (GHz)	2,20
Stepping	1
Speichermodul(e)	
Gesamtarbeitsspeicher im System (GB)	192
Anzahl der Speichermodule	12
Anbieter und Modell	Hynix HMA82GR7AFR8N-VK
Größe (GB)	16
Typ	PC4-21300R
Geschwindigkeit (MHz)	2.666
Geschwindigkeit bei Ausführung im Server (MHz)	2.444
Speicher-Controller	
Anbieter und Modell	Dell PERC H330 Mini
Firmwareversion	25.3.0004
Treiberversion	4.27

Informationen zur Serverkonfiguration	4 x Dell EMC PowerEdge FC640
Lokale Festplatten	
Anzahl der Laufwerke	2
Laufwerkanbieter und -modell	Seagate® ST600MM0238
Laufwerksgröße (GB)	600
Informationen zum Laufwerk (Geschwindigkeit, Schnittstelle, Typ)	10.000, 12-Gbit-SAS, HDD
Netzwerkadapter	
Anbieter und Modell	Intel Ethernet 10G 2P X710-k bND
Portanzahl und -typ	2 x 10GbE
Treiberversion	18.016

Speicherkonfigurationsinformationen	1 x Dell Storage SC9000 Array-Controller
Controller-Firmwareversion	6.7.5
Anzahl der Speichercontroller	2
Anzahl der Speichereinschübe	1
Anzahl der Laufwerke pro Einschub	24
Laufwerke Nr. 1	
Anzahl der Laufwerke	12
Anbieter und Modellnummer des Laufwerks	Dell LB806M
Laufwerksgröße (GB)	800
Informationen zum Laufwerk (Geschwindigkeit, Schnittstelle, Typ)	6 Gbit/s, SAS, SSD
Laufwerke Nr. 2	
Anzahl der Laufwerke	6
Anbieter und Modellnummer des Laufwerks	Dell HUSMH8040BSS200
Laufwerksgröße (GB)	400
Informationen zum Laufwerk (Geschwindigkeit, Schnittstelle, Typ)	12 Gbit/s, SAS, SSD
Laufwerke Nr. 3	
Anzahl der Laufwerke	6
Anbieter und Modellnummer des Laufwerks	Dell HUSMM1680ASS200
Laufwerksgröße (GB)	800
Informationen zum Laufwerk (Geschwindigkeit, Schnittstelle, Typ)	12 Gbit/s, SAS, SSD

Details zur Konfiguration des Servergehäuses	Dell EMC PowerEdge FX2s
Anzahl der Managementmodule	2
Firmwareversion des Managementmoduls	2.0
CMC-Modulfirmware	2.00
Version der Mittelplatine	1.0
Erster Typ I/O-Modul	
Anbieter und Modellnummer	Dell 1GbE-Pass-Through-Modul
Firmwareversion des I/O-Moduls	X03
Anzahl der Module	1
Besetzte Steckplätze	A2
Netzteile	
Anbieter und Modellnummer	Dell 0W1R7VA00
Anzahl der Netzteile	2
Jeweilige Leistung in Watt (W)	2.000
Lüfter	
Anzahl der Lüfter	8

Anhang B: Einrichtung der Testumgebung

Dieser Anhang bietet einen Einblick in den Einrichtungsprozess für die Private Cloud von Dell EMC und die AWS-Public-Cloud-Umgebungen. Unsere für die Tests verwendeten Anwendungsfälle gehen in allen Fällen von bereits vorhandenen Umgebungen aus und diese Schritte sind nicht Teil unseres Vergleichs.

Bereitstellen einer lokalen Cloud mit Dell EMC und VMware

Wir haben jeden Dell EMC PowerEdge FC640-Server mit einem virtuellen Laufwerk konfiguriert, das zwei physische Laufwerke in einer RAID-10-Konfiguration als lokalen Speicher und für die Hypervisor-Installation verwendet. Wir haben vier Volumes (eins für jeden Server) auf dem Dell Storage SC9000-Array erstellt, das als nicht lokaler Speicher verwendet werden soll.

Installieren von VMware ESXi 6.5

1. Schließen Sie das Installationsmedium am Server an.
2. Starten Sie den Server.
3. Auf dem VMware-Installationsbildschirm drücken Sie die Eingabetaste.
4. Drücken Sie im EULA-Bildschirm F11 zum Bestätigen und Fortfahren.
5. Wählen Sie unter „Speichergeräte“ die entsprechende Festplatte aus und drücken Sie die Eingabetaste.
6. Wählen Sie „US“ als Tastaturbelegung aus und drücken Sie die Eingabetaste.
7. Geben Sie zweimal ein Root-Passwort ein und drücken Sie die Eingabetaste.
8. Drücken Sie F11, um die Installation zu starten.
9. Um den Server neu zu starten, entfernen Sie das Installationsmedium und drücken Sie die Eingabetaste.
10. Nach dem Neustart des Servers drücken Sie F2, und geben die Root-Anmeldedaten ein.
11. Wählen Sie „Configure Management Network“ aus und drücken Sie die Eingabetaste.
12. Wählen Sie die IPv4-Konfiguration aus und geben Sie die gewünschten Konfigurationsdetails ein. Drücken Sie die Eingabetaste.
13. Wählen Sie „DNS Configuration“ aus und geben Sie den primären DNS-Server ein. Drücken Sie die Eingabetaste.
14. Drücken Sie die Esc-Taste und anschließend die Taste „Y“, um Änderungen zu akzeptieren.

Bereitstellen der VMware vCenter Server 6.5-Appliance

1. Öffnen Sie den Ordner des Installationsmediums.
2. Wählen Sie „vcsa-ui-installer“ aus und klicken Sie mit der rechten Maustaste auf die Installationsanwendung.
3. Klicken Sie auf Als Administrator ausführen.
4. Klicken Sie auf „Yes“.
5. Klicken Sie im Fenster „Appliance 6.5 Installer“ auf „Install“.
6. Klicken Sie auf der Seite „Introduction“ auf „Next“.
7. Akzeptieren Sie die Bedingungen der Lizenzvereinbarung und klicken Sie auf „Next“.
8. Wählen Sie „Install vCenter Server with an Embedded Platform Services Controller“ aus und klicken Sie auf „Next“.
9. Geben Sie die IP-Adresse für den ESXi-Zielserver, den Nutzernamen und das Passwort ein und klicken Sie auf „Next“.
10. Klicken Sie auf „Yes“, um das Zertifikat zu akzeptieren.
11. Geben Sie ein Root-Passwort für die Appliance ein, bestätigen Sie die Eingabe und klicken Sie auf „Next“.
12. Wählen Sie die Bereitstellungsgröße aus (wir haben „Tiny“ und die Standardspeichergröße ausgewählt) und klicken Sie auf „Next“.
13. Aktivieren Sie das Kontrollkästchen, um den Thin-Festplattenmodus zu aktivieren, und klicken Sie auf „Next“.
14. Geben Sie die gewünschten Netzwerkinformationen ein (IP-Adresse der Anwendung, Subnetz, Gateway und DNS) und klicken Sie auf „Next“.
15. Überprüfen Sie die Informationen für Stufe 1 und klicken Sie auf „Finish“.
16. Klicken Sie auf „Next“, um mit Stufe 2 der Bereitstellung fortzufahren.
17. Klicken Sie auf der Seite „Introduction“ auf „Next“.
18. Geben Sie die NTP-Server für die Synchronisation ein, aktivieren Sie SSH und klicken Sie auf „Next“.
19. Geben Sie einen Domainnamen, ein Passwort und einen Standortnamen ein und klicken Sie auf „Next“.
20. Für CEIP klicken Sie auf „Next“.
21. Überprüfen Sie die Einstellungen für Stufe 2 und klicken Sie auf „Finish“.
22. Klicken Sie nach dem Einrichten auf „Close“.

Installieren des VMware Enhanced Authentication-Plug-ins

1. Öffnen Sie einen Webbrowser und geben Sie die IP-Adresse der vCenter Server-Appliance ein.
2. Klicken Sie, um vSphere Web Client (Flash) zu öffnen.
3. Klicken Sie auf „Download Enhanced Authentication Plugin“.
4. Klicken Sie auf „Save File“.
5. Navigieren Sie zu „Downloads“ und doppelklicken Sie auf die Installationsanwendung.
6. Klicken Sie auf „OK“.
7. Klicken Sie auf „OK“.
8. Klicken Sie im Begrüßungsfenster der Installationsanwendung auf „Next“.
9. Akzeptieren Sie die Bedingungen der Lizenzvereinbarung und klicken Sie auf „Next“.
10. Klicken Sie auf „Install“.
11. Klicken Sie auf „Finish“.
12. Klicken Sie im Fenster „Installation“ des Plug-in-Service auf „Next“.
13. Akzeptieren Sie die Bedingungen der Lizenzvereinbarung und klicken Sie auf „Next“.
14. Klicken Sie auf „Install“.
15. Klicken Sie auf „Finish“.

Bereitstellen und Konfigurieren von vRealize Operations Manager (vROM)

1. Klicken Sie in vSphere Web Client mit der rechten Maustaste auf das Cluster.
2. Wählen Sie „Deploy OVF Template...“ aus.
3. Klicken Sie auf „Browse...“.
4. Navigieren Sie zur OVF-Datei und klicken Sie auf „Open“.
5. Klicken Sie auf „Next“.
6. Geben Sie einen Namen für die OVF ein und klicken Sie auf „Next“.
7. Wählen Sie eine Ressource für die OVF aus und klicken Sie auf „Next“.
8. Überprüfen Sie die Vorlagendetails und klicken Sie auf „Next“.
9. Akzeptieren Sie die Lizenzvereinbarungen und klicken Sie auf „Next“.
10. Wählen Sie die Konfigurationsgröße aus (wir haben „Extra Small“ gewählt) und klicken Sie auf „Next“.
11. Wählen Sie das Format des virtuellen Laufwerks und den Datenspeicher aus und klicken Sie auf „Next“.
12. Wählen Sie das Netzwerk aus und klicken Sie auf „Next“.
13. Geben Sie die IP-Adressen für den DNS und das Standardgateway ein.
14. Geben Sie die IP-Adresse für die OVF und die Netzmaske ein.
15. Erweitern Sie die zusätzlichen Einstellungen und wählen Sie die richtige Zeitzone aus.
16. Klicken Sie auf „Next“.
17. Überprüfen Sie die Konfiguration und klicken Sie auf „Finish“.
18. Schalten Sie die VM ein.
19. Navigieren Sie im Webbrowser zur IP-Adresse von vROM.
20. Klicken Sie auf „New Installation“.
21. Klicken Sie auf „Next“.
22. Geben Sie ein Passwort für das Administratorkonto ein, bestätigen Sie es und klicken Sie auf „Next“.
23. Wählen Sie eine Zertifikatmethode aus und klicken Sie auf „Next“.
24. Geben Sie einen Master-Node-Namen für das Cluster und eine NTP-Serveradresse ein.
25. Klicken Sie auf „Next“.
26. Klicken Sie auf „Finish“.
27. Nachdem die Initialisierung abgeschlossen ist, klicken Sie auf „START vREALIZE OPERATIONS MANAGER“.
28. Klicken Sie auf „Yes“.
29. Wenn vROM online ist, melden Sie sich mit dem Administratorkonto und dem zuvor festgelegten Passwort bei vROM an.
30. Klicken Sie im angezeigten Fenster auf „Next“.
31. Akzeptieren Sie die EULA und klicken Sie auf Next.
32. Geben Sie einen Produktschlüssel ein oder wählen Sie „Product Evaluation“ aus und klicken Sie auf „Next“.
33. Klicken Sie auf „Next“.
34. Klicken Sie auf „Finish“.
35. Wählen Sie VMware vSphere aus.
36. Klicken Sie auf das Zahnradsymbol, um die Konfiguration durchzuführen.
37. Geben Sie einen Anzeigenamen und die IP-Adresse von vCenter ein.
38. Klicken Sie auf das grüne Pluszeichen, geben Sie den Namen, den Nutzernamen und das Passwort für die vCenter-Administratoranmeldedaten ein.

39. Klicken Sie auf „OK“.
40. Klicken Sie auf Test Connection.
41. Klicken Sie auf „ACCEPT“, um das Zertifikat zu akzeptieren.
42. Klicken Sie nach einer erfolgreichen Testverbindung auf „OK“.
43. Klicken Sie auf „SAVE SETTINGS“.
44. Klicken Sie auf „OK“.
45. Klicken Sie auf „CLOSE“.

Bereitstellen und Konfigurieren von vRealize Log Insight (vRLI)

1. Klicken Sie in vSphere Web Client mit der rechten Maustaste auf das Cluster.
2. Wählen Sie „Deploy OVF Template...“ aus.
3. Klicken Sie auf „Browse...“.
4. Navigieren Sie zur OVF-Datei und klicken Sie auf „Open“.
5. Klicken Sie auf „Next“.
6. Geben Sie einen Namen für die OVF ein und klicken Sie auf „Next“.
7. Wählen Sie eine Ressource für die OVF aus und klicken Sie auf „Next“.
8. Überprüfen Sie die Vorlagendetails und klicken Sie auf „Next“.
9. Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf „Next“.
10. Wählen Sie die Konfigurationsgröße aus (wir haben „Extra Small“ gewählt) und klicken Sie auf „Next“.
11. Wählen Sie das Format des virtuellen Laufwerks und den Datenspeicher aus und klicken Sie auf „Next“.
12. Wählen Sie das Zielnetzwerk aus und klicken Sie auf „Next“.
13. Geben Sie die IP-Adressen für den DNS, die DNS-Domain und den DNS-Suchpfad ein.
14. Geben Sie die IP-Adressen für das Standardgateway und die VM ein.
15. Geben Sie die Netzmaske ein und erweitern Sie die Optionsliste.
16. Geben Sie ein Root-Passwort ein, bestätigen Sie es und klicken Sie auf „Next“.
17. Überprüfen Sie die Konfigurationsdaten und klicken Sie auf „Finish“.
18. Schalten Sie die VM ein.
19. Navigieren Sie im Webbrowser zur IP-Adresse von vRLI.
20. Klicken Sie auf „Next“.
21. Klicken Sie auf „Start New Deployment“.
22. Geben Sie eine E-Mail-Adresse ein. Geben Sie außerdem ein neues Passwort ein und bestätigen Sie es.
23. Klicken Sie auf „Save“ und dann auf „Continue“.
24. Geben Sie einen Lizenzschlüssel ein oder klicken Sie auf „Skip“, um den Bewertungsmodus zu verwenden.
25. Geben Sie eine E-Mail-Adresse und URLs für den Erhalt von Systemmeldungen ein. Klicken Sie auf „Save“ und dann auf „Continue“.
26. Geben Sie weitere NTP-Server ein und klicken Sie auf „Test“.
27. Nachdem die Tests erfolgreich abgeschlossen wurden, klicken Sie auf „Save“ und dann auf „Continue“.
28. Geben Sie zusätzliche SMTP-Konfigurationseinstellungen ein oder klicken Sie auf „Skip“.
29. Klicken Sie auf „Finish“.
30. Klicken Sie auf „Configure vSpehre integration“.
31. Geben Sie die IP-Adresse, den Nutzernamen und das Passwort für den vCenter-Server ein.
32. Klicken Sie auf „Test Connection“.
33. Klicken Sie auf „Save“, nachdem der Test erfolgreich abgeschlossen wurde.
34. Klicken Sie auf „OK“.
35. Klicken Sie im Seitenmenü auf „vRealize Operations“.
36. Geben Sie den Hostnamen, den Nutzernamen und das Passwort für vROM ein.
37. Klicken Sie auf „Test Connection“.
38. Klicken Sie auf „Next“, nachdem der Test erfolgreich abgeschlossen wurde.
39. Klicken Sie auf „OK“.

Erstellen und Konfigurieren des IaaS-Windows-Servers

1. Klicken Sie in der vCenter-Webkonsole mit der rechten Maustaste auf das Cluster oder den Server, wählen Sie „New Virtual Machine“ aus und klicken Sie dann auf „New Virtual Machine“.
2. Wählen Sie „Create a new virtual machine“ aus und klicken Sie auf „Next“.
3. Geben Sie einen Namen für die virtuelle Maschine ein, wählen Sie ein Rechenzentrum aus und klicken Sie auf „Next“.
4. Wählen Sie eine Rechnerressource aus und klicken Sie auf „Next“.
5. Wählen Sie einen Datenspeicher aus und klicken Sie auf „Next“.
6. Wählen Sie die gewünschte Kompatibilität/Version aus und klicken Sie auf „Next“.

7. Wählen Sie die Produktreihe für das Gastbetriebssystem (Windows) und die Version des Gastbetriebssystems (Windows Server 2016) aus und klicken Sie auf „Next“.
8. Passen Sie die Hardware nach Bedarf an (wir haben 2 vCPUs und 8.192 MB Arbeitsspeicher ausgewählt) und klicken Sie auf „Next“.
9. Überprüfen Sie die Konfiguration und klicken Sie auf „Finish“.
10. Stellen Sie entweder über die Webkonsole oder VRMC eine Verbindung zur virtuellen Konsole her.
11. Schließen Sie das Installationsmedium für Windows Server 2016 an.
12. Schalten Sie die VM ein.
13. Klicken Sie im Bildschirm der Sprachauswahl auf „Next“.
14. Klicken Sie auf „Install Now“.
15. Geben Sie den Produktschlüssel ein und klicken Sie auf „Next“.
16. Wählen Sie die Desktoperfahrung aus und klicken Sie auf „Next“.
17. Akzeptieren Sie die Lizenzbedingungen und klicken Sie auf „Next“.
18. Wählen Sie die Installationsoption „Custom“ aus.
19. Klicken Sie auf „Next“.
20. Geben Sie das gewünschte Passwort für den Administrator ein und klicken Sie auf „Finish“.
21. Kehren Sie zur vCenter-Webkonsole zurück.
22. Klicken Sie mit der rechten Maustaste auf die VM, wählen Sie das Gastbetriebssystem und anschließend „Install VMware Tools...“ aus.
23. Kehren Sie zur VM zurück, doppelklicken Sie auf das Installationsprogramm für die VMware-Tools und befolgen Sie die Anweisungen zur Installation der VMware-Tools.
24. Führen Sie Windows Update aus und starten Sie die VM gegebenenfalls neu.
25. Fügen Sie den Server zur Domain hinzu.
26. Nachdem Sie den Server zur Domain hinzugefügt haben, klicken Sie im Servermanagerfenster auf „Add Roles and Features“.
27. Fügen Sie die folgenden Funktionen hinzu: .NET 3.5 (HTTP- und Nicht-HTTP-Authentifizierung), .NET 4.6 (HTTP und Nicht-HTTP-Authentifizierung) und IIS. Führen Sie einen Neustart durch, falls erforderlich.
28. Öffnen Sie einen Webbrowser und navigieren Sie zu `http://java.com/en/download/.`
29. Klicken Sie auf „Free Java Download“.
30. Öffnen Sie das Installationsmedium und befolgen Sie die Anweisungen, um Java zu installieren.
31. Nachdem die Installation abgeschlossen ist, suchen Sie über die Befehlszeile oder den Datei-Explorer nach der Java-Installation (Beispiel: C:\Program Files\jre 1.8.version).
32. Rufen Sie über das Control Panel die erweiterten Systemeinstellungen auf.
33. Klicken Sie auf „Environment Variables“.
34. Klicken Sie auf „New“.
35. Geben Sie als Namen der Variable `JAVA_HOME` und den Pfad zum Java-Ordner als Wert ein.
36. Klicken Sie auf „OK“.
37. Verbinden Sie das Installationsmedium für Microsoft SQL Server 2016 mit der VM.
38. Starten Sie das Installationsprogramm für Microsoft SQL Server.
39. Klicken Sie auf „Installation“ und wählen Sie „New installation“ aus oder fügen Sie einer vorhandenen Installation Funktionen hinzu.
40. Geben Sie den Produktschlüssel ein und klicken Sie auf „Next“.
41. Aktivieren Sie „Use Microsoft Update“ und klicken Sie auf „Next“.
42. Klicken Sie auf „Installieren“, um die Setupsupportdateien zu installieren.
43. Wählen Sie SQL Server Funktionsinstallation aus und klicken Sie auf Weiter.
44. Wählen Sie „Database Engine Services“, „Full-Text Search“, „Client Tools Connectivity“, „Client Tools Backwards Compatibility“ sowie „Management Tools Basic“ und „Management Tools Complete“ aus. Klicken Sie auf „Next“.
45. Übernehmen Sie die Standardwerte der Instanzkonfiguration und klicken Sie auf „Next“.
46. Übernehmen Sie die Standardwerte der Serverkonfiguration und klicken Sie auf „Next“.
47. Wählen Sie Gemischter Modus aus und geben Sie ein Passwort für das SA-Konto ein. Klicken Sie auf Aktuellen Benutzer hinzufügen und dann auf Weiter.
48. Überprüfen Sie die Konfigurationsregeln für die Installation und klicken Sie auf „Install“.
49. Klicken Sie auf dem Abschlussbildschirm auf Schließen.
50. Öffnen Sie einen Webbrowser und navigieren Sie zu `http://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms.`
51. Laden Sie Microsoft SQL Server Management Studio herunter und befolgen Sie die Installationsanweisungen zur Installation von SSMS.

Bereitstellen und Konfigurieren von vRealize Automation (vRA)

1. Klicken Sie in vSphere Web Client mit der rechten Maustaste auf das Cluster.
2. Wählen Sie „Deploy OVF Template...“ aus.
3. Klicken Sie auf „Browse...“.
4. Navigieren Sie zur OVF-Datei und klicken Sie auf „Open“.
5. Klicken Sie auf „Next“.
6. Geben Sie einen Namen für die OVF ein und klicken Sie auf „Next“.
7. Wählen Sie eine Ressource für die OVF aus und klicken Sie auf „Next“.

8. Überprüfen Sie die Vorlagendetails und klicken Sie auf „Next“.
9. Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf „Next“.
10. Wählen Sie das Format des virtuellen Laufwerks und den Datenspeicher aus und klicken Sie auf „Next“.
11. Wählen Sie das Zielnetzwerk aus und klicken Sie auf „Next“.
12. Aktivieren Sie das Kontrollkästchen, um SSH zu aktivieren.
13. Geben Sie einen Hostnamen und ein Passwort ein und erweitern Sie durch Klicken die Netzwerkeigenschaften.
14. Geben Sie die IP-Adresse von Standardgateway, DNS und VM ein.
15. Geben Sie die Netzmaske ein und klicken Sie auf „Next“.
16. Klicken Sie auf „Finish“.
17. Schalten Sie die VM ein.
18. Navigieren Sie im Webbrowser zur IP-Adresse von vRA.
19. Melden Sie sich mit dem `Root`- und dem bei der Einrichtung eingegebenen Passwort an.
20. Klicken Sie im Installationsassistenten auf „Next“.
21. Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf Next.
22. Wählen Sie die Bereitstellungsgröße aus (wir haben uns für eine minimale Bereitstellung entschieden), behalten Sie die Standardinstallation von IaaS bei und klicken Sie auf „Next“.
23. Wählen Sie „Use Time Server“ aus.
24. Klicken Sie auf das grüne Pluszeichen, um einen NTP-Server hinzuzufügen.
25. Öffnen Sie eine Remotekonsolensitzung zum IaaS-Windows-Server.

Installation des Management-Agent auf dem IaaS-Windows-Server

1. Öffnen Sie auf dem IaaS-Windows-Server einen Webbrowser und navigieren Sie zur IP-Adresse von vRA.
2. Melden Sie sich mit dem `Root`- und dem bei der Einrichtung eingegebenen Passwort an.
3. Klicken Sie im Installationsassistenten auf „Next“.
4. Laden Sie den IaaS-Management-Agent herunter.
5. Klicken Sie auf „Save“.
6. Klicken Sie auf Öffnen.
7. Klicken Sie in vRA im Einrichtungsfenster des Management-Agent auf „Next“.
8. Akzeptieren Sie die EULA und klicken Sie auf Next.
9. Behalten Sie den Standardzielordner bei und klicken Sie auf „Next“.
10. Geben Sie die IP-Informationen für die vRA-Appliance, den Root-Nutzernamen und das Passwort ein.
11. Klicken Sie auf „Load“, um das Servicezertifikat für die Managementwebsite zu laden.
12. Aktivieren Sie das Kontrollkästchen, um die übereinstimmenden Fingerabdrücke zu bestätigen.
13. Klicken Sie auf „Next“.
14. Geben Sie das Passwort für das IaaS-Windows-VM-Administratorkonto ein und klicken Sie auf „Next“.
15. Klicken Sie auf „Install“.
16. Klicken Sie auf „Finish“.
17. Kehren Sie zum Webbrowser zurück, um die vRA-Konfiguration abzuschließen.

Abschließen der vRA-Konfiguration

1. Stellen Sie über den vRA-Installationsassistenten sicher, dass der IaaS-Host in der Liste angezeigt wird, und klicken Sie auf „Next“.
2. Klicken Sie auf „Run“, um die Voraussetzungsüberprüfung auszuführen.
3. Klicken Sie auf „Fix“, falls Voraussetzungen nicht erfüllt sind.
4. Klicken Sie auf „Next“, nachdem die Voraussetzungsüberprüfung mit dem Status „OK“ abgeschlossen wurde.
5. Geben Sie den DNS-Alias oder den FQDN für die vRA-Appliance ein und klicken Sie auf „Next“.
6. Geben Sie ein Passwort für das Administratorkonto ein, bestätigen Sie es und klicken Sie auf „Next“.
7. Geben Sie den DNS-Alias oder den FQDN für den IaaS-Webserver ein.
8. Geben Sie den Nutzernamen und das Passwort für den IaaS-Webserver ein.
9. Geben Sie zur Sicherheit der Datenbank eine Passphrase ein, bestätigen Sie die Passphrase und klicken Sie auf „Validate“.
10. Nach der erfolgreichen Validierung klicken Sie auf „Next“.
11. Geben Sie den Servernamen einer bestehenden SQL-Instanz ein und wählen Sie „Use existing empty database“ aus.
12. Klicken Sie auf „Next“.
13. Überprüfen Sie die DEM-Informationen und klicken Sie auf „Next“.
14. Überprüfen Sie die Informationen des Agent und klicken Sie auf „Next“.
15. Wählen Sie „Generate Certificate“ aus und geben Sie eine Organisation, eine Organisationseinheit und einen Ländercode ein.
16. Klicken Sie auf „Save Generated Certificate“.
17. Klicken Sie auf „Next“.

18. Wählen Sie „Generate Certificate“ aus und geben Sie eine Organisation, eine Organisationseinheit und einen Ländercode ein.
19. Klicken Sie auf „Save Generated Certificate“.
20. Klicken Sie auf „Next“.
21. Klicken Sie auf Validate.
22. Klicken Sie nach Abschluss der Validierung auf „Next“.
23. Erstellen Sie sämtliche gewünschten Snapshots der VMs oder Appliances und klicken Sie auf „Next“.
24. Klicken Sie auf „Install“.
25. Klicken Sie nach Abschluss der Installation auf „Next“.
26. Geben Sie den Lizenzschlüssel ein und klicken Sie auf „Next“.
27. Deaktivieren Sie das Kontrollkästchen, um nicht am Customer Experience Improvement Programm teilzunehmen, und klicken Sie auf „Next“.
28. Wählen Sie „Configure Initial Content“ aus und klicken Sie auf „Next“.
29. Geben Sie ein Passwort für das Konto des Konfigurationsadministrators ein, bestätigen Sie es und klicken Sie auf „Create Initial Content“.
30. Klicken Sie auf „Next“, nachdem die anfängliche Konfiguration von Inhalten abgeschlossen wurde.
31. Klicken Sie auf „Finish“.

Bereitstellen und Konfigurieren von vRealize Business for Cloud (vRBC)

1. Klicken Sie in vSphere Web Client mit der rechten Maustaste auf das Cluster.
2. Wählen Sie „Deploy OVF Template...“ aus.
3. Klicken Sie auf „Browse...“.
4. Navigieren Sie zur OVF-Datei und klicken Sie auf „Open“.
5. Klicken Sie auf „Next“.
6. Geben Sie einen Namen für die OVF ein und klicken Sie auf „Next“.
7. Wählen Sie eine Ressource für die OVF aus und klicken Sie auf „Next“.
8. Überprüfen Sie die Vorlagendetails und klicken Sie auf „Next“.
9. Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf „Next“.
10. Wählen Sie das Format des virtuellen Laufwerks und den Datenspeicher aus und klicken Sie auf „Next“.
11. Wählen Sie das Zielnetzwerk aus und klicken Sie auf „Next“.
12. Belassen Sie „USD“ als Standardwährung und aktivieren Sie das Kontrollkästchen, um SSH zu aktivieren.
13. Geben Sie das Root-Nutzerpasswort ein und bestätigen Sie es.
14. Erweitern Sie durch Klicken die Netzwerkeigenschaften.
15. Geben Sie Standardgateway, Domain und DNS ein.
16. Geben Sie die IP-Adresse für die VM und die Netzmaske ein und klicken Sie auf „Next“.
17. Überprüfen Sie die Konfigurationsdaten und klicken Sie auf „Finish“.
18. Schalten Sie die VM ein.
19. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://vRBC-IP:5480.`
20. Geben Sie das `Root`- und das während der Bereitstellung erstellte Passwort ein und klicken Sie auf „Log in“.
21. Geben Sie den Hostnamen von vRA, den Standardmandanten, den Administratornutzer und das Passwort ein.
22. Aktivieren Sie das Kontrollkästchen, um das Zertifikat anzunehmen, und klicken Sie auf „Register“.

Beginnen der Konfiguration des Standardmandanten mit dem ersten Einrichtungskatalogeintrag

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://vra-ip/vcac/.`
2. Melden Sie sich mit dem zuvor erstellten Passwort als `configurationadmin` an.
3. Wählen Sie „Administration“ aus.
4. Wählen Sie Nutzer und Gruppen aus.
5. Wählen Sie Verzeichnisnutzer und -gruppen aus.
6. Suchen Sie nach `configurationadmin`.
7. Wählen Sie `configurationadmin` aus.
8. Aktivieren Sie alle Kontrollkästchen, um dem Nutzer alle Rollen hinzuzufügen.
9. Klicken Sie auf „Finish“.
10. Klicken Sie auf „Logout“.
11. Klicken Sie auf „Go back to login page“.
12. Melden Sie sich als `configurationadmin` bei vRA an.
13. Wählen Sie „Catalog“ aus.
14. Klicken Sie auf „vSphere Initial Setup“.
15. Klicken Sie auf „Request“.

16. Wählen Sie „Yes“ aus, um den aktuellen Mandanten zu konfigurieren, und klicken Sie auf „Next“.
17. Geben Sie Namen, FQDN und Rechnerressource für den vSphere-Endpunkt ein.
18. Geben Sie den Nutzernamen und das Passwort für den vSphere-Endpunkt ein und klicken Sie auf „Submit“.
19. Klicken Sie auf „OK“.
20. Wählen Sie „Inbox“ aus.
21. Klicken Sie auf „Manual User Action“.
22. Wählen Sie die abzuschließende Aktion aus.
23. Klicken Sie auf „View Details“.
24. Wählen Sie die VM-Vorlagen aus, die als Katalogartikel veröffentlicht werden sollen.
25. Wählen Sie im Drop-down-Menü den Reservierungsspeicher aus.
26. Wählen Sie im Drop-Down-Menü den Ressourcenpool für die Reservierung aus.
27. Wählen Sie im Drop-down-Menü das Reservierungsnetzwerk aus.
28. Klicken Sie auf „Submit“.
29. Nachdem die Anfrage erfolgreich abgeschlossen wurde, melden Sie sich von vRA ab.

Fortsetzen der Konfiguration des Standardmandanten

1. Melden Sie sich als `configurationadmin` bei vRA an.
2. Wählen Sie „Business Management“ aus.
3. Geben Sie für das Produkt eine Seriennummer ein und klicken Sie auf „Save“.
4. Wählen Sie die Registerkarte „Infrastructure“ aus.
5. Klicken Sie auf Endpoints.
6. Klicken Sie auf Endpoints.
7. Klicken Sie auf „New“.
8. Wählen Sie „Management“ aus und klicken Sie auf „vRealize Operations Manager“.
9. Geben Sie einen Namen für den Endpunkt, die VM-Adresse, den Nutzernamen und das Passwort ein.
10. Klicken Sie auf Test Connection.
11. Klicken Sie auf „OK“, um dem Endpunkt zu vertrauen.
12. Klicken Sie auf „OK“.
13. Wählen Sie die Registerkarte „Administration“ aus.
14. Klicken Sie auf „Directories Management“.
15. Klicken Sie auf „Directories“.
16. Klicken Sie auf „Add Directory“.
17. Wählen Sie „Add Directory over LDAP/IWA“ aus.
18. Geben Sie einen Verzeichnisnamen ein.
19. Geben Sie Basis-DN, Bind DN und Bind-DN-Passwort ein und halten Sie sich dabei an das angegebene Beispielformat.
20. Klicken Sie auf Test Connection.
21. Nach einer erfolgreichen Testverbindung klicken Sie auf „Save“ und „Next“.
22. Klicken Sie auf „Next“.
23. Klicken Sie auf „Next“.
24. Wählen Sie den einzuschließenden Nutzer aus und klicken Sie auf „Next“.
25. Wählen Sie den auszuschließenden Nutzer aus und klicken Sie auf „Next“.
26. Klicken Sie auf „Sync Directory“.
27. Klicken Sie auf die Registerkarte Administration.
28. Klicken Sie auf „vRO Configuration“.
29. Klicken Sie auf Endpoints.
30. Klicken Sie auf „New“.
31. Wählen Sie „Active Directory“ aus und klicken Sie auf „Next“.
32. Geben Sie einen Namen für den Enpunkt ein und klicken Sie auf „Next“.
33. Geben Sie die IP-Adresse des Servers, die Basis-DN (DC=domain,DC=com), den Nutzernamen (DOMAIN\Administrator) und das Passwort ein.
34. Klicken Sie auf „Finish“.
35. Wählen Sie die Registerkarte „Administration“ aus.
36. Klicken Sie auf „Reclamation“.
37. Klicken Sie auf „Metrics Provider“.
38. Wählen Sie den vRealize Operations Manager-Endpunkt aus.
39. Geben Sie URL, Nutzernamen und Passwort ein.
40. Klicken Sie auf Test Connection.

41. Klicken Sie auf „Save“.
42. Klicken Sie auf „OK“, um dem Endpunkt zu vertrauen.
43. Wählen Sie „Infrastructure“ aus.
44. Klicken Sie auf „Reservations“.
45. Klicken Sie auf „Reservations“.
46. Wählen Sie die vom Blueprint „Initial Setup“ erstellte Reservierung aus.
47. Klicken Sie auf Resources.
48. Bearbeiten Sie die Reservierung nach Bedarf und klicken Sie auf „OK“.
49. Klicken Sie auf „Placement Policy“.
50. Aktivieren Sie das Kontrollkästchen, um vROM zu verwenden.
51. Klicken Sie auf „Apply“.
52. Klicken Sie zur Bestätigung auf „Yes“.

Konfigurieren von vROM-Managementpaketen

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://[IP-address-of-vROM]`.
2. Melden Sie sich als `admin` an.
3. Wählen Sie „Administration“ aus.
4. Wählen Sie den VMware vRealize Log Insight-Adapter aus.
5. Klicken Sie auf die Zahnradsymbole, um den Adapter zu konfigurieren.
6. Geben Sie einen Anzeigenamen und die IP-Adresse des vRLI-Servers ein.
7. Klicken Sie auf Test Connection.
8. Klicken Sie auf „Save settings“, nachdem die Verbindung erfolgreich hergestellt wurde.
9. Schließen Sie das Fenster.
10. Wählen Sie den VMware vRealize Business for Cloud-Adapter aus.
11. Klicken Sie auf die Zahnradsymbole, um den Adapter zu konfigurieren.
12. Geben Sie einen Anzeigenamen und die IP-Adresse des vRBC-Servers ein.
13. Klicken Sie auf Test Connection.
14. Klicken Sie auf „Save settings“, nachdem die Verbindung erfolgreich hergestellt wurde.
15. Schließen Sie das Fenster.
16. Wählen Sie den VMware vRealize Automation-Adapter aus.
17. Klicken Sie auf die Zahnradsymbole, um den Adapter zu konfigurieren.
18. Geben Sie einen Anzeigenamen und die IP-Adresse des vRA-Servers ein.
19. Klicken Sie auf das grüne Pluszeichen neben „Credential“.
20. Geben Sie einen Namen für die Berechtigung ein.
21. Geben Sie `administrator@vsphere.local` als SysAdmin-Nutzernamen und das zugehörige Passwort ein.
22. Geben Sie `configurationadmin@vsphere.local` als SuperUser-Nutzernamen und das zugehörige Passwort ein.
23. Klicken Sie auf „OK“.
24. Klicken Sie auf Test Connection.
25. Klicken Sie auf „Save settings“, nachdem die Verbindung erfolgreich hergestellt wurde.
26. Schließen Sie das Fenster.

Bereitstellen einer AWS Public Cloud

Wir haben unsere Tests mit einem kostenlosen AWS-Konto und Zugriff auf das Passwort und die Einstellungen des primären/Root-Kontos durchgeführt.

Hinzufügen zusätzlicher Policies für den Servicekatalog

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://console.aws.amazon.com.`
2. Melden Sie sich mit der E-Mail-Adresse und dem Passwort des primären Kontos an.
3. Wählen Sie im Hauptdashboard „IAM“ aus.
4. Klicken Sie auf „Create policy“, um eine ergänzende Policy für Katalogadministratoren zu erstellen.
5. Geben Sie einen Policy-Namen und eine Beschreibung ein.

6. Kopieren Sie folgenden Text in das Policy-Dokument:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateKeyPair",
                "iam:AddRoleToInstanceProfile",
                "iam:AddUserToGroup",
                "iam:AttachGroupPolicy",
                "iam:CreateAccessKey",
                "iam:CreateGroup",
                "iam:CreateInstanceProfile",
                "iam:CreateLoginProfile",
                "iam:CreateRole",
                "iam:CreateUser",
                "iam:Get*",
                "iam:List*",
                "iam:PutRolePolicy",
                "iam:UpdateAssumeRolePolicy"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

7. Klicken Sie auf „Create policy“.
8. Klicken Sie auf „Aktualisieren“.
9. Geben Sie in das Suchfeld `ServiceCatalog` ein.
10. Aktivieren Sie das Kontrollkästchen neben `ServiceCatalogAdminFullAccess` und der neu erstellten Policy.
11. Klicken Sie auf „Next: Review“.
12. Überprüfen Sie die Details und klicken Sie auf „Create user“.
13. Klicken Sie auf „Policies“, um eine ergänzende Policy für Katalognutzer zu erstellen.
14. Klicken Sie auf „Create policy“.
15. Klicken Sie auf „Select“ neben „Create Your Own Policy“.
16. Geben Sie einen Namen und eine Beschreibung ein.
17. Kopieren Sie folgenden Text in das Policy-Dokument:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicecatalog:ProvisionProduct"
            ],
            "Resource": "*"
        }
    ]
}
```

18. Klicken Sie auf „Create policy“.
19. Kehren Sie zum AWS-Dashboard zurück.
20. Wählen Sie „EC2“ aus.
21. Klicken Sie auf „Key Pairs“.
22. Klicken Sie auf „Create Key Pair“.
23. Geben Sie einen Namen für das Schlüsselpaar ein.
24. Klicken Sie auf „Create“.
25. Speichern Sie die Datei, wenn Sie dazu aufgefordert werden.

26. Kehren Sie zum AWS-Dashboard zurück.
27. Wählen Sie „Service Catalog“ aus.
28. Klicken Sie auf „Create portfolio“.
29. Geben Sie einen Namen, eine Beschreibung und einen Eigentümer ein.
30. Klicken Sie auf „Create“.
31. Klicken Sie auf „Upload new product“.
32. Geben Sie einen Produktnamen, eine Beschreibung und unter „Provided by“ einen Namen ein.
33. Klicken Sie auf „Next“.
34. Geben Sie die gewünschten Supportdetails ein und klicken Sie auf „Next“.
35. Suchen Sie die gewünschte Vorlage oder geben Sie eine S3-URL für die Vorlage ein.
36. Geben Sie einen Versionstitel und eine Beschreibung ein.
37. Klicken Sie auf „Next“.
38. Überprüfen Sie die Details und klicken Sie auf „Create“.

Konfigurieren der AWS Connector-CLI und Hochladen einer AMI-Datei

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://console.aws.amazon.com`.
2. Melden Sie sich mit der E-Mail-Adresse und dem Passwort des primären Kontos an.
3. Wählen Sie „S3“ aus.
4. Klicken Sie auf „Create Bucket“.
5. Geben Sie einen neuen Bucket-Namen ein.
6. Wählen Sie eine Region aus.
7. Klicken Sie auf „Next“.
8. Legen Sie bei Bedarf Eigenschaften für Versionierung, Protokollierung oder Tags fest.
9. Klicken Sie auf „Next“.
10. Behalten Sie die Standardberechtigungen bei und klicken Sie auf „Next“.
11. Überprüfen Sie die Einstellungen und klicken Sie auf „Create Bucket“.
12. Wählen Sie den neu erstellten Bucket aus.
13. Klicken Sie auf „Upload“.
14. Klicken Sie auf „Add files“.
15. Navigieren Sie zu den Dateien für die VM-Vorlage oder das Image.
16. Wählen Sie die Dateien aus.
17. Klicken Sie auf Öffnen.
18. Überprüfen Sie die Berechtigungen und klicken Sie auf „Next“.
19. Überprüfen Sie die Eigenschaften und klicken Sie auf „Next“.
20. Überprüfen Sie den Upload und klicken Sie auf „Upload“.
21. Klicken Sie auf den Drop-down-Pfeil neben dem Nutzernamen.
22. Klicken Sie auf „My Security Credentials“.
23. Klicken Sie auf „Access Keys“.
24. Klicken Sie auf „Download Key File“.
25. Klicken Sie auf „Save“, wenn Sie dazu aufgefordert werden.
26. Öffnen Sie ein Terminal oder ein Befehlsfenster.
27. Installieren Sie awscli, indem Sie folgenden Befehl ausführen: `pip3 install awscli --upgrade --user`
28. Überprüfen Sie, ob awscli korrekt installiert wurde, indem Sie den folgenden Befehl ausführen: `aws --version`
29. Erstellen Sie eine Datei mit dem Namen `trust-policy.json` und geben Sie Folgendes ein:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": { "Service": "vmie.amazonaws.com" },
         "Action": "sts:AssumeRole",
         "Condition": {
            "StringEquals":{
               "sts:Externalid": "vmimport"
            }
         }
      }
   ]
}
```

30. Erstellen Sie eine Datei mit dem Namen `role-policy.json` und geben Sie Folgendes ein:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
         ],
         "Resource": [
            "arn:aws:s3:::disk-image-file-bucket"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "s3:GetObject"
         ],
         "Resource": [
            "arn:aws:s3:::disk-image-file-bucket/*"
         ]
      },
      {
         "Effect": "Allow",
         "Action":[
            "ec2:ModifySnapshotAttribute",
            "ec2:CopySnapshot",
            "ec2:RegisterImage",
            "ec2:Describe*"
         ],
         "Resource": "*"
      }
   ]
}
```

31. Konfigurieren Sie die AWS-CLI, indem Sie den folgenden Befehl ausführen: `aws configure`
32. Geben Sie den AWS-Zugriffsschlüssel aus der heruntergeladenen Zugriffsschlüsseldatei ein.
33. Drücken Sie die Eingabetaste.
34. Geben Sie den geheimen AWS-Schlüssel aus der heruntergeladenen Zugriffsschlüsseldatei ein.
35. Drücken Sie die Eingabetaste.
36. Geben Sie den Namen der Standardregion ein (wir haben `us-east-1` verwendet).
37. Drücken Sie die Eingabetaste.
38. Geben Sie das Ausgabeformat ein (wir haben `json` verwendet).
39. Drücken Sie die Eingabetaste.
40. Erstellen Sie eine Rolle für den Import von VMs, indem Sie den folgenden Befehl ausführen: `aws iam create-role --role-name vmimport --assume-role-policy-document file://trust-policy.json`
41. Wenden Sie eine Policy für die erstellte Rolle an, indem Sie den folgenden Befehl ausführen: `aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-document file://role-policy.json`
42. Erstellen Sie eine Datei mit dem Namen `containers.json` und geben Sie Folgendes ein:

```
[
  {
    "Description": "UploadDescription",
    "Format": "VMDK",
    "UserBucket": {
        "S3Bucket": "name_of_bucket",
        "S3Key": "name_of_file.vmdk"
    }
}]
```

43. Importieren Sie die VM, indem Sie den folgenden Befehl ausführen: `aws ec2 import-image --description "UploadDescription" --license-type BYOL --disk-containers file://containers.json`
44. Überprüfen Sie den Fortschritt des Uploads, indem Sie den folgenden Befehl ausführen: `aws ec2 describe-import-image-tasks --import-task-ids import-ami-ID_goes_here`
45. Kehren Sie zur AWS-Webkonsole zurück.
46. Klicken Sie auf die Home-Schaltfläche.

Erstellen einer VM und einer Vorlage unter Windows 2012 R2

Erstellen der VM unter Windows 2012 R2

1. Navigieren Sie zu vSphere Web Client.
2. Melden Sie sich als `administrator@vsphere.local` an.
3. Wählen Sie „Create a new virtual machine“ aus.
4. Wählen Sie „Custom“ aus und klicken Sie auf „Next“.
5. Geben Sie einen Namen für die virtuelle Maschine ein und klicken Sie auf „Next“.
6. Wählen Sie den Host aus und klicken Sie auf Next.
7. Wählen Sie den entsprechenden Speicher aus und klicken Sie auf „Next“.
8. Wählen Sie „Windows“ und anschließend „Microsoft Windows Server 2012 R2 (64-bit)“ aus und klicken Sie auf „Next“.
9. Wählen Sie für „CPUs“ zwei virtuelle Prozessorsockel und einen Core pro virtuellem Sockel aus und klicken auf „Next“.
10. Wählen Sie „8 GB RAM“ aus und klicken Sie auf „Next“.
11. Klicken Sie für die Anzahl der NICs auf „1“. Wählen Sie „VMXNET3“ aus, stellen Sie eine Verbindung mit dem VM-Netzwerk her und klicken Sie auf „Next“.
12. Behalten Sie den standardmäßigen virtuellen Speicher-Controller bei und klicken Sie auf Next.
13. Erstellen Sie ein neues virtuelles Laufwerk, und klicken Sie auf Next.
14. Stellen Sie die Größe des virtuellen Laufwerks für das Betriebssystem auf 50 GB ein, wählen Sie thin-provisioned aus, geben Sie den Speicher an und klicken Sie auf Next.
15. Behalten Sie den standardmäßigen virtuellen Geräteknoten (0:0) bei und klicken Sie auf Next.
16. Klicken Sie auf Finish.
17. Verbinden Sie die virtuelle CD-ROM der VM mit der Installations-CD von Microsoft Windows Server 2012 R2.
18. Starten Sie die VM.
19. Klicken Sie mit der rechten Maustaste auf die VM und wählen Sie Open Console aus.
20. Klicken Sie auf dem Windows-Bildschirm zur Sprachauswahl auf Next.
21. Klicken Sie auf Install Now.
22. Geben Sie den Schlüssel ein und klicken Sie auf Next.
23. Wählen Sie Windows Server 2012 R2 Datacenter (Server mit einer GUI) aus und klicken Sie auf Next.
24. Aktivieren Sie das Kontrollkästchen „I accept the license terms“ und klicken Sie auf „Next“.
25. Klicken Sie auf Custom.
26. Klicken Sie auf „Next“.
27. Geben Sie in beiden Feldern das gewünschte Passwort für den Administrator ein und klicken Sie auf Finish.
28. Melden Sie sich in der VM an und installieren Sie VMware-Tools.
29. Legen Sie für die VM eine statische IP-Adresse fest.
30. Stellen Sie eine Verbindung mit dem Internet her und installieren Sie alle verfügbaren Windows-Updates. Führen Sie einen Neustart durch, falls erforderlich.
31. Aktivieren Sie den Remotedesktopzugriff und deaktivieren Sie Firewalls und IE-Sicherheit nach Bedarf.
32. Ändern Sie den Hostnamen, treten Sie der entsprechenden Domain bei und führen Sie einen Neustart durch, wenn Sie dazu aufgefordert werden.
33. Navigieren Sie in der neuen VM zu `https://IP-of-vra/software/index.html` und laden Sie die entsprechende Version des Windows-Gast-Agent herunter.
34. Klicken Sie auf „Save“ und speichern Sie den Gast-Agent auf dem Laufwerk „C:“.
35. Navigieren Sie zur Gast-Agent-Datei, klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie „Properties“ aus.
36. Klicken Sie auf „Unblock“.
37. Klicken Sie auf „Apply“ und dann auf „OK“.
38. Um die Datei zu extrahieren, doppelklicken Sie darauf.
39. Klicken Sie auf das Startmenü und geben Sie „RUN“ ein.
40. Geben Sie `sysprep` ein und drücken Sie die Eingabetaste.
41. Klicken Sie mit der rechten Maustaste auf „sysprep“ und wählen Sie „Run as Administrator“ aus.
42. Aktivieren Sie das Kontrollkästchen „Generalize“. Wählen Sie unter „Shutdown Options“ die Option „Reboot“ aus.
43. Nachdem die VM heruntergefahren wurde, kehren Sie zur vCenter-Webkonsole zurück und wählen die VM aus.
44. Klicken Sie mit der rechten Maustaste auf die VM, wählen Sie „Clone“ aus und klicken Sie auf „Clone to Template“.
45. Navigieren Sie im vSphere Client zur Startseite und klicken Sie auf „Customization Specifications Manager“.
46. Klicken Sie auf „New“, um eine neue Anpassungsvorlage zu erstellen.
47. Wählen Sie „Windows“ aus, benennen Sie die Gastanpassung und klicken Sie auf „Next“.
48. Geben Sie die Namen eines Eigentümers und eines Unternehmens ein und klicken Sie auf „Next“.
49. Wählen Sie „Use the virtual machine name“ aus und klicken Sie auf „Next“.
50. Geben Sie bei Bedarf einen Produktschlüssel ein oder lassen Sie das Feld leer. Klicken Sie auf „Next“.
51. Geben Sie ein Passwort für das Administratorkonto ein, bestätigen Sie es und klicken Sie auf „Next“.
52. Wählen Sie die richtige Zeitzone aus und klicken Sie auf „Next“.

53. Geben Sie bei Bedarf einen Befehl ein, der bei der ersten Anmeldung ausgeführt wird. Klicken Sie auf „Next“.
54. Wählen Sie die Standardeinstellungen für das Netzwerk aus und klicken Sie auf „Next“.
55. Wählen Sie „Windows Server Domain“ aus und geben Sie die Domaininformationen ein. Geben Sie den AD-Nutzernamen und das Passwort ein und klicken Sie auf „Next“.
56. Aktivieren Sie das Kontrollkästchen „Generate New Security ID“ und klicken Sie auf „Next“.
57. Überprüfen Sie die Zusammenfassung und klicken Sie auf „Finish“.

Exportieren der VM als OVF

1. Klicken Sie in der vCenter-Webkonsole mit der rechten Maustaste auf die VM.
2. Wählen Sie „Template“ aus und klicken Sie auf „Export OVF Template…“.
3. Geben Sie einen Namen für die OVF ein und klicken Sie auf „OK“.
4. Laden Sie für AWS-Tests die OVF gemäß den in **Konfigurieren der AWS Connector-CLI und Hochladen einer AMI-Datei** aufgeführten Schritten hoch.

VMware: Erstellen eines Blueprint in vRA

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://vra-ip/vcac/.`
2. Melden Sie sich als `configurationadmin` an.
3. Wählen Sie „Design“ und anschließend „Blueprint“ aus und klicken Sie auf „New“.
4. Geben Sie einen Namen für den Blueprint ein. Klicken Sie auf „OK“.
5. Wählen Sie im Design-Canvas „Machine Types“ aus, klicken Sie auf eine vSphere-Maschine und ziehen Sie sie auf den Canvas.
6. Wählen Sie unter „Build Informationen“ für „Action“ die Option „Clone“ aus.
7. Wählen Sie unter „Clone From“ die zuvor erstellte Vorlage aus.
8. Geben Sie in den Spezifikationen der Anpassung den Namen der Gastanpassung in vSphere ein (der Name muss exakt übereinstimmen).
9. Klicken Sie auf „Machine Resources“ und legen Sie die Minimal- und Maximalwerte für Ihre Einstellungen fest.
10. Klicken Sie auf „Storage“ und anschließend auf „New“. Fügen Sie den gewünschten Speicher hinzu und aktivieren Sie das Kontrollkästchen „Allow user to see and change storage reservation policies“.
11. Wählen Sie im Design-Canvas „Networks & Security“ aus, klicken Sie auf „Existing Network“ und ziehen Sie diese Option auf den Canvas.
12. Wählen Sie Unter „Existing Network“ das externe Netzwerk aus und klicken Sie auf „OK“.
13. Kehren Sie zur vSphere-Maschinenkonfiguration zurück und klicken Sie auf „Network“.
14. Klicken Sie auf „New“ und wählen Sie das externe Netzwerk aus. Geben Sie die gewünschte IP-Konfiguration ein.
15. Klicken Sie auf „Finish“.
16. Wählen Sie unter „Blueprints“ den erstellen Blueprint aus und klicken Sie auf „Publish“.
17. Wählen Sie „Administration“, „Catalog Management“ und dann „Services“ aus.
18. Wählen Sie den gewünschten Service aus und klicken Sie dann auf „Manage Catalog Items“.
19. Klicken Sie auf das grüne Pluszeichen.
20. Fügen Sie das Katalogelement zum Service hinzu und klicken Sie auf „OK“.

AWS: Erstellen einer CloudFormation-Vorlage

1. Melden Sie sich als Root-Nutzer bei der AWS-Webkonsole an.
2. Navigieren Sie zu `https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-sample-templates.html.`
3. Wählen Sie die entsprechende Region aus (wir haben „US East (Northern Virginia) Region“ ausgewählt).
4. Wählen Sie „Services“ aus.
5. Wählen Sie „EC2“ aus.
6. Klicken Sie für eine Amazon EC2-Instanz in einer Sicherheitsgruppe auf „View in Designer“.
7. Ändern Sie die Vorlage so, dass AWSInstanceType2Arch auf die AMI verweist, die gemäß den Schritten unter **Konfigurieren der AWS Connector-CLI und Hochladen einer AMI-Datei** hochgeladen und konvertiert wurde.
8. Klicken Sie nach der Änderung auf das Häkchen, um die Vorlage zu validieren.
9. Klicken Sie nach erfolgreicher Validierung auf das Seitensymbol und anschließend auf „Save“.
10. Speichern Sie die Vorlage entweder als lokale Datei oder im Amazon S3-Bucket.
11. Benennen Sie die Datei und klicken Sie auf „Save“.
12. Kehren Sie zur AWS-Konsole zurück.
13. Wählen Sie „Service Catalog“ aus.
14. Wählen Sie das Standardportfolio aus.
15. Klicken Sie auf „Upload new product“.
16. Geben Sie einen Namen für das Produkt, eine Beschreibung und einen Anbieter ein und klicken Sie auf „Next“.
17. Geben Sie die gewünschten Supportdetails ein und klicken Sie auf „Next“.
18. Suchen Sie nach der hochzuladenden Vorlagendatei (bei lokaler Speicherung) oder geben Sie die URL der Vorlage an, falls sie im S3-Bucket gespeichert wurde.
19. Geben Sie die Versionsdetails ein und klicken Sie auf „Next“.
20. Überprüfen Sie die Informationen und klicken Sie auf „Create“.

Erstellen von VMs und Vorlagen für den LAMP-Stack

Erstellen von VMs für den LAMP-Stack

1. Klicken Sie in der vSphere HTML5-Webkonsole mit der rechten Maustaste auf den Infrastrukturhost und wählen Sie „New Virtual Machine“ aus.
2. Klicken Sie im Assistenten „Create New Virtual Machine“ auf „Next“.
3. Geben Sie einen Namen ein, der der Rolle der virtuellen Maschine entspricht („LAMP1“, „LAMP2“ oder „loadbalancer“), stellen Sie sicher, dass der richtige Inventarort ausgewählt ist und klicken Sie auf „Next“.
4. Wählen Sie die richtige Computerressource aus und klicken Sie auf „Next“.
5. Wählen Sie den Zielspeicher für die Dateien der virtuellen Maschine aus und klicken Sie auf „Next“.
6. Setzen Sie die Kompatibilität auf „ESXi 6.5“ oder höher und klicken Sie auf „Next“.
7. Ändern Sie das Gastbetriebssystem zu Linux, wählen Sie im Drop-down-Menü „Version“ die Option „CentOS 7 (64-bit)“ aus und klicken Sie auf „Next“.
8. Wählen Sie das richtige Netzwerk und den richtigen Adapter aus und klicken Sie auf „Next“.
9. Überprüfen Sie die Einstellungsübersicht für die neue virtuelle Maschine und klicken Sie auf „Finish“.
10. Klicken Sie mit der rechten Maustaste auf die neu erstellte virtuelle Maschine und wählen Sie „Open Console“ aus. Um die virtuelle Maschine einzuschalten, klicken Sie auf das grüne Wiedergabesymbol.
11. Wiederholen Sie die Schritte 1–10 zwei weitere Male, um insgesamt drei virtuelle Maschinen mit den folgenden Namen zu erstellen: „LAMP1“, „LAMP2“ und „loadbalancer“.
12. Klicken Sie im vSphere-Konsolenemulator für die erste virtuelle Maschine auf das Schraubenschlüsselsymbol, wählen Sie „CD/DVD drive 1“ und anschließend „Connect to ISO image on local disk“ aus. Navigieren Sie zum Installationsmedium für CentOS 7 und klicken Sie auf „Open“.
13. Wenn die CentOS 7-Eingabeaufforderung angezeigt wird, wählen Sie mit den Pfeiltasten „Install CenOS 7“ aus und drücken Sie die Eingabetaste.
14. Wenn der Installationsassistent für CentOS 7 angezeigt wird, behalten Sie die Standardeinstellungen für Sprache und Tastatur bei und klicken Sie auf „Continue“.
15. Wählen Sie auf der Seite mit der Installationszusammenfassung „Software Selection“ aus.
16. Ändern Sie die Einstellung für „Base Environment“ zu „Infrastructure Server“ und klicken Sie auf „Done“.
17. Wählen Sie einen Zielort für die Installation aus.
18. Für unsere Tests haben wir die Standardeinstellungen für die Geräteauswahl und die Partitionierungsmethode beibehalten („Automatically configure partitioning“). Klicken Sie auf „Done“.
19. Wählen Sie „Network & Hostname“ aus.
20. Schalten Sie den NIC ein, stellen Sie sicher, dass eine DHCP-Adresse zugewiesen wurde, und geben Sie einen Hostnamen ein, der dem virtuellen Maschinennamen entspricht („LAMP1“, „LAMP2“ oder „loadbalancer“). Klicken Sie auf „Done“.
21. Klicken Sie auf „Installation starten“.
22. Klicken Sie während der Installation auf „Root Password“, geben Sie ein Root-Passwort ein und bestätigen Sie es.
23. Klicken Sie auf „Reboot“, wenn die Installation abgeschlossen ist.
24. Wiederholen Sie die Schritte 12–23 zwei weitere Male, um insgesamt drei CentOS 7-Installationen mit den folgenden Hostnamen zu erstellen: „LAMP1“, „LAMP2“ und „loadbalancer“.
25. Öffnen Sie eine Remotekonsolenverbindung zur ersten virtuellen Maschine und melden Sie sich mit den Root-Berechtigungen an.
26. Führen Sie den Befehl `vim /etc/sysconfig/selinux` aus, um die SELinux-Konfigurationsdatei zu öffnen.
27. Ändern Sie `SELINX=enforcing zu SELINUX=disabled`, speichern Sie die Änderungen und beenden Sie VIM.
28. Führen Sie den Befehl `yum -y update` aus, um alle Pakete zu aktualisieren.
29. Starten Sie den Server neu, wenn die Paketaktualisierungen abgeschlossen sind.
30. Wiederholen Sie die Schritte 25–29 zwei weitere Male, um SELinux zu deaktivieren und Standardpakete für alle drei virtuellen Maschinen zu aktualisieren.
31. Führen Sie über die Remotekonsolenverbindung zur virtuellen Maschine „LAMP1“ den Befehl `yum -y install httpd php mariadb-server mariadb` aus, um den Apache HTTP-Service, PHP5 und MariaDB zu installieren.
32. Führen Sie den Befehl `systemctl start httpd` aus, um den Apache HTTP-Service zu starten.
33. Führen Sie den Befehl `systemctl enable httpd` aus, um sicherzustellen, dass der Apache HTTP-Service beim Hochfahren gestartet wird.
34. Führen Sie den Befehl `systemctl start mariadb` aus, um den MariaDB-Service zu starten.
35. Führen Sie den Befehl `systemctl enable mariadb` aus, um sicherzustellen, dass der MariaDB-Service beim Hochfahren gestartet wird.
36. Führen Sie den Befehl `mysql_secure_installation` aus und befolgen Sie die Eingabeaufforderungen, um ein Root-Passwort festzulegen, anonyme Nutzer zu deaktivieren und die Testdatenbank zu entfernen.
37. Führen Sie den Befehl `mysql -u root -p` aus und melden Sie sich mit den Root-Berechtigungen an, um auf die SQL Server-Eingabeaufforderung zuzugreifen.
38. Geben Sie in die SQL-Eingabeaufforderung die folgenden Zeilen ein (Trennung durch Drücken der Eingabetaste), um die Proof-of-Concept-Datenbank zu erstellen (beim Wiederholen dieses Schritts für LAMP2 den Hostnamen entsprechend zu LAMP1 ändern). Um diesen Schritt beenden zu können, müssen Sie sich als Nutzer anmelden, der für den Remotezugriff auf die Datenbank authentifiziert ist.

```
CREATE DATABASE testdb;
USE testdb;
GRANT REPLICATION SLAVE ON *.* TO testuser@LAMP2 IDENTIFIED BY 'password';
FLUSH PRIVILEGES;
CREATE TABLE testable (testname VARCHAR(100), testnumber DOUBLE);
INSERT INTO testable VALUES ('first', 100);
INSERT INTO testable VALUES ('second', 200);
exit;
```

39. Führen Sie den Befehl `vim /etc/my.cnf` aus, um die MariaDB-Konfigurationsdatei zu öffnen.
40. Fügen Sie die folgenden Zeilen am Anfang der Datei ein (wenn Sie diesen Schritt für LAMP2 wiederholen, ändern Sie den Wert für „server-id" zu „2"):

```
server-id = 1
log_bin = /var/log/mariadb/mariad.log
binlog_do_db = testdb
```

41. Fügen Sie die folgenden Zeilen am Ende der Datei ein (wenn Sie diesen Schritt für LAMP2 wiederholen, ändern Sie den Wert für „auto-increment-offset" zu „2" und den Wert für „master-host" zu „LAMP2"):

```
replicate-same-server-id = 0
auto-increment-increment = 2
auto-increment-offset = 1
master-host = LAMP1
master-user = testuser
master-password = password
master-connect-retry = 60
replicate-do-db = testdb
```

42. Speichern Sie Änderungen und beenden Sie VIM.
43. Führen Sie den Befehl `systemctl restart mariadb` aus, um MariaDB erneut zu starten.
44. Führen Sie den Befehl `mysql –u root –p` aus und melden Sie sich mit den Root-Berechtigungen an, um auf die SQL Server-Eingabeaufforderung zuzugreifen.
45. Geben Sie in die SQL-Eingabeaufforderung die folgenden Zeilen ein (Trennung durch Drücken der Eingabetaste), um die Master-Master-Replikation zu aktivieren (wenn Sie diesen Schritt für LAMP2 wiederholen, ändern Sie den Wert für „MASTER_HOST" zu „LAMP1"):

```
CHANGE MASTER TO MASTER_HOST='LAMP2',
MASTER_USER='testuser', MASTER_PASSWORD='password',
MASTER_LOG_FILE='mariadb.log';
START SLAVE;
exit;
```

46. Wiederholen Sie die Schritte 31–45 ein weiteres Mal, um den LAMP-Stack für die virtuellen Maschinen LAMP1 und LAMP2 zu konfigurieren.
47. Führen Sie über die Remotekonsolenverbindung zur virtuellen Maschine „loadbalancer" den Befehl `yum –y install httpd php` aus, um den Apache HTTP-Service und PHP zu installieren.
48. Das Modul „mod_proxy_balancer" sollte standardmäßig installiert und aktiviert sein. Führen Sie den Befehl `vim /etc/httpd/conf/httpd.conf` aus, um Konfigurationseinstellungen für dieses Modul hinzuzufügen.
49. Fügen Sie der Datei die folgenden Informationen hinzu:

```
Allow from all

BalancerMember LAMP1
BalancerMember LAMP2

ProxyPass / balancer://mycluster
```

50. Führen Sie den Befehl `systemctl restart httpd` aus, um den Apache HTTP-Service erneut zu starten.
51. Fahren Sie alle VMs herunter.
52. Klicken Sie mit der rechten Maustaste auf eine VM, wählen Sie „Template" aus und klicken Sie auf „Convert to Template".
53. Wiederholen Sie Schritt 52 für jede VM des LAMP-Stacks.

Erstellen des Blueprint in vRA

1. Melden Sie sich als Infrastrukturadministrator bei vRA an und wählen Sie die Registerkarte „Design" aus.
2. Klicken Sie unter „Blueprints" auf „New".
3. Geben Sie auf der Registerkarte „General" den Namen, die ID, eine Beschreibung, die Archivierungstage und die Leasingtage ein und klicken Sie auf „OK".
4. Wählen Sie unter „Categories" die Option „Network and Security" aus.
5. Ziehen Sie das Symbol „Existing Network" auf den Canvas und legen Sie es dort ab.
6. Wählen Sie auf der Registerkarte „General" für das vorhandene Netzwerk die Option „External Network" aus und klicken Sie auf „OK".
7. Wählen Sie unter „Categories" die Option „Machine Types" aus.
8. Ziehen Sie eine vSphere-Maschine auf den Canvas und legen Sie sie dort ab.

9. Geben Sie auf der Registerkarte „General“ die ID, das Maschinenpräfix und die Anzahl der Instanzen an.
10. Klicken Sie auf die Registerkarte „Build Information“ und wählen Sie als Blueprint-Typ die Option „Server“, als Aktion die Option „Clone“, als Provisioning-Workflow die Option „CloneWorkflow“ sowie für „Clone from“ die entsprechende Vorlage aus.
11. Wählen Sie die Registerkarte „Network“ aus und klicken Sie auf „Next“.
12. Wählen Sie im Drop-down-Menü die Option „External Network“ aus.
13. Wählen Sie den entsprechenden Zuweisungstyp aus und klicken Sie auf „OK“.
14. Wiederholen Sie die Schritte 8–13 zwei weitere Male, um zwei weitere vSphere-Maschinen auf dem Canvas zu erstellen.
15. Klicken Sie auf „Finish“.
16. Markieren Sie den Blueprint und klicken Sie auf „Publish“.
17. Fügen Sie den Blueprint zu einem Anspruch und einem Service hinzu, um ihn zum Katalog hinzuzufügen.

Anhang C: Testverfahren

Wir begannen den Vergleich, als alle anderen Komponenten bereits konfiguriert waren, da es sich um einmalige, nicht wiederholbare Aktionen handelte. Wir haben für die AWS Public Cloud nach Bedarf kostenpflichtige, abonnementbasierte Services eingesetzt, um möglichst gleichwertige Konfigurationen zu erreichen.

Erstellen eines neuen Nutzers in einem bestehenden Mandanten

VMware

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://vra-ip/vcac/`.
2. Melden Sie sich als `administrator` an.
3. Wählen Sie den Mandanten aus, zu dem der neue Nutzer hinzugefügt werden soll.
4. Klicken Sie auf „Local users“.
5. Klicken Sie auf „New“.
6. Geben Sie für den neuen Nutzer Vor- und Nachnamen an.
7. Geben Sie für den neuen Nutzer eine E-Mail-Adresse und einen Nutzernamen ein.
8. Geben Sie für den neuen Nutzer ein Passwort ein und bestätigen Sie es.
9. Klicken Sie auf „OK“.
10. Klicken Sie auf „Finish“.
11. Klicken Sie auf „Logout“.
12. Klicken Sie auf „Go back to login page“.
13. Melden Sie sich als `configurationadmin` an.
14. Wählen Sie „Administration“ aus.
15. Klicken Sie auf „Users & Groups“.
16. Klicken Sie auf „Business Groups“.
17. Wählen Sie die zu bearbeitende Unternehmensgruppe aus.
18. Klicken Sie auf „Members“.
19. Fügen Sie das neue Mitglied zur passenden Rolle bzw. zu den passenden Rollen hinzu.
20. Klicken Sie auf „Finish“.

AWS

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://console.aws.amazon.com`.
2. Melden Sie sich mit der E-Mail-Adresse und dem Passwort des primären Kontos an.
3. Wählen Sie „IAM“ aus.
4. Klicken Sie auf „Users“.
5. Klicken Sie auf „Add user“.
6. Geben Sie einen Nutzernamen ein.
7. Wählen Sie „AWS Management Console access“ aus.
8. Wählen Sie „Custom password“ aus.
9. Geben Sie ein Passwort ein.
10. Wählen Sie aus, ob der Nutzer bei der nächsten Anmeldung ein neues Passwort erstellen muss, und klicken Sie auf „Next: Permissions“.
11. Klicken Sie auf „Copy permissions from existing user“.
12. Wählen Sie den Nutzer aus, dessen Berechtigungen kopiert werden sollen.
13. Klicken Sie auf „Next: Review“.
14. Klicken Sie auf „Create User“.
15. Kehren Sie zur Hauptkonsole zurück.
16. Wählen Sie „Service Catalog“ aus.
17. Wählen Sie das Portfolio aus, zu dem der neue Nutzer hinzugefügt werden soll.
18. Klicken Sie auf „Users, groups and roles“.
19. Klicken Sie auf „Add user, group or role“.
20. Klicken Sie auf „Users“.
21. Wählen Sie den neu erstellten Nutzer aus.
22. Klicken Sie auf „Add Access“.

Bereitstellen einer angepassten VM aus einem Katalog

VMware

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://vra-ip/vcac/org/[tenant].`
2. Melden Sie sich als Katalognutzer an.
3. Wählen Sie „Catalog“ aus.
4. Klicken Sie auf den gewünschten Katalogeintrag.
5. Klicken Sie auf „Request“.
6. Klicken Sie auf „Submit“.
7. Klicken Sie auf „OK“.

AWS-Option 1: Nutzen des Servicekatalogs

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://[service-catalog-user-IP]`.
2. Melden Sie sich als Katalognutzer an.
3. Wählen Sie „Service Catalog“ aus.
4. Klicken Sie auf das Drop-down-Menü „Service Catalog“ und anschließend auf „Dashboard“.
5. Wählen Sie das Produkt aus, das Sie starten möchten.
6. Klicken Sie auf „Launch product“.
7. Geben Sie einen Namen für das bereitgestellte Produkt ein und wählen Sie eine Version aus.
8. Klicken Sie auf „Next“.
9. Wählen Sie den Namen eines bestehenden EC2 KeyPair aus und ändern Sie bei Bedarf SSHLocation oder InstanceType.
10. Klicken Sie auf „Next“.
11. Geben Sie den Schlüssel und den Wert für ein bestehendes Tag ein.
12. Klicken Sie auf „Next“.
13. Aktivieren Sie nicht „SNS topic streaming“ und klicken Sie auf „Next“.
14. Überprüfen Sie die Konfiguration und klicken Sie auf „Launch“.

AWS-Option 2: Direktes Verwenden von EC2

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://[service-catalog-user-IP]`.
2. Melden Sie sich als EC2-Nutzer an.
3. Wählen Sie „EC2“ aus.
4. Klicken Sie auf „Launch Instance“.
5. Klicken Sie auf „My AMIs“.
6. Wählen Sie die AMI aus und klicken Sie auf „Select“.
7. Wählen Sie einen Instanztyp aus und klicken Sie auf „Next: Configure Instance Details“.
8. Ändern Sie alle gewünschten Parameter oder behalten Sie die Standardeinstellungen bei, indem Sie auf „Next: Add Storage“ klicken.
9. Ändern Sie das bereitgestellte Root-Volume, fügen Sie ein neues Volume hinzu oder behalten Sie die Standardeinstellungen bei, indem Sie auf „Next: Add Tags“ klicken.
10. Klicken Sie auf „Add Tag“.
11. Geben Sie einen Schlüssel und einen Wert ein und klicken Sie auf „Next: Security Group“.
12. Ändern Sie alle gewünschten Parameter oder behalten Sie die Standardeinstellungen bei, indem Sie auf „Review and Launch“ klicken.
13. Überprüfen Sie die Details und klicken Sie auf „Launch“.
14. Wählen Sie ein bestehendes Schlüsselpaar aus oder erstellen Sie ein neues Paar und klicken Sie auf „Launch Instance“.

Konfigurieren und Aufrechterhalten des Monitorings von Cloudvorgängen

VMware

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://[IP-address-of-vROM]`.
2. Melden Sie sich als Administrator an.
3. Überprüfen Sie den Status der Integrität, die schlechteste Integrität sowie vorgeschlagene Korrekturen für die Systeme.

AWS

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://console.aws.amazon.com`.
2. Melden Sie sich mit der E-Mail-Adresse und dem Passwort des primären Kontos an.
3. Wählen Sie „CloudWatch“ aus.
4. Klicken Sie auf „Dashboards“.
5. Wählen Sie das gewünschte Dashboard aus.
6. Überprüfen Sie die Informationen des Dashboards.

Konfigurieren und Aufrechterhalten des Monitorings von Protokolldateien

VMware

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://[IP-address-of-vRLI]`.
2. Melden Sie sich als `admin` an.
3. Überprüfen Sie die Ereignisse, Fehler und Benachrichtigungen im Dashboard.

AWS

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://console.aws.amazon.com`.
2. Melden Sie sich mit der E-Mail-Adresse und dem Passwort des primären Kontos an.
3. Wählen Sie „CloudWatch“ aus.
4. Klicken Sie auf „Logs“.
5. Wählen Sie die gewünschte Protokollgruppe aus.
6. Wählen Sie den gewünschten Protokollstream aus.
7. Überprüfen Sie die im Protokollstream angezeigten Ereignisse.

Konfigurieren von angepassten Chargeback-Berichten

VMware

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://vra-ip/vcac/.`
2. Melden Sie sich als `configurationadmin` an.
3. Wählen Sie „Business Management“ aus.
4. Klicken Sie auf „Reports“.
5. Wählen Sie den gewünschten vorkonfigurierten oder angepassten Bericht aus.
6. Klicken Sie auf „Export“.

AWS

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://console.aws.amazon.com`.
2. Melden Sie sich mit der E-Mail-Adresse und dem Passwort des primären Kontos an.
3. Klicken Sie auf den Drop-down-Pfeil neben dem Kontonamen.
4. Klicken Sie auf „My Billing Dashboard“.
5. Klicken Sie auf „Cost Explorer“.
6. Klicken Sie auf „Launch Cost Explorer“.
7. Klicken Sie auf „Reports“.
8. Wählen Sie den gewünschten vorkonfigurierten oder angepassten Bericht aus.
9. Klicken Sie auf „Download CSV“.

Konfigurieren des Capacity-Managements zur Erkennung, Vorhersage und Optimierung eines Overprovisioning von VMs

VMware

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://[IP-address-of-vROM]`.
2. Melden Sie sich als `admin` an.
3. Überprüfen Sie die vorgeschlagenen Aktionen im Dashboard.

AWS

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://console.aws.amazon.com`.
2. Melden Sie sich mit der E-Mail-Adresse und dem Passwort des primären Kontos an.
3. Auswählen eines vertrauenswürdigen Beraters
4. Überprüfen Sie die Vorschläge bezüglich Kostenoptimierung, Leistung, Sicherheit und Fehlertoleranz.

Bereitstellen eines LAMP-Stacks mit mehreren VMs

VMware

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://vra-ip/vcac/org/[tenant].`
2. Melden Sie sich als Katalognutzer bei vRA an.
3. Wählen Sie die Registerkarte „Catalog“ aus.
4. Wählen Sie „All Services“ aus.
5. Suchen Sie den Blueprint und klicken Sie auf „Request“.
6. Überprüfen Sie alle Blueprint-Komponenten und klicken Sie auf „Submit“.

AWS-Option 1: Nutzen des Servicekatalogs

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://[service-catalog-user-IP]`.
2. Melden Sie sich als Katalognutzer an.
3. Wählen Sie „Service Catalog“ aus.
4. Klicken Sie auf das Drop-down-Menü „Service Catalog“ und anschließend auf „Dashboard“.
5. Wählen Sie das Produkt aus, das Sie starten möchten.
6. Klicken Sie auf „Launch product“.
7. Geben Sie einen Namen für das bereitgestellte Produkt ein und wählen Sie eine Version aus.
8. Klicken Sie auf „Next“.
9. Wählen Sie den Namen eines bestehenden EC2 KeyPair und die gewünschten Subnetze aus und geben Sie ein Datenbankpasswort ein.
10. Wählen Sie die VPC-ID aus und geben Sie einen Datenbanknutzernamen ein.
11. Ändern Sie die gewünschten Standardwerte und klicken Sie auf „Next“.
12. Geben Sie den Schlüssel und den Wert für ein bestehendes Tag ein.
13. Klicken Sie auf „Next“.
14. Aktivieren Sie nicht „SNS topic streaming“ und klicken Sie auf „Next“.
15. Überprüfen Sie die Konfiguration und klicken Sie auf „Launch“.

AWS-Option 2: Direktes Verwenden von EC2

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://[service-catalog-user-IP]`.
2. Melden Sie sich als EC2-Nutzer an.
3. Wählen Sie „EC2“ aus.
4. Klicken Sie auf „Launch Instance“.
5. Klicken Sie auf „AWS Marketplace“.
6. Suchen Sie über das Suchfeld nach `LEMP 7 Optimized`.
7. Wählen Sie die AMI aus und klicken Sie auf „Select“.
8. Überprüfen Sie die Preisangaben und klicken Sie auf „Next“.
9. Wählen Sie einen Instanztyp aus und klicken Sie auf „Next: Configure Instance Details“.
10. Ändern Sie alle gewünschten Parameter oder behalten Sie die Standardeinstellungen bei, indem Sie auf „Next: Add Storage“ klicken.
11. Ändern Sie das bereitgestellte Root-Volume, fügen Sie ein neues Volume hinzu oder behalten Sie die Standardeinstellungen bei, indem Sie auf „Next: Add Tags“ klicken.
12. Klicken Sie auf „Add Tag“.
13. Geben Sie einen Schlüssel und einen Wert ein und klicken Sie auf „Next: Security Group“.
14. Ändern Sie alle gewünschten Parameter oder behalten Sie die Standardeinstellungen bei, indem Sie auf „Review and Launch“ klicken.
15. Überprüfen Sie die Details und klicken Sie auf „Launch“.
16. Wählen Sie ein bestehendes Schlüsselpaar aus oder erstellen Sie ein neues Paar und klicken Sie auf „Launch Instance“.

Erstellen eines Snapshot einer verwalteten VM

VMware

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://vra-ip/vcac/org/[tentant]`.
2. Melden Sie sich als Katalognutzer an.
3. Wählen Sie „Items“ aus.
4. Klicken Sie auf „Machines“.
5. Wählen Sie die gewünschte VM aus.
6. Klicken Sie auf „Actions“.
7. Klicken Sie auf „Create snapshot“.
8. Benennen Sie den Snapshot gegebenenfalls um, geben Sie eine Beschreibung ein und wählen Sie, ob Sie den Arbeitsspeicher einbeziehen möchten. Ansonsten klicken Sie auf „Submit“.
9. Klicken Sie auf „OK“.

AWS

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://[service-catalog-user-IP]`.
2. Melden Sie sich als EC2-Nutzer an.
3. Wählen Sie „EC2“ aus.
4. Wählen Sie in der Seitenleiste „Volumes“ aus.
5. Wählen Sie das gewünschte Volume aus.
6. Klicken Sie auf „Actions“ und wählen Sie „Create Snapshot“ aus.
7. Geben Sie einen Namen und eine Beschreibung für den Snapshot ein.
8. Klicken Sie auf „Create“.

Anhang D: Ergebnisse

Wir haben die mediane Zeit von drei aufeinanderfolgenden Läufen sowie die Anzahl der Schritte gemäß Zählung aus Anhang C aufgezeichnet. Da bei unseren Tests mit AWS öffentliche Netzwerke verwendet wurden, können alle Zeiten abhängig vom Netzwerkdatenverkehr leicht variieren. Zwei der Szenarien führten zu zwei ähnlichen Methoden für die Ausführung der Aufgaben in AWS, sodass wir die Zeit und die Schritte für jede Methode erfasst haben.

Wir haben die prozentuale Differenz zwischen der Anzahl der Schritte, die von jeder Cloudlösung für jede der acht von uns getesteten Managementaufgaben benötigt wurde, berechnet. Dann haben wir diese prozentualen Differenzen für alle acht Aufgaben gemittelt, wobei wir mit der niedrigsten Anzahl an Schritten gerechnet haben, mit der besagte Aufgabe ausgeführt werden konnte. Aus diesem Durchschnitt ergab sich der prozentuale Gesamtgewinn.

	Dell EMC und VMware		AWS		AWS (mit EC2)		Prozentualer Gewinn/ Verlust
	Zeit (m:s)	Schritte	Zeit (m:s)	Schritte	Zeit (m:s)	Schritte	
Erstellen eines neuen Nutzers	1:01	20	0:59	22	–	–	9,09 %
Bereitstellen einer angepassten VM	0:14	7	0:34	14	0:34	14	50,00 %
Konfigurieren des Monitorings von Vorgängen	0:10	3	0:12	6	–	–	50,00 %
Konfigurieren des Monitorings von Protokolldateien	0:07	3	0:10	7	–	–	57,14 %
Konfigurieren von angepassten Chargeback-Berichten	0:23	6	0:18	9	–	–	33,33 %
Konfigurieren des Capacity-Managements	0:08	3	0:08	4	–	–	25,00 %
Bereitstellen eines LAMP-Stacks	0:17	6	0:47	15	0:37	16	60,00 %
Erstellen eines Snapshot	0:15	9	0:12	8	–	–	-12,50 %
						Durchschnittlicher prozentualer Gewinn	34,01 %

Dieses Projekt wurde von Dell EMC in Auftrag gegeben.