Sicherheit für vCloud Director

VMware Cloud Director 9.5
vCloud Director 9.1

vmware®

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

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

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

docfeedback@vmware.com

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

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

Inhalt

Einführung

1

VMware vCloud Director ist ein flexibles System zur Bereitstellung von Cloud Computing-Diensten, das die wichtigsten Virtualisierungs- und Management-Technologien von VMware für die Unterstützung von Cloud-Umgebungen nutzt und erweitert.

Da das System im Hinblick auf Mandantenfähigkeit, Skalierbarkeit und andere Sicherheitsaspekte entwickelt und getestet wurde, kann die Art und Weise, wie es eingesetzt wird, einen erheblichen Einfluss auf die Sicherheit des Gesamtsystems haben. Dieses Dokument beschreibt einige mögliche Bedrohungen, denen das System ausgesetzt ist, sowie die Sicherheitsfunktionen des gesamten VMware-Software-Stacks und der damit verbundenen Komponenten wie z. B. Datenbanken.

Kein Leitfaden kann alle möglichen Anwendungsfälle auf Kundenseite abdecken. Jede Bereitstellung von vCloud Director kann eine eigene IT-Umgebung haben, die sich von anderen hinsichtlich Netzwerktopologie, internen Sicherheitssystemen und -standards, Kundenanforderungen und Anwendungsfällen unterscheidet. Dem Rechnung tragend beschränkt sich das Dokument auf einige allgemeine Richtlinien zur Erhöhung der Gesamtsicherheit des Systems. Gegebenenfalls werden auch speziellere Nutzungsszenarien berücksichtigt und eine auf diese Fälle zugeschnittene Orientierungshilfe gegeben. Dennoch hängen die konkreten Empfehlungen dieses Leitfadens, deren Umsetzung Sie in Betracht ziehen möchten, letztendlich von Ihrer individuellen Bereitstellungsumgebung sowie von den Bedrohungen ab, die Sie als Risiko für Ihr Unternehmen einschätzen und mindern möchten.

Bedrohungen für vCloud Director lassen sich generell zwei separaten Kategorien zuordnen: internen und externen Bedrohungen. Interne Bedrohungen betreffen in der Regel Probleme mit der Mandantenfähigkeit, während externe Bedrohungen auf die Sicherheit der gehosteten Cloud-Umgebung abzielen, aber diese Abgrenzungen sind nicht festgeschrieben. Es gibt beispielsweise interne Bedrohungen, welche die Sicherheit der Hosting-Umgebung angreifen.

Neben den Anleitungen in diesem Dokument, die Sie befolgen sollten, gibt es noch die Sicherheitshinweise unter http://www.vmware.com/security/advisories.html, deren Beachtung wir empfehlen. Über das Formular auf dieser Seite können Sie sich anmelden, um per E-Mail auf dem Laufenden gehalten zu werden. Zusätzliche Anleitungen und aktuelle Sicherheitshinweise bezüglich vCloud Director werden dort veröffentlicht.

Geltungsbereich der Empfehlungen

Die Empfehlungen in diesem Handbuch beschränken sich auf das Management von Sicherheitsproblemen, die speziell für vCloud Director relevant sind. Als Webanwendung, die auf einer Linux-Plattform gehostet wird, unterliegt vCloud Director den Gefährdungen durch Sicherheitslücken beider Kategorien, die alle an anderer Stelle dokumentiert sind.

Zudem sei daran erinnert, dass die sichere Bereitstellung von Software nur ein Teil eines umfassenden Sicherheitsprozesses ist, der physische Sicherheit, Schulung, Betriebsabläufe, Patch-Strategie, Eskalations- und Reaktionspläne, Disaster Recovery und viele andere Aspekte umfasst. Die meisten dieser ergänzenden Aspekte werden im vorliegenden Leitfaden nicht behandelt.

Bedrohungen

2

Sicherheitsbedrohungen für vCloud Director können entweder als interne Bedrohungen, die innerhalb des Systems und seiner Mandanten entstehen, oder als externe Bedrohungen, die außerhalb des Systems entstehen, kategorisiert werden. Diese letzte Kategorie umfasst Bedrohungen für die Infrastruktur, die für das Hosting einer vCloud Director-Servergruppe erstellt wurde, sowie Bedrohungen für die installierte vCloud Director-Software.

Mandantenfähigkeit und interne Bedrohungen

vCloud Director wurde entwickelt, um den Mandanten verwalteten Zugriff auf Netzwerk-, Computer- und Speicherressourcen von VMware vSphere ® zu ermöglichen. Mandantenbenutzer können sich bei vCloud Director anmelden und erhalten in der Regel die Berechtigung, virtuelle Maschinen bereitzustellen bzw. zu verwenden, Speicherplatz zu nutzen, Anwendungen auszuführen und (in begrenztem Umfang) Ressourcen mit anderen Benutzern gemeinsam zu verwenden.

Eine der wichtigsten Funktionen von vCloud Director ist, dass die meisten Ressourcen auf Systemebene – einschließlich physischer Hostinformationen wie IP-Adressen, MAC-Adressen, CPU-Typ, ESXi-Zugriff, physische Speicherorte usw. – für nicht-administrative Benutzer nicht direkt sichtbar oder zugänglich sind. Benutzer können jedoch weiterhin versuchen, Zugriff auf Informationen über die Systeminfrastruktur zu erhalten, auf der ihre cloudfähigen Anwendungen ausgeführt werden. Wenn sie dazu in der Lage wären, könnten sie in der Lage sein, Angriffe gegen die unteren Ebenen des Systems besser zu starten.

Selbst auf der Ebene der virtualisierten Ressourcen können Benutzer versuchen, ihren legitimen Zugriff zu nutzen, um unbefugten Zugriff auf Teile des Systems zu erhalten, auf die sie keinen Anspruch haben, wie beispielsweise Ressourcen, die einer anderen Organisation gehören. Sie könnten versuchen, Berechtigungen zu eskalieren, insbesondere um Zugang zu Aktionen zu erhalten, die Administratoren vorbehalten sind. Die Benutzer können auch Aktionen durchführen, die absichtlich oder unabsichtlich die allgemeine Verfügbarkeit und Leistung des Systems stören, was im Extremfall zu einem „Denial-of-Service“ für andere Benutzer führt.

Darüber hinaus gibt es in der Regel eine Vielzahl von administrativen Benutzern. Dazu gehören der Systemadministrator für eine vCloud Director-Site, Mandantenorganisationsadministratoren, Administratoren von Datenbanken und Netzwerken sowie Benutzer mit Zugriffsrechten auf ESXi, vCenter und Gastbetriebssysteme, die Verwaltungstools ausführen. Diese Benutzer haben im Vergleich zu normalen Benutzern mehr Berechtigungen und sind in der Regel direkt bei internen Systemen angemeldet. Dennoch sind ihre Berechtigungen nicht unbegrenzt. Möglicherweise besteht die Gefahr, dass auch sie eine Berechtigungseskalation durchführen oder schädliche Maßnahmen ergreifen.

Wie man sehen wird, basiert die Sicherheit, mit der vCloud Director auf diese Bedrohungen reagiert, auf der Architektur, dem Design und der Implementierung von vCloud Director, vSphere und VMware NSX® zusammen mit anderen Sicherheitssystemen und der Infrastruktur, auf der diese Systeme eingesetzt werden. Aufgrund der Flexibilität und Dynamik dieser Systeme ist es wichtig, die geltenden Sicherheitskonfigurationsrichtlinien für alle diese Komponenten zu befolgen.

Sicheres Hosting und externe Bedrohungen

Die Quellen externer Bedrohungen sind Systeme und Benutzer von außerhalb der Cloud, einschließlich des Internets, die vCloud Director über ihre APIs und Webschnittstellen (die vCloud Director-Webkonsole und das vCloud Director-Mandantenportal) angreifen, sowie der vApp-Übertragungsdienst und die VM-Remote-Konsole. Ein Remotebenutzer, der keine Zugriffsrechte auf das System hat, kann versuchen, sich als autorisierter Benutzer Zugang zu verschaffen. Authentifizierte Benutzer dieser Schnittstellen können auch als Quelle externer Bedrohungen angesehen werden, da sie versuchen können, Schwachstellen im System auszunutzen, die nicht für nicht authentifizierte Benutzer verfügbar sind.

In der Regel versuchen diese Akteure, Fehler in der Systemimplementierung oder deren Bereitstellung auszunutzen, um Informationen zu erhalten, Zugang zu Diensten zu erhalten oder einfach den Betrieb der Cloud durch Verlust der Systemverfügbarkeit oder der System- und Informationsintegrität zu stören. Wie die Beschreibung dieser Angriffe impliziert, verletzen einige dieser Angriffe die Mandantengrenzen und Hardware-Abstraktionsebenen, die vCloud Directorversucht zu erzwingen. Während der Einsatz der verschiedenen Ebenen des Systems die Abwehr dieser Bedrohungen beeinträchtigt, sind die externen Schnittstellen, einschließlich Firewalls, Router, VPNs usw., von größter Bedeutung.

Architektur und Sicherheitsfunktionen von vCloud Director

3

vCloud Director stellt VMware vSphere ® - und VMware NSX®-Infrastruktur als Dienst zur Verfügung und ermöglicht so die in einer Cloud-Umgebung erforderliche Mandantenisolation.

Eine vCloud Director-Servergruppe besteht aus einem oder mehreren Linux-Servern. Jeder Server in der Gruppe führt eine Auswahl von Diensten aus, die als vCloud Director-Zelle bezeichnet wird. Alle Zellen teilen sich eine einzige vCloud Director-Datenbank und verbinden sich mit mehreren vCenter Server-Systemen, den von ihnen verwalteten ESXi-Hosts und den NSX-Managern, die Netzwerkdienste bereitstellen.

Abbildung 3-1. vCloud Director-Architekturdiagramm

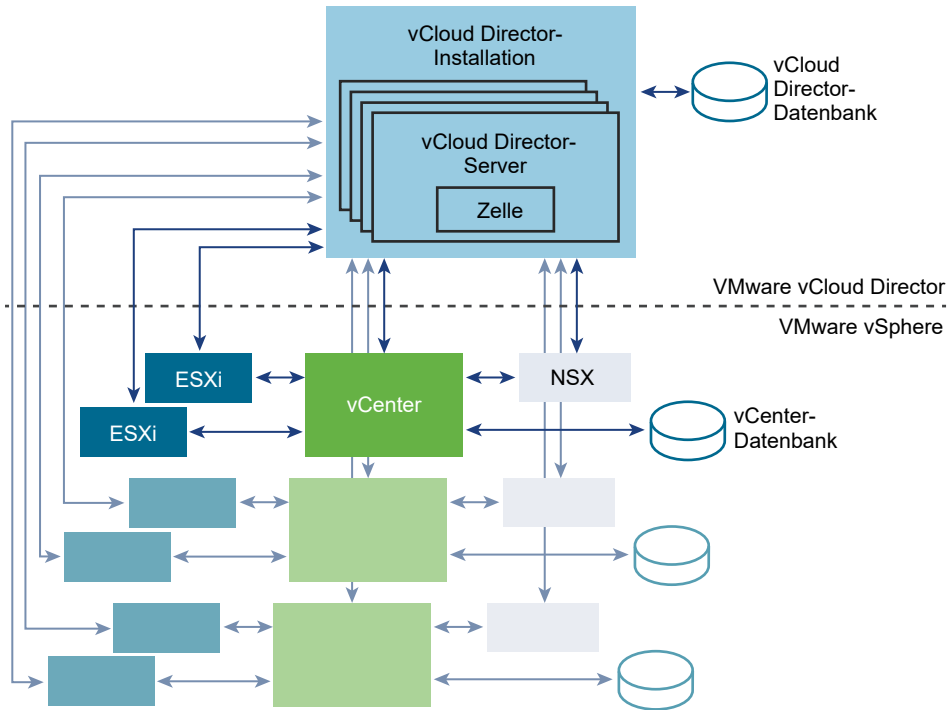


Abbildung Abbildung 3-1. vCloud Director-Architekturdiagramm zeigt eine einzelne vCloud Director-Servergruppe (Installation). Innerhalb der Servergruppe kann es viele vCloud Director-Serverhosts geben, auf denen jeweils eine einzige Zelle ausgeführt wird. Die Servergruppe teilt sich die vCloud Director-Datenbank und eine NFS-Dateifreigabe (nicht angezeigt). Die Cloud-Abstraktion basiert auf der

vCloud Director-Software und nutzt die Funktionen in vCenter und NSX, die im Diagramm als Verbindung zur Servergruppe dargestellt sind. vCloud Director-Organisationen und ihre Benutzer interagieren nicht direkt mit vCenter und NSX, um ihre Arbeitslasten zu erstellen und zu verwalten. Für andere Personen als Systemadministratoren werden alle Interaktionen mit vCenter und NSX als vCloud Director-Operationen auf vCloud Director-Objekten dargestellt. Die Berechtigung, auf vCloud Director-Objekte zuzugreifen und diese zu bearbeiten, ist rollenbasiert. Vordefinierte Rollen bieten Basiszugriff auf gängige Aufgaben. Organisationsadministratoren können zudem benutzerdefinierte Rollen erstellen, die eine Reihe von fein abgestuften Rechten nutzen.

Die nachfolgenden Unterabschnitte beschreiben die Sicherheit auf der Ebene des virtuellen Computings, der Cloud-Abstraktion und des virtuellen Netzwerks.

Dieses Kapitel enthält die folgenden Themen:

Sicherheit und Isolierung von virtuellen Maschinen

Wenn wir in diesem Dokument die Sicherheit und Netzwerkisolierung untersuchen, wollen wir das Risiko einschätzen, ob die Kontrollen für die Trennung von Netzwerken und die Isolierung von Datenverkehr unzureichend sind, und die empfohlenen Korrekturmaßnahmen auswählen.

Wenn wir uns die Netzwerksegmentierung ansehen, haben wir den Begriff einer Vertrauenszone. Vertrauenszonen sind eine proaktive Sicherheitskontrolle, um den Zugriff auf den Netzwerkverkehr zu kontrollieren. Eine Vertrauenszone wird grob als ein Netzwerksegment definiert, in dem Daten relativ frei fließen, während Daten, die in und aus der Vertrauenszone fließen, stärkeren Beschränkungen unterliegen. Beispiele für vertrauenswürdige Zonen:

- Umkreisnetzwerke (auch als demilitarisierte Zonen oder DMZ bezeichnet)
- Datenumgebung für Payment Card Industry (PCI)-Karteninhaber
- Standortspezifische Zonen, z. B. Segmentierung nach Abteilung oder Funktion
- Anwendungsdefinierte Zonen, z. B. die drei Ebenen einer Webanwendung

Sicherheit und die zugrunde liegende Virtualisierungsebene

Ein wesentlicher Teil der vCloud Director-Sicherheit, insbesondere beim Schutz der Cloud-Mandanten vor internen Bedrohungen, ergibt sich aus dem Sicherheitskonzept und der spezifischen Konfiguration der zugrunde liegenden Virtualisierungsebene. Dies umfasst den Entwurf und die Konfiguration von vSphere, die zusätzliche Sicherheit von vCloud Director softwaredefinierten Netzwerken, die Nutzung von NSX-Technologie und die Sicherheit der ESXi-Hosts selbst.

Sicherheit und die vCloud Director-Abstraktion

vSphere legt eine strikte Trennung zwischen vCloud Director-Vorgängen und den täglichen operativen Anforderungen des Mandanten fest.

Die vCloud Director-Abstraktion ermöglicht es einem Dienstanbieter, die Erstellung, Verwaltung und Nutzung von vApps an Mandantenorganisationen zu delegieren (oder an eine IT-Abteilung, die diese Funktionen an Fachabteilungen delegiert). Administratoren und Benutzer von Mandantenorganisationen arbeiten nicht mit vCenter-Funktionen wie vMotion, vSAN usw. oder verwalten diese. Mandanten beschäftigen sich ausschließlich mit der Bereitstellung ihrer Arbeitslasten (vApps) für Ressourcenpools und Speicherprofile und deren Anbindung an VDC-Netzwerke ihrer Organisation. Da sich Administratoren und Benutzer der Organisation nie bei vCenter anmelden, besteht keine Möglichkeit einer falsch konfigurierten vCenter-Berechtigung, die dem Benutzer zu viele Rechte erteilen könnte. Darüber hinaus steht es dem Anbieter frei, die Zusammensetzung der Ressourcenpools und Speicherprofile zu ändern, ohne dass die Organisation etwas ändern muss.

Noch wichtiger ist, dass diese Abstraktion verschiedene Organisationen voneinander trennt. Selbst wenn ihnen gemeinsame Netzwerke, Datenspeicher oder Ressourcenpools zugewiesen werden, können sie die vApps des anderen nicht ändern oder gar sehen. (Die Ausnahme sind vApps, die mit demselben externen Netzwerk verbunden sind, da sie denselben vSwitch verwenden.) Durch die Bereitstellung eigener dedizierter Datenspeicher, Netzwerke und Ressourcenpools für jede Mandantenorganisation, ohne dass das System dies erfordert, kann der Dienstanbieter eine noch stärkere Trennung zwischen den Organisationen erzwingen.

Einschränken des Zugriffs auf Systeminformationen für Mandanten

Obwohl das vCloud Director-System so konzipiert ist, dass es die Operationen auf Systemebene vor den Mandanten verbirgt, können bestimmte Funktionen des Systems so konfiguriert werden, dass sie Informationen liefern, die von einem böswilligen Mandanten missbraucht werden könnten.

Deaktivieren des Sendens von Host-Leistungsdaten an Gastbetriebssysteme

vSphere umfasst Leistungsindikatoren für virtuelle Maschinen auf Windows-Betriebssystemen, bei denen VMware Tools installiert ist. Standardmäßig legt vSphere gegenüber der virtuellen Gastmaschine keine Hostinformationen offen. Da Informationen über den physischen Host von einem böswilligen Mandanten missbraucht werden könnten, sollten Sie überprüfen, ob dieses Standardverhalten vorhanden ist. Detaillierte Informationen hierzu finden Sie unter Überprüfen, ob das Senden von Host-Leistungsdaten an Gastbetriebssysteme deaktiviert ist im Handbuch *vSphere-Sicherheit*.

Einschränken der Erfassung von VM-Metriken

vCloud Director kann Metriken mit aktuellen und historischen Informationen über die Leistung der virtuellen Maschine und den Ressourcenverbrauch erfassen. Da einige dieser Metriken Informationen über den physischen Host enthalten, die von einem böswilligen Mandanten missbraucht werden könnten, sollten Sie das Subsystem zum Erfassen von Metriken so

konfigurieren, dass nur solche Metriken erfasst werden, die nicht böswillig verwendet werden. Detaillierte Informationen hierzu finden Sie unter Konfigurieren der Erfassung von Metriken im Handbuch *vCloud Director-Administratorhandbuch*.

Vorsicht bei Erweiterungen

vCloud Director unterstützt eine Reihe von Erweiterungsmöglichkeiten. Während diese Methoden alle darauf abzielen, zu verhindern, dass eine Erweiterung Rechte erwirbt, die den Mandanten nicht gewährt wurden, oder die Rechte, die ihnen bei der Installation zugewiesen wurden, eskaliert, kann eine Erweiterung absichtlich oder unabsichtlich zusätzliche Angriffsflächen bieten, die jemand, der Kenntnis von der Erweiterung hat, ausnutzen könnte. Dienstanbieter und Mandantenadministratoren sollten vorsichtig sein, wenn sie Erweiterungen anbieten, überprüfen oder installieren. Darüber hinaus kann eine sorgfältige Verwaltung der erlaubten Erweiterungen und die Verwendung geeigneter Sicherheitsvorkehrungen wie dem `X-Content-Type-Options: nosniff`-Header verhindern, dass Plug-Ins schädliche Inhalte laden.

Sicherheit und die virtuelle Netzwerkebene

vCloud Director-Netzwerke nutzen die Software-Defined Networking-Funktionen von vSphere und NSX, um Mandanten einen sicheren Zugang zu gemeinsamen Netzwerkressourcen zu ermöglichen. Die Verantwortung des Dienstanbieters beschränkt sich auf die Bereitstellung externer Verbindungen und der erforderlichen Netzwerkinfrastruktur, um diese Verbindungen für die Mandanten nutzbar zu machen, sowie auf die Zuordnung von Netzwerkressourcen auf Systemebene zu Netzwerkpools, damit diese von den Mandanten genutzt werden können.

Diese Kurzübersicht über vCloud Director soll den Kontext aufzeigen, in dem wir die Anforderungen an die Vernetzung auf Anbieter- und Mandantenebene aus Sicht der Sicherheitskonfiguration diskutieren können. Diese Funktionen sind in der vCloud Director-Dokumentation unter http://docs.vmware.com detailliert beschrieben.

Netzwerkressourcen auf Anbieterebene

In der Regel ist ein Dienstanbieter dafür verantwortlich, eine oder mehrere Verbindungen zwischen vCloud Director und einem externen Netzwerk wie dem Internet oder dem Unternehmensnetzwerk eines Kunden herzustellen. Diese Art von Netzwerk ist im Wesentlichen eine Standard-IP-Netzwerkverbindung. Das Netzwerk bietet keine Vertraulichkeit, wenn Pakete auf der physischen Ebene abgefangen werden, und bietet keine VLAN- oder VXLAN-Netzwerkisolierungsfunktionen für vCloud Director.

Um Mandantenorganisationsnetzwerke zu ermöglichen, muss der Dienstanbieter einen oder mehrere Netzwerkpools erstellen, die Ressourcen von ESXi-DVswitches und Portgruppen in einer Form zusammenfassen, die den Mandantenorganisationen zur Verfügung gestellt werden kann. (Ein externes Netzwerk verbraucht keine Ressourcen aus einem Netzwerkpool.) Ein VXLAN- oder VLAN-gestützter Netzwerkpool ermöglicht die Isolierung über VLANs über einen vNetwork Distributed Switch. Ein vCloud

Director-VXLAN-Netzwerk kann auch eine Isolierung bieten, indem es Schicht-2-Pakete in andere Schicht-2-Pakete (MAC-in-MAC) im Kernel einkapselt, sodass der ESXi-Kernel beim Deaktivieren von Paketen diese an die richtigen Gast-VMs weiterleiten kann, die mit den aus dieser Art von Pool erstellten Netzwerken verbunden sind.

Der Dienstanbieter ist auch für das Erstellen und Verwalten der NSX-Infrastruktur verantwortlich, die zwischen den von den Mandanten selbst erstellten Netzwerken und den Ressourcen auf Systemebene steht, wie zum Beispiel von ESXi bereitgestellte Switches und Portgruppen. Anhand dieser Ressourcen können Mandantenorganisationen eigene Netzwerke erstellen.

VDC-Organisationsnetzwerke

Ein VDC-Organisationsnetzwerk ermöglicht es virtuellen Maschinen im Organisations-VDC, miteinander zu kommunizieren und auf andere Netzwerke zuzugreifen, einschließlich VDC-Organisationsnetzwerke und externe Netzwerke – entweder direkt oder über ein Edge-Gateway, das Firewall- und NAT-Dienste bereitstellen kann.

- Ein direktes VDC-Organisationsnetzwerk stellt eine direkte Verbindung zu einem externen Netzwerk her. Nur ein Systemadministrator kann ein direktes VDC-Organisationsnetzwerk erstellen.
- Ein geroutetes VDC-Organisationsnetzwerk stellt eine Verbindung zu einem externen Netzwerk über ein Edge-Gateway her. Für ein VDC-Organisationsnetzwerk ist es ebenfalls erforderlich, dass das VDC einen Netzwerkpool enthält. Nachdem ein Systemadministrator ein Organisations-VDC mit einem Edge-Gateway ausgestattet und mit einem Netzwerkpool verknüpft hat, können Organisationsadministratoren oder Systemadministratoren geroutete VDC-Organisationsnetzwerke in diesem VDC erstellen.
- Ein VDC-Organisationsnetzwerk einer isolierten Organisation erfordert zwar kein Edge-Gateway oder externes Netzwerk, das enthaltene VDC muss aber einem Netzwerkpool zugeordnet sein. Nachdem ein Systemadministrator ein Organisations-VDC mit einem Netzwerkpool erstellt hat, können Organisationsadministratoren oder Systemadministratoren isolierte VDC-Organisationsnetzwerke in diesem VDC erstellen.

Tabelle 3-1. Typen von VDC-Organisationsnetzwerken und ihre Voraussetzungen

VDC-Organisationsnetzwerkverbindung	Beschreibung	Voraussetzungen
Direkte Verbindung mit einem externen Netzwerk.	Bietet direkte Ebene-2-Konnektivität zu Maschinen und Netzwerken außerhalb des Organisations-VDC. Virtuelle Maschinen außerhalb dieses Organisations-VDC können direkt eine Verbindung zu den virtuellen Maschinen im VDC herstellen.	Die Cloud muss ein externes Netzwerk enthalten.
Geroutete Verbindung zu einem externen Netzwerk.	Bietet kontrollierten Zugriff auf Maschinen und Netzwerke außerhalb der Organisations-VDC über ein Edge-Gateway. Die System- und Organisationsadministratoren können das NAT-Modul und die Firewall-Einstellungen für das Gateway so konfigurieren, dass der Zugriff von einem externen Netzwerk auf bestimmte virtuelle Maschinen im VDC ermöglicht wird.	Das VDC muss ein Edge-Gateway und einen Netzwerkpool enthalten.
Keine Verbindung zu einem externen Netzwerk.	Bietet ein isoliertes, privates Netzwerk, mit dem sich Maschinen im Organisations-VDC verbinden können. Dieses Netzwerk bietet keine eingehende oder ausgehende Konnektivität für Maschinen außerhalb dieses Organisations-VDC.	Das VDC muss einen Netzwerkpool enthalten.

Standardmäßig können nur virtuelle Maschinen im Organisations-VDC, das das Netzwerk enthält, es verwenden. Wenn Sie ein VDC-Organisationsnetzwerk erstellen, können Sie angeben, dass es gemeinsam genutzt wird. Ein gemeinsames VDC-Organisationsnetzwerk kann von allen virtuellen Maschinen in der Organisation verwendet werden.

vApp-Netzwerke

Jede vApp enthält ein vApp-Netzwerk. Ein vApp-Netzwerk ist ein logisches Netzwerk, das steuert, wie die virtuellen Maschinen in einer vApp miteinander und mit VDC-Organisationsnetzwerken verbunden werden. Benutzer können vApp-Netzwerke erstellen und aktualisieren und sie mit VDC-Organisationsnetzwerken verbinden, entweder direkt oder mit NAT- und Firewall-Schutz.

Sicherheit der Infrastruktur

4

Ein Großteil dieses Leitfadens befasst sich mit dem Schutz von vCloud Director selbst. Die Sicherheit des Systems als Ganzes erfordert jedoch auch die Sicherung der Infrastruktur, von der vCloud Director abhängt und die auch die Komponenten vSphere, NSX, die Linux-Zellenplattform und die vCloud Director-Datenbank einschließt.

Die Anwendung aktueller Sicherheitspatches auf jede dieser Infrastrukturkomponenten vor der Installation ist ein wichtiger Schritt, und die laufende Überwachung dieser Komponenten ist ebenfalls entscheidend, um sie auf einem aktuellen Patch-Stand zu halten.

Sichern der VMware-Infrastruktur

Die Sicherung von vSphere und NSX ist ein wichtiger erster Schritt zur Sicherung von vCloud Director. Administratoren sollten die Checklisten unter https://www.vmware.com/security/hardening-guides.html lesen und auch die ausführlicheren Sicherheitsinformationen in den folgenden Dokumenten berücksichtigen:

Sicherheit von vSphere	*vSphere-Sicherheit*. https://docs.vmware.com/de/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html
Sicherheit von NSX	*Sichern von VMware NSX for vSphere*. https://communities.vmware.com/docs/DOC-27674 und https://communities.vmware.com/docs/DOC-28142.

Sichern der Zellenplattformen

vCloud Director-Zellen werden unter einem Linux-basierten Betriebssystem als ein nicht berechtigter Benutzer (`vcloud.vcloud`) ausgeführt, der während der Installation erstellt wurde. Die Liste der unterstützten Zellenplattform-Betriebssysteme ist in dem Dokument *vCloud Director-Versionshinweise* zu finden. Die Sicherung der Zellenplattform, ob physisch oder virtuell, ist ein wesentlicher Bestandteil der Sicherung von vCloud Director.

Auf die Zellenplattform sollten standardmäßige Sicherheitshärtungsverfahren angewendet werden, einschließlich Deaktivieren unnötiger Netzwerkdienste, Entfernen unnötiger Pakete, Einschränken des Remote-Root-Zugriffs und Durchsetzung starker Kennwortrichtlinien. Verwenden Sie nach Möglichkeit einen zentralisierten Authentifizierungsdienst wie Kerberos. Erwägen Sie die Installation von Überwachungs- und Intrusion Detection-Tools.

Sie können zusätzliche Anwendungen installieren und zusätzliche Benutzer auf der Zellenbetriebssystem-Instanz bereitstellen, dies wird jedoch nicht empfohlen. Die Erweiterung des Zugriffs auf das Zellenbetriebssystem kann die Sicherheit beeinträchtigen.

Schützen von vertraulichen Dateien nach der Installation

Während der Installation von vCloud Director werden Installationsdaten einschließlich Kennwörtern in Dateien im lokalen Dateisystem des Linux-basierten Zellen-Hosts gespeichert. Diese Dateien namens `global.properties` und `responses.properties`, die Sie unter `$ $vcloud_home/Etc` finden, enthalten vertrauliche Informationen, die Sie wiederverwenden müssen, wenn Sie weitere Server zu einer Servergruppe hinzufügen. Die Datei `responses.properties` enthält Antworten, die vom Administrator beim Ausführen des Konfigurationsskripts bereitgestellt werden. Diese Datei enthält eine verschlüsselte Version des vCloud Director-Datenbankpassworts und der Kennwörter für den System-Keystore. Nicht autorisierter Zugang zu dieser Datei kann einem Angreifer Zugriff auf die vCloud Director-Datenbank mit denselben Berechtigungen wie der im Konfigurationsskript angegebene Datenbankbenutzer gewähren. Die Datei `global.properties` enthält ebenfalls verschlüsselte Anmeldeinformationen, die nur einem Zellenadministrator zugänglich gemacht werden sollten.

Bei der Erstellung werden die Dateien `responses.properties` und `global.properties` durch Zugriffskontrollen für den Ordner `$ $vcloud_home/Etc` und die Dateien selbst geschützt. Ändern Sie nicht die Berechtigungen für die Dateien oder den Ordner, da dies dazu führen kann, dass entweder zu viel Zugriff gewährt oder der Zugriff zu stark einschränkt wird. Zu viel Zugriff verringert die Sicherheit, während eine zu starke Beschränkung die ordnungsgemäße Ausführung der vCloud Director-Software verhindert. Damit die Zugriffskontrollen ordnungsgemäß funktionieren, muss der physische und logische Zugriff auf die vCloud Director-Server strikt auf diejenigen beschränkt sein, die sich anmelden müssen und nur über die minimalen erforderlichen Zugangsberechtigungen verfügen. Dies beinhaltet die Einschränkung der Nutzung des Root-Kontos durch `sudo` und andere Best Practices, die nicht Gegenstand dieses Dokuments sind. Außerdem müssen alle Backups der Server streng geschützt und verschlüsselt sein, wobei die Schlüssel getrennt von den Backups selbst verwaltet werden müssen.

Weitere Informationen hierzu finden Sie unter Schützen und Wiederverwenden der Antwortdatei im *vCloud Director-Installations- und Upgrade-Handbuch*.

Administrative Anmeldedaten

Stellen Sie sicher, dass alle Anmeldeinformationen, die für den administrativen Zugriff auf die Zelle, vSphere, die vCloud Director-Datenbank, externe Firewalls und andere Geräte verwendet werden, den Standards für eine angemessene Kennwortkomplexität entsprechen. Erwägen Sie, wo immer möglich, die Anwendung einer Verfalls- und Rotationsrichtlinie für Kennwörter. Beachten Sie jedoch, dass ein abgelaufenes oder geändertes Datenbank-, vSphere- oder NSX--Kennwort die Cloud-Infrastruktur teilweise oder vollständig außer Funktion setzt, bis vCloud Director mit den neuen Kennwörtern aktualisiert wird.

Ein wichtiger Punkt im Sinne einer Tiefenverteidigung ist die Variation der administrativen Kennwörter für die verschiedenen Server in der vCloud Director-Umgebung einschließlich der vCloud Director-Zellen, der vCloud Director-Datenbank, der vSphere-Server und des NSX-Managers. Sie sorgt dafür, dass die Kompromittierung eines Satzes von Anmeldeinformationen (z. B. durch einen unzufriedenen Mitarbeiter, der das Unternehmen verlässt) nicht automatisch andere Systeme in der gesamten Infrastruktur gefährdet.

Weitere Informationen zur Konten- und Anmeldedatenverwaltung für Administratoren und Mandanten finden Sie unter Verwaltung von Benutzerkonten.

Dieses Kapitel enthält die folgenden Themen:

Datenbanksicherheit

Im Allgemeinen ist die Datenbanksicherheit nicht Gegenstand dieses Dokuments. Wie bei allen anderen Systemen, die in Ihrer Cloud-Bereitstellung verwendet werden, wird von Ihnen erwartet, dass Sie die vCloud Director-Datenbank gemäß branchenüblichen Best Practices ordnungsgemäß absichern.

Das vCloud Director-Datenbankbenutzerkonto sollte nur über die Systemberechtigungen verfügen, die in der entsprechenden Anleitung zur Datenbankkonfiguration im *vCloud Director-Installations- und Upgrade-Handbuch* aufgeführt sind. Benutzer der vCloud Director-Datenbank sollten keine Berechtigungen bezüglich anderer Datenbanken auf diesem Server oder sonstige Systemadministrationsberechtigungen erhalten. Dies würde das Prinzip der Mindestberechtigung auf dem Datenbankserver verletzen und dem Benutzer mehr Berechtigungen als nötig erteilen.

Es wird empfohlen, die folgenden Dokumente mit Informationen zur Datenbanksicherheit zu konsultieren.

Microsoft SQL Server	*SQL Server Security Best Practices* unter http://download.microsoft.com/download/8/f/a/8fabacd7-803e-40fc-adf8-355e7d218f4c/sql_server_2012_security_best_practice_whitepaper_apr2012.docx. **Hinweis** vCloud Director bietet keine Unterstützung für SSL-Verbindungen zu einer Microsoft SQL Server-Datenbank.
Oracle	*Oracle Database Security Guide* unter https://docs.oracle.com/cd/B28359_01/network.111/b28531.pdf. **Hinweis** vCloud Director 9.5 bietet keine Unterstützung für Oracle-Datenbanken. vCloud Director 9.1 unterstützt Oracle-Datenbanken, aber keine HTTPS- und SSL-Verbindungen zu einer Oracle-Datenbank.
PostgreSQL	Zusätzlich zur Aktivierung von SSL für PostgreSQL-Verbindungen wird empfohlen, die Dokumente zur PostgreSQL-Serververwaltung und das Dokument Total security in a PostgreSQL database von IBM developerWorks zu studieren.

Systemsicherheit

5

Der Dienstanbieter und die Systemadministratoren sind für die Sicherheit von jeder vCloud Director-Servergruppe verantwortlich.

Um eine vCloud Director-Servergruppe vor externen Angreifern zu schützen, müssen Sie die für alle webbasierten Dienste üblichen Abwehrmaßnahmen ergreifen, einschließlich der Sicherung von HTTPS-Endpoints mit signierten Zertifikaten und der Platzierung einer Web Application Firewall zwischen dem System und dem Internet. Zusätzlich müssen Sie sicherstellen, dass Sie die Dienste, von denen vCloud Director abhängig ist (einschließlich RabbitMQ AMQP-Broker und einer optionalen Apache Cassandra-Datenbank) so konfigurieren, dass die Möglichkeiten für externe Akteure, diese Systeme zu gefährden, minimiert werden.

Dieses Kapitel enthält die folgenden Themen:

Empfehlungen für die Netzwerksicherheit

Voraussetzung für den sicheren Betrieb von vCloud Director ist eine sichere Netzwerkumgebung. Konfigurieren und testen Sie diese Netzwerkumgebung, bevor Sie mit der Installation von vCloud Director beginnen.

Verbinden Sie alle vCloud Director-Server mit einem gesicherten und überwachten Netzwerk. Für die Netzwerkverbindungen von vCloud Director sind mehrere zusätzliche Anforderungen zu beachten:

- Verbinden Sie vCloud Director nicht direkt mit dem öffentlichen Internet. Schützen Sie die Netzwerkverbindungen von vCloud Director stets mit einer Firewall. Nur Port 443 (HTTPS) muss für eingehende Verbindungen geöffnet sein. Die Ports 22 (SSH) und 80 (HTTP) können bei Bedarf ebenfalls für eingehende Verbindungen geöffnet sein. Zusätzlich dazu benötigt das `cell-management-tool` Zugriff auf die Loopback-Adresse der Zelle. Der gesamte übrige eingehende Datenverkehr von einem öffentlichen Netzwerk, einschließlich der Anforderungen an JMX (Port 8999), muss von der Firewall zurückgewiesen werden.

Tabelle 5-1. Ports, die eingehende Pakete von vCloud Director-Hosts zulassen müssen

Port	Protokoll	Kommentare
111	TCP, UDP	NFS-Portmapper, vom Übertragungsdienst verwendet
920	TCP, UDP	NFS rpc.statd, vom Übertragungsdienst verwendet
61611	TCP	AMQP
61616	TCP	AMQP

- Verbinden Sie die für ausgehende Verbindungen verwendeten Ports nicht mit dem öffentlichen Netzwerk.

Tabelle 5-2. Ports, die ausgehende Pakete von vCloud Director-Hosts zulassen müssen

Port	Protokoll	Kommentare
25	TCP, UDP	SMTP
53	TCP, UDP	DNS
111	TCP, UDP	NFS-Portmapper, vom Übertragungsdienst verwendet
123	TCP, UDP	NTP
389	TCP, UDP	LDAP
443	TCP	vCenter-, NSX Manager- und ESXi-Verbindungen, die den Standardport verwenden. Wenn Sie einen anderen Port für diese Dienste ausgewählt haben, deaktivieren Sie die Verbindung mit Port 443, und aktivieren Sie diese für den von Ihnen ausgewählten Port.
514	UDP	Optional. Aktiviert die syslog-Verwendung.
902	TCP	vCenter und ESXi-Verbindungen.
903	TCP	vCenter und ESXi-Verbindungen.
920	TCP, UDP	NFS rpc.statd, vom Übertragungsdienst verwendet.
1433	TCP	Microsoft SQL Server-Standarddatenbankport.
5672	TCP, UDP	Optional. AMQP-Meldungen für Aufgabenerweiterungen.

Tabelle 5-2. Ports, die ausgehende Pakete von vCloud Director-Hosts zulassen müssen (Fortsetzung)

Port	Protokoll	Kommentare
61611	TCP	AMQP
61616	TCP	AMQP

- Leiten Sie den Datenverkehr zwischen vCloud Director-Servern und den folgenden Servern über ein dediziertes privates Netzwerk weiter.
  - vCloud Director-Datenbankserver
  - RabbitMQ
  - Cassandra
- Leiten Sie den Datenverkehr soweit möglich zwischen vSphere-Servern, NSX und vCloud Director über ein dediziertes privates Netzwerk weiter.
- Virtuelle Switches und Distributed Virtual Switches, die Provider-Netzwerke unterstützen, müssen voneinander isoliert sein. Sie können das physische Layer 2-Netzwerksegment nicht gemeinsam nutzen.
- Verwenden Sie NFSv4 für den Übertragungsdienstspeicher. Die am häufigsten verwendete NFS-Version NFSv3 bietet keine Transit-Verschlüsselung, was bei manchen Konfigurationen das Ermitteln oder Manipulieren von übertragenen Daten in Echtzeit ermöglicht. In NFSv3 vorhandene Bedrohungen werden im SANS-Whitepaper NFS Security in Both Trusted and Untrusted Environments (NFS-Sicherheit in vertrauenswürdigen und nicht vertrauenswürdigen Umgebungen) beschrieben. Weitere Informationen zum Konfigurieren und Sichern des vCloud Director-Übertragungsdiensts finden Sie im VMware-Knowledgebase-Artikel 2086127.

Zertifikate

vCloud Director verwendet HTTPS (TLS oder SSL), um den gesamten Netzwerkverkehr zu allen externen Endpunkten zu sichern. HTTPS wird auch für viele interne Endpunkte einschließlich AMQP und LDAP unterstützt. Es ist besonders wichtig, dass Sie ein von einer bekannten Zertifizierungsstelle (CA) signiertes Zertifikat für externe Endpunkte zur Verfügung stellen. Interne Endpunkte sind weniger anfällig und können in den meisten Fällen mit unternehmenseigenen oder sogar selbst signierten Systemen ausreichend gesichert werden.

Alle Zertifikate sollten ein Common Name (CN)-Feld aufweisen, das dem vollqualifizierten Domänennamen (FQDN) des Servers, auf dem sie installiert sind, entspricht. Normalerweise bedeutet dies, dass der Server beim DNS registriert ist und damit einen wohldefinierten und eindeutigen FQDN hat, und es impliziert auch, dass Sie sich mit ihm unter Verwendung des FQDN und nicht über eine IP-Adresse verbinden. Wenn Sie beabsichtigen, eine Verbindung über die IP-Adresse herzustellen, sollte das Zertifikat das Feld `subjectAltName` enthalten, dessen Inhalt der IP-Adresse des Hosts entspricht.

Weitere Informationen finden Sie in (RFC 6125) und (RFC 5280). Sie sollten auch Ihre Zertifizierungsstelle konsultieren.

Zertifikate für öffentliche Endpunkte

Endpunkte, die einem Unternehmensnetzwerk oder einem anderen öffentlichen Netzwerk wie dem Internet zugänglich sind, sollten mit einem von einer bekannten Stammzertifizierungsstelle signierten Zertifikat geschützt werden. Zu diesen Endpunkten gehören:

- die HTTPS-Adresse der Zelle und die Konsolen-Proxy-Adresse. Bei der Installation müssen Sie beide Adressen konfigurieren und deren Zertifikats- und Keystore-Details angeben.
- SSL-terminierende Lastausgleichsdienste. Weitere Informationen finden Sie unter Lastausgleichsdienste und SSL-Terminierung.

In der Regel müssen gut signierte Zertifikate nicht importiert werden, da jeder SSL-Client die Vertrauenskette bis zum Root verifizieren kann. Eingeschränkte Zertifikate (von einer Unternehmens-CA oder selbstsigniert) können auf diese Weise nicht überprüft werden. Sie wurden von Ihrem lokalen Sicherheitsteam erstellt, das Ihnen sagen kann, woher sie importiert werden sollen.

Zertifikate für private (interne) Endpunkte

Endpunkte in privaten Netzwerken, die aus öffentlichen Netzwerken nicht erreichbar sind und in der Regel speziell für die Nutzung durch vCloud Director-Komponenten wie die Datenbank und AMQP erstellt wurden, können von einer Unternehmens-CA signierte Zertifikate oder bei Bedarf sogar selbst signierte Zertifikate verwenden. Zu diesen Endpunkten gehören:

- Interne Verbindungen zu vSphere und NSX
- AMQP-Endpunkte, die vCloud Director und RabbitMQ miteinander verbinden
- PostgreSQL-Datenbankverbindungen (optional)

Ein signiertes Zertifikat verringert die Wahrscheinlichkeit, dass eine schädliche Anwendung, die es schafft, sich Zugang zu einem privaten Netzwerk zu verschaffen, sich als legitime vCloud Director-Komponente ausgeben kann.

Unterstützte Protokolle und Verschlüsselungssuiten

vCloud Director unterstützt mehrere HTTPS-Protokolle einschließlich TLS und SSL. TLS v1.0 wird standardmäßig nicht unterstützt, da es bekannte Schwachstellen aufweist. Nach der Installation können Sie mit dem Zellenverwaltungstool die Protokolle und Verschlüsselungssuiten konfigurieren, die das System für HTTPS-Verbindungen unterstützt. Weitere Informationen hierzu finden Sie in unter *vCloud Director-Versionshinweise*.

Konfigurieren von vSphere-Zertifikaten

Ab vSphere 6.0 stellt die VMware Certificate Authority (VMCA) für jeden ESXi-Host und jeden vCenter Server-Dienst ein Zertifikat bereit, das standardmäßig von VMCA signiert ist. Sie können die vorhandenen Zertifikate durch neue VMCA-signierte Zertifikate ersetzen, VMCA als untergeordnete Zertifizierungsstelle einrichten oder alle Zertifikate durch benutzerdefinierte Zertifikate ersetzen. Weitere Informationen zum Erstellen und Ersetzen von Zertifikaten, die von vCenter und ESXi genutzt werden, finden Sie unter vSphere-Sicherheitszertifikate im *vSphere-Sicherheit*-Leitfaden.

Konfigurieren von vCloud Director für die Überprüfung von vCenter-Zertifikaten

Um vCloud Director für die Überprüfung von vCenter-Zertifikaten zu konfigurieren, erstellen Sie einen Java-Keystore im JCEKS-Format, der die vertrauenswürdigen Zertifikate enthält, die zum Signieren von vCenter-Zertifikaten verwendet werden. (Zertifikate für die einzelnen vCenter-Server sind nicht in diesem Speicher - nur die CA-Zertifikate, die zu ihrer Signierung verwendet werden.)

Ein Befehl wie dieser importiert ein PEM-verschlüsseltes Zertifikat aus `/tmp/cacert.pem` in einen Keystore namens `myca.ks`:

```
$ keytool –import –alias default –keystore myca.ks –file /tmp/cacert.pem –storepass password –
storetype JCEKS
```

Ein Befehl wie dieser fügt ein weiteres Zertifikat (in diesem Beispiel `/tmp/cacert2.pem`) zum selben Keystore hinzu:

```
$ keytool –importcert–keystore myca.ks –storepass password –file /tmp/cacert2.pem –storetype JCEKS
```

Nachdem Sie den Keystore erstellt haben, melden Sie sich als Systemadministrator bei vCloud Director an. Klicken Sie im Abschnitt **Systemeinstellungen** auf der Registerkarte **Administration** auf **Allgemein** und navigieren Sie zum Ende der Seite.

Wählen Sie **vCenter- und vSphere SSO-Zertifikate überprüfen** und **NSX Manager-Zertifikate überprüfen** aus. Klicken Sie auf die Schaltfläche **Durchsuchen**, um nach Ihrem Java-Keystore zu suchen, und klicken Sie dann auf **Öffnen**. Geben Sie das Keystore-Kennwort ein und klicken Sie auf **Übernehmen**.

Nach dem Abschluss des Vorgangs werden Ihre vertrauenswürdigen Zertifikate und andere Informationen zur vCloud Director-Datenbank hochgeladen. Sie müssen den Vorgang also nur einmal für alle Zellen durchführen.

Sobald diese Option aktiviert ist, werden alle vCenter- und NSX -Manager-Zertifikate überprüft, so dass jeder vCenter- und NSX-Manager über eine korrekte Zertifikatskette und ein Zertifikat verfügen muss, das seinem FQDN entspricht. Ist diese Bedingung nicht erfüllt, schlagen Verbindungen zu vCenter und NSX fehl.

Wichtig Wenn Sie Zertifikate geändert haben, nachdem Sie vCenter-Server und NSX-Manager zu vCloud Director hinzugefügt haben, müssen Sie eine erneute Verbindung zu den Servern erzwingen.

Aktualisieren von Zertifikaten und Schlüsseln für vCloud Director-Zellen

Jeder vCloud Director-Server benötigt zwei SSL-Zertifikate in einer Java-Keystore-Datei: eines für den HTTP- und eines für den Konsolen-Proxy-Dienst. Sie müssen den Pfadnamen für diese Keystores bei der Installation von vCloud Director bereitstellen. Signierte Zertifikate bieten die höchste Vertrauensebene.

Mit dem Befehl `certificates` im Zellenverwaltungstool wird der Vorgang zum Ersetzen der vorhandenen Zertifikate durch neue Zertifikate automatisiert. Verwenden Sie den Befehl `certificates`, um selbstsignierte Zertifikate durch signierte Zertifikate oder ablaufende Zertifikate durch neue Zertifikate zu ersetzen. Informationen zum Erstellen eines JCEKS-Keystores, der signierte Zertifikate enthält, finden Sie unter Erstellen und Importieren eines signierten SSL-Zertifikats im *vCloud Director-Installations- und Upgrade-Handbuch*.

Verwenden Sie einen Befehl im folgenden Format, um SSL-Zertifikate für einen oder beide Endpoints zu ersetzen:

```
cell-management-tool certificates Optionen
```

Weitere Informationen finden Sie unter Ersetzen von Zertifikaten für die HTTP- und Konsolen-Proxy-Endpunkte im *vCloud Director-Administratorhandbuch*.

Firewalls

vCloud Director-Zellen müssen für Mandanten und Systemadministratoren zugänglich sein, die in der Regel von außerhalb des Netzwerkperimeters des Dienstanbieters darauf zugreifen. Der empfohlene Ansatz zur Bereitstellung von vCloud Director-Diensten für die Außenwelt besteht darin, eine Webanwendungs-Firewall zwischen dem Internet (oder einem anderen Unternehmensnetzwerk) und jedem öffentlichen vCloud Director-Endpunkt zu platzieren.

Netzwerk-Firewalls segmentieren physische und/oder virtuelle Netzwerke so, dass nur ein begrenzter, klar definierter Datenverkehr unter Verwendung bestimmter Ports und Protokolle zwischen ihnen hindurchgeht. Dieses Dokument erläutert nicht die allgemeinen Gründe für den Einsatz von Firewalls oder die Details der Firewall-Einrichtung. Diese Themen sind nicht Gegenstand dieses Leitfadens. In diesem Leitfaden wird vielmehr erklärt, wo Netzwerk-Firewalls in Bezug auf die verschiedenen Komponenten einer vCloud Director-Bereitstellung platziert werden sollten.

Hinweis Administrative Verbindungen können über IP-Adressbeschränkungen im Netzwerk oder auf einzelne Mandanten-VPNs bezogen weiter eingeschränkt werden. Dieses Schutzniveau kann bei bestimmten Bereitstellungen angemessen sein, ist aber nicht Gegenstand dieses Dokuments.

Da sich die vCloud Director-Zellen in der DMZ befinden, sollte ihr Zugriff auf die benötigten Dienste auch über eine Netzwerk-Firewall vermittelt werden. Insbesondere wird empfohlen, den Zugriff auf die vCloud Director-Datenbank, vCenter Server, die ESXi-Hosts, AMQP und alle Backup- oder ähnlichen Dienste auf ein internes Netzwerk zu beschränken, das von der öffentlichen Seite der Firewall aus nicht erreichbar ist. Unter Empfehlungen für die Netzwerksicherheit finden Sie eine Liste der Ports, die in dieser Firewall geöffnet sein müssen.

Blockieren von bösartigem Datenverkehr

Eine Reihe von Firewall-Regeln wird empfohlen, um das System vor Netzwerkbedrohungen zu schützen:

- Verwerfen von Paketen, die scheinbar von nicht routingfähigen Adressen stammen (IP-Spoofing)
- Verwerfen von fehlerhaften TCP-Paketen

- Begrenzung der Anzahl von Anfragen, insbesondere von SYN-Anfragen - zum Schutz vor einem SYN-Flood-Angriff (einem versuchten Denial-of-Service)
- Erwägen Sie, ausgehenden Datenverkehr der Firewall abzulehnen, sofern er nicht von einer eingehenden Anfrage stammt.

Diese und andere Regeln werden typischerweise von Webanwendungs-Firewalls angewendet und können standardmäßig von der Netzwerk-Firewall angewendet werden, die Sie bereitstellen möchten. In der Dokumentation zu Ihrer Firewall finden Sie genaue Konfigurationsanweisungen und Standardfunktionen.

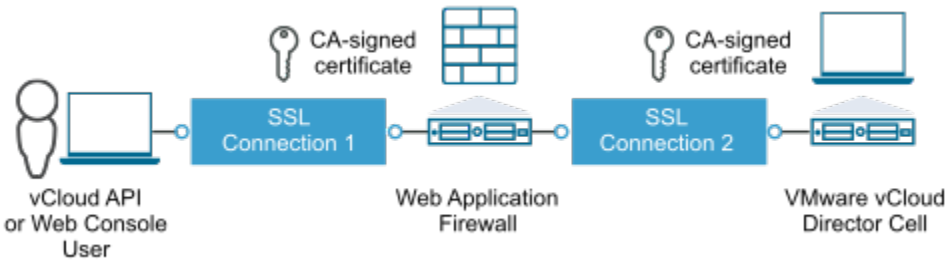
Lastausgleichsdienste und SSL-Termininierung

Sie sollten öffentliche vCloud Director-Endpoints mit einer Web Application Firewall (WAF) schützen. In Verbindung mit einem Lastausgleichsdienst konfigurieren Sie die WAF so, dass die Überprüfung und Blockierung von bösartigem Datenverkehr ermöglicht wird, indem Sie die HTTPS-Verbindung an der WAF beenden, sodass die WAF den Handshake mit ihrem eigenen Zertifikat abschließen und akzeptable Anforderungen an die Zelle mit einem `X-Forwarded-For`-Header weiterleiten kann.

Clientanforderungen an vCloud Director müssen für einen HTTPS-Endpoint vorgenommen werden. (Eine HTTP-Verbindung zur Zelle wird unterstützt, ist aber nicht sicher.) Selbst wenn die Kommunikation zwischen dem Remoteclient und der WAF mit HTTPS gesichert sind, ist es erforderlich, dass auch die WAF-Zelle-Kommunikation über HTTPS ausgeführt wird.

Das folgende einfache Diagramm, in dem der Lastausgleichsdienst nicht aufgeführt ist, veranschaulicht die beiden TLS- oder SSL-Verbindungen, die bei Verwendung von TLS- oder SSL-Terminierung vorhanden sind. Dabei handelt es sich um eine Verbindung zwischen dem Computer des Benutzers und dem WAF und eine Verbindung zwischen der Firewall und der vCloud Director-Zelle.

Abbildung 5-1. TLS/SSL-Konfiguration mit WAF



TLS/SSL-Beendigung und Zertifikate

Bei der Konfiguration der TLS- oder SSL-Terminierung ist es wichtig, nicht nur ein CA-signiertes Zertifikat auf der WAF zu installieren, damit Clientanwendungen wie die vCloud-API und die Webkonsole von der Identität des Servers überzeugt sind, sondern auch ein CA-signiertes Zertifikat für die Zellen zu verwenden, obwohl diese nur von der WAF gesehen werden. Selbstsignierte Zertifikate sind, selbst wenn

sie von der WAF akzeptiert werden, nur angemessen, wenn jedes Zertifikat manuell zum Zeitpunkt der Bereitstellung akzeptiert wird. Dies beschränkt jedoch die Flexibilität der vCloud Director-Servergruppe, da jede Zelle manuell konfiguriert werden muss (und neu konfiguriert werden muss, wenn Zertifikate erneuert werden).

Wenn der Lastausgleichsdienst unabhängig von der WAF ist, sollte auch er ein CA-signiertes Zertifikat verwenden. Verfahren zum Hinzufügen von Zertifikatskettenpfaden für Lastausgleichsdienst-Endpoints sind im Abschnitt Öffentliche Endpunkte anpassen in *vCloud Director-Administratorhandbuch*dokumentiert.

X-Forwarded-For-Header

`X-Forwarded-For` ist ein weit verbreiteter Header, der von vielen Proxys und Firewalls unterstützt. Es wird empfohlen, die Generierung dieses Headers wenn möglich an der Firewall zu aktivieren.

Wenn eine Firewall vor einer Zelle vorhanden ist, fragt die Zelle möglicherweise die IP-Adresse des Clients ab, um diese zu protokollieren. In der Regel bezieht Sie aber stattdessen die Adresse der Firewall. Wenn der `X-Forwarded-For`-Header allerdings in der Anforderung vorhanden ist, die die Zelle erhält, protokolliert er diese Adresse als die Clientadresse und die Firewalladresse als separates `proxyAddress`-Feld im Protokoll.

Sicherung von AMQP (RabbitMQ)

AMQP (Advanced Message Queuing Protocol) ist ein offener Standard für Nachrichtenwarteschlangen, der flexible Messaging-Funktionen für Unternehmenssysteme unterstützt. vCloud Director verwendet den AMQP-Broker RabbitMQ zum Bereitstellen des Nachrichtenbusses, der von Erweiterungsdiensten, Objekterweiterungen und Benachrichtigungen über blockierende Aufgaben verwendet wird.

An RabbitMQ veröffentlichte Nachrichten enthalten vertrauliche Informationen. Der AMQP-Datenverkehr zwischen vCloud Director-Zellen kann eine Sicherheitsbedrohung für das System und seine Mandanten darstellen. AMQP-Endpunkte sollten für die Verwendung von SSL konfiguriert werden. AMQP-Ports sollten in der System-Firewall blockiert werden. Drittanbieter-Clients, die AMQP-Nachrichten verbrauchen, muss die Ausführung in der DMZ gestattet werden. Jeder Code, der vCloud Director-Nachrichten verbraucht, sollte vom Sicherheitsteam des Dienstanbieters überprüft werden.

Weitere Informationen zu RabbitMQ und seiner Arbeitsweise in Verbindung mit vCloud Director finden Sie im vCat-SP-Blog unter https://blogs.vmware.com/vcat/2015/08/vcloud-director-for-service-providers-vcd-sp-and-rabbitmq-security.html

Schützen des AMQP-Dienstes mit SSL

Um SSL in Verbindung mit dem AMQP-Dienst von vCloud Director zu verwenden, müssen Sie die Option **SSL verwenden** im Abschnitt **AMQP Broker-Einstellungen** auf der Seite **Erweiterbarkeit** der vCloud Director-Webkonsole auswählen und eine der beiden folgenden Angaben machen:

- den Pfadnamen eines SSL-Zertifikats
- den Pfadnamen, den Benutzernamen und das Kennwort für einen JCEKS-Truststore

Das vollständige Verfahren ist unter Konfigurieren eines AMQP Brokers im *vCloud Director-Administratorhandbuch* beschrieben.

Wichtig Obwohl die Option **Alle Zertifikate akzeptieren** verfügbar ist, sollten Sie diese nicht auswählen, wenn es um Sicherheit geht. Die Annahme aller Zertifikate ohne Überprüfung öffnet den Weg für Man-in-the-middle-Angriffe.

Blockieren von AMQP-Ports in der System-Firewall

Wie unter Empfehlungen für die Netzwerksicherheit beschrieben, müssen mehrere AMQP-Ports im Verwaltungsnetzwerk zugänglich sein. AMQP-Endpunkte sollten von öffentlichen Netzwerken oder Unternehmensnetzwerken aus nicht zugänglich sein.

Sichern von Cassandra (VM-Metrikendatenbank)

Cassandra ist eine Open Source-Datenbank, die Sie verwenden können, um den zugrunde liegenden Speicher für eine skalierbare, leistungsfähige Lösung zur Erfassung von Zeitreihendaten (z. B. Metriken für virtuelle Maschinen) bereitzustellen. Daten, die an den Cassandra-Cluster gesendet und dort gespeichert werden, können vertraulich sein und sollten geschützt werden.

Ihre Cassandra-Infrastruktur sollte nicht nur in einem dedizierten Verwaltungsnetzwerk platziert sein, sondern auch mit SSL gesichert werden.

Aktivieren der Client-Knoten-Verschlüsselung von Cassandra

Auf der Cassandra-Seite Client-to-node encryption (Client-Knoten-Verschlüsselung) finden Sie Informationen zum Installieren von SSL-Zertifikaten und zum Aktivieren der Verschlüsselung.

Wir empfehlen die Verwendung von Zertifikaten, die von einer bekannten Zertifizierungsstelle signiert wurden. Wenn Sie dies tun, ist keine zusätzliche Konfiguration in vCloud Director erforderlich. Wenn Sie selbstsignierte Zertifikate verwenden, müssen Sie sie manuell in vCloud Director Director importieren. Verwenden Sie den Befehl `import-trusted-certificates` des Zellenverwaltungstools. Erläuterungen hierzu finden Sie unter Importieren von SSL-Zertifikaten aus externen Diensten im Handbuch *vCloud Director-Administratorhandbuch*.

Sichern des Zugriffs auf JMX

Wie im *vCloud Director-Administratorhandbuch* beschrieben, macht jede vCloud Director-Zelle eine Reihe von MBeans über JMX öffentlich verfügbar, über die die technische Verwaltung des Servers und der Zugriff auf interne Statistiken erfolgt. Da diese Schnittstelle vertrauliche Informationen über das laufende System preisgeben und dessen Betrieb beeinflussen kann, ist es unerlässlich, dass der Zugriff auf JMX streng kontrolliert wird.

JMX-Authentifizierung

Der Zugriff auf die JMX-Schnittstelle kann nur über vCloud Director-Systemadministratoren erfolgen, die sich bei JMX mit denselben Anmeldedaten wie für den Zugriff auf vCloud Director authentifizieren müssen. Diese Funktion ist nicht konfigurierbar.

Einschränken von Verbindungen zu JMX

Da JMX eine Verwaltungsschnittstelle ist, die nur für Systemadministratoren gedacht ist, gibt es keinen Grund dafür, dass sie außerhalb des vCloud Director-Verwaltungsnetzwerks eingesetzt wird. Wenn das System über eine dritte IP-Adresse verfügt, die ausschließlich für die Verwaltung vergeben wird, binden Sie JMX direkt an diese IP-Adresse. Standardmäßig wird der vCloud Director-JMX-Connector an die bei der Systemkonfiguration angegebene primäre IP-Adresse gebunden. Sie können diese Standardeinstellung außer Kraft setzen, indem Sie die folgende Eigenschaft in `/opt/vmware/vcloud-service-director/etc/global.properties` einfügen:

```
vcloud.cell.ip.management=IP-Adresse oder Hostname für das Verwaltungsnetzwerk, an das der JMX-Connector gebunden werden soll
```

Die sicherste Konfiguration bindet den JMX-Connector an die localhost-Adresse:

```
vcloud.cell.ip.management=127.0.0.1
```

Unabhängig von den verwendeten Routing- und Firewall-Geräten sollten die diesem Verwaltungsnetzwerk zugewiesenen IP-Adressen und der JMX-Port (Standardeinstellung = 8999) nicht die Netzwerkgrenze zu den Internet- oder Organisationsbenutzern überschreiten dürfen.

Mit dieser Einstellung in `global.properties` kann JMX nur vom lokalen vCloud Director-System erreicht werden. Unabhängig von der Routing-Konfiguration des Netzwerks kann keine externe Verbindung zum JMX-Port hergestellt werden.

Sichern der JMX-Kommunikation

Wenn JMX nur für die localhost-Adresse (`127.0.0.1`) verfügbar ist, können Sie die JMX-Kommunikation durch die Verwendung von SSH als Tunneling-Mechanismus für jeden Zugriff auf JMX sichern.

Wenn Ihre Verwaltungsanforderungen die Verwendung dieser Konfiguration nicht zulassen und JMX außerhalb der vCloud Director-Zelle verfügbar gemacht werden muss, dann sollte JMX mit HTTPS gesichert werden. Legen Sie hierfür die folgende Umgebungsvariable fest:

```
# export VCLOUD_JAVA_OPTS="-Dcom.sun.management.jmxremote.ssl=true \
-Djavax.net.keyStore=pathTokeystore \
-Djavax.net.sll.keyStorePassword=password \
-Djavax.net.ssl.keyStoreType=storeType"
```

Im Anschluss daran muss vCloud Director neu gestartet werden.

JMX-Clients müssen sich nun mit HTTPS verbinden, aber sie müssen Zugriff auf das Zertifikat der Zertifizierungsstelle haben. Beispielsweise sollten Sie für `jconsole` das Zertifikat der Zertifizierungsstelle in einen Keystore auf der Maschine importieren, auf der `jconsole` ausgeführt werden soll. Starten Sie dann `jconsole` mit den folgenden Befehlszeilenargumenten:

```
# jconsole –J–Djavax.net.ssl.trustStoreType=store type \
–J–Djavax.net.ssl.trustStore=pathTokeystore \
–J–Djavax.net.ssl.trustStorePassword=password
```

Selbstsignierte Zertifikate (nicht für eine Bereitstellung in einer Produktionsumgebung empfohlen) würden diesen Prozess erschweren, da Sie jedes selbstsignierte Zertifikat in einem Keystore auf der Maschine benötigen würden, auf der der JMX-Client ausgeführt wird. Die Verwendung der von der Zertifizierungsstelle signierten Zertifikate ist einfacher hier, da auf dem JMX-Clientcomputer nur das Zertifikat einer Zertifizierungsstelle erforderlich ist.

Konfiguration des Verwaltungsnetzwerks

Das vCloud Director-Verwaltungsnetzwerk ist ein privates Netzwerk, das in der Cloud-Infrastruktur eingesetzt wird und Zugriff für Clientsysteme bietet, die zum Ausführen von Verwaltungsfunktionen in vCloud Director verwendet werden.

Mit dem Verwaltungsnetzwerk verbundene Systeme beinhalten den vCloud Director-Datenbankserver, einen NFS-Server für Übertragungsspeicher, die vCenter-Server, ein optionales LDAPv3-Verzeichnis für die Authentifizierung von Anbieter-Administratoren, alle vom Anbieter für die Authentifizierung von Organisationsbenutzern verwalteten LDAPv3-Verzeichnisse sowie NSX-Manager. Die vCenter-Server in diesem Netzwerk benötigen auch Zugriff auf ihre eigenen Active Directory-Server.

Anforderungen an die Konfiguration des Verwaltungsnetzwerks in der virtuellen Infrastruktur

Es ist wichtig, das Verwaltungsnetzwerk von den VM-Datennetzwerken getrennt sind. Dies ist sogar noch wichtiger in einer Cloud-Umgebung, in der die Anbieter und Mandanten aus separaten Organisationen stammen. Es ist nicht ratsam, das Verwaltungsnetzwerk des Anbieters nicht für Angriffe aus den vApps der Organisationen zu öffnen. Ebenso muss das Verwaltungsnetzwerk von der DMZ getrennt sein, das den Zugriff für Organisationsadministratoren ermöglicht. Auch wenn sie auf die gleichen Schnittstellen wie die Systemadministratoren der Anbieter zugreifen, ist das Konzept der DMZ wichtig, um den öffentlichen und den privaten Datenverkehr zu segmentieren und zu schützen.

Aus Sicht der physischen Konnektivität muss das Datennetzwerk der virtuellen Maschine vom Verwaltungsnetzwerk getrennt sein. Dies ist die einzige Möglichkeit, Verwaltungssysteme vor böswilligen virtuellen Maschinen zu schützen. Ebenso sind die vCloud Director-Zellen physisch in der DMZ vorhanden. Im Diagramm für die physische Bereitstellung werden die Server im Verwaltungs-Pod, die sich mit den Cloud-Pods verbinden, über ein separates physisches Netzwerk verbunden, und bestimmte Firewall-Regeln lassen diesen Datenverkehr passieren.

Die interne Firewall, die vCenter- und vCloud Director-Verbindungen zu vSphere (und anderen Netzwerken) vermittelt, ist aus Sicht der Netzwerkarchitektur erforderlich. Dabei geht es nicht darum, ob sich verschiedene virtuelle Maschinen auf einem einzigen Host sowohl mit einer DMZ als auch mit einem privaten Netzwerk verbinden können. Es gibt stattdessen virtuelle Maschinen in diesem Verwaltungs-Pod, die Cloud-Zellen, die selbst eine Verbindung mit beiden Netzwerken herstellen. Die vCloud Director-Software wurde in Anlehnung an die Richtlinie für Produktsicherheit von VMware und unter Berücksichtigung der Sicherheitsanforderungen entwickelt und implementiert, sie ist jedoch keine Firewall und sollte daher nicht allein den Datenverkehr zwischen der DMZ und den privaten Verwaltungsnetzwerken vermitteln. Dies ist die Rolle der Firewall.

Andere verbundene Netzwerke

Wie aus den physischen und logischen Bereitstellungsdiagrammen hervorgeht, sind auch die Speichernetzwerke physisch getrennt. Dies resultiert aus den Best Practices von vSphere und schützt Mandanten und Speicheranbieter vor bösartigen virtuellen Maschinen. Gleiches gilt für das Sicherungsnetzwerk. Technisch gesehen ist es ein Zweig des Verwaltungsnetzwerks. Seine spezifischen Anforderungen und dessen Konfiguration hängen von der Sicherungssoftware und der verwendeten Konfiguration ab.

vMotion ist nicht immer in einem vom Verwaltungsnetzwerk separaten Netzwerk platziert; in der Cloud ist es jedoch aus Sicht der Aufgabentrennung wichtig. vMotion ist in der Regel unverschlüsselt, und bei einem Einsatz im Verwaltungsnetzwerk kann ein Anbieter-Administrator oder ein anderer Benutzer mit Zugriff auf dieses Netzwerk den vMotion-Datenverkehr „ausspionieren“ und somit die Privatsphäre von Organisationen verletzen. Aus diesem Grund sollten Sie ein separates physisches Netzwerk für die vMotion-basierte Migration von Cloud-Arbeitslasten erstellen.

Überwachung und Protokollierung

Die Möglichkeit zum Aufzeichnen und Überwachen der Aktivitäten von Benutzern ist ein wichtiger Bestandteil der Systemsicherheit insgesamt. Die meisten Unternehmen haben Regeln, die bestimmen, wer auf Software und zugehörige Hardwareressourcen zugreifen und Änderungen vornehmen darf. Das Pflegen eines Überwachungsprotokolls wichtiger Aktivitäten ermöglicht es dem Unternehmen, die Einhaltung von Regeln zu überprüfen, Verstöße zu erkennen und Gegenmaßnahmen zu ergreifen. Einige Unternehmen unterliegen externen Gesetzen und Vorschriften, die eine laufende Überwachung und Überprüfung der Zugangs- und Autorisierungsregeln verlangen.

Ein Überwachungsprotokoll kann auch hilfreich sein, um Versuche aufzuspüren, ob erfolgreich oder nicht, unrechtmäßigen Zugriff auf das System zu erlangen, seine Daten zu durchsuchen oder seinen Betrieb zu beeinträchtigen. Zu wissen, dass ein Angriff versucht wurde, und die Details des Versuchs können helfen, den Schaden zu mindern und zukünftige Angriffe zu verhindern.

Unabhängig davon, ob es erforderlich ist oder nicht, gehört es zur guten Sicherheitspraxis, Protokolle regelmäßig auf verdächtige, ungewöhnliche oder nicht autorisierte Aktivitäten zu untersuchen. Die routinemäßige Protokollanalyse hilft auch, Systemfehlkonfigurationen und -ausfälle zu erkennen und die Einhaltung von SLAs sicherzustellen.

vCloud Director umfasst zwei Arten von Protokollen:

Diagnoseprotokolle	Diagnoseprotokolle werden im Protokollverzeichnis jeder Zelle gepflegt. Diese Protokolle können für die Problembehebung nützlich sein, sind aber nicht dazu gedacht, einen Überwachungspfad der wesentlichen Systeminteraktionen zu erhalten. Jede vCloud Director-Zelle erstellt mehrere Diagnoseprotokolldateien, die unter Anzeigen der vCloud Director-Protokolle im *vCloud Director-Administratorhandbuch* beschrieben sind.
Überwachungsprotokolle	Überwachungsprotokolle zeichnen wichtige Aktionen auf, einschließlich An- und Abmeldevorgängen. Das Systemüberwachungsprotokoll wird in der vCloud Director-Datenbank verwaltet und kann über die Web-Benutzeroberfläche überwacht werden. Jeder Organisationsadministrator und der Systemadministrator haben Einblick in das Protokoll, das auf ihren speziellen Zuständigkeitsbereich zugeschnitten ist.

Für die Pflege dieses und anderer vCloud Director-Protokolle wird die Verwendung des Dienstprogramms `syslog` empfohlen. Darüber hinaus sollten Sie die Verwendung von vRealize Log Insight in Betracht ziehen, das die Remote-Erfassung anderer Protokolle wie z. B. Anforderungsprotokolle unterstützt, die nicht auf `log4j` basieren.

Verwendung von Syslog mit vCloud Director

Wie im *vCloud Director-Installations- und Upgrade-Handbuch* beschrieben, kann während der Installation ein `syslog`-Server eingerichtet werden. Der Export von Protokollen auf einen `syslog`-Server wird aus mehreren Gründen empfohlen:

- Datenbankprotokolle werden nicht länger als 90 Tage aufbewahrt, während per `syslog` übermittelte Protokolle beliebig lange aufbewahrt werden können.
- Er ermöglicht es, Überwachungsprotokolle von allen Zellen gleichzeitig an zentraler Stelle einzusehen.
- Zudem schützt er vor dem Verlust von Überwachungsprotokollen auf dem lokalen System aufgrund von Ausfällen, Speicherplatzmangel, Manipulation usw.
- Er unterstützt diagnostische Operationen bei Problemen wie den oben genannten.
- Er ist die Methode, mit der sich viele Protokollverwaltungs- und Security Information and Event Management (SIEM)-Systeme in vCloud Director integrieren lassen. Das ermöglicht
  - die Korrelation von Ereignissen und Aktivitäten zwischen vCloud Director, vSphere und NSX und sogar den physikalischen Hardware-Layern des Stacks, sowie
  - die Integration von Cloud-Sicherheitsvorgängen in die übrigen Sicherheitsvorgänge des Cloud-Anbieters oder Unternehmens, die sich über physische, virtuelle und Cloud-Infrastrukturen erstrecken.
- Die Anmeldung bei einem anderen externen System als dem, auf dem die Zelle bereitgestellt wird, verhindert Manipulationen an den Protokollen. Ein manipuliertes Verhalten der Zelle ermöglicht nicht notwendigerweise den Zugriff auf das Überwachungsprotokoll oder dessen Manipulation.

Wenn Sie bei der Erstinstallation kein `syslog`-Ziel für die Protokollierung eingerichtet haben, können Sie es später konfigurieren, indem Sie zu jeder Zelle gehen, die Datei `$VCLOUD_HOME/etc/global.properties` entsprechend bearbeiten und die Zelle neu starten.

Unter Empfehlungen für die Netzwerksicherheit finden Sie eine Liste der Ports, die vom vCloud Director-Host zum `syslog`-Server geöffnet bleiben müssen. Die Konfigurationsdetails des `syslog`-Servers sind systemspezifisch und nicht Gegenstand dieses Dokuments. Es wird empfohlen, den `syslog`-Server redundant zu konfigurieren, um sicherzustellen, dass wichtige Ereignisse stets protokolliert werden.

Die obige Diskussion bezieht sich nur auf das Senden des Überwachungsprotokolls an einen `syslog`-Server. Die Sicherheitsvorgänge und der IT-Betrieb von Organisationen können ebenfalls von der erwähnten zentralen Zusammenführung und Verwaltung der Diagnoseprotokolle profitieren. Es gibt eine Vielzahl von Methoden zum Sammeln dieser Protokolle, einschließlich der Planung eines Jobs zum periodischen Kopieren an einen zentralen Speicherort, dem Einrichten eines weiteren Loggers in der Datei `log4j.properties` (`$VCLOUD_HOME/etc/log4j.properties`) auf einem zentralen Syslog-Server oder der Verwendung eines Protokollsammlungsprogramms wie vRealize Log Insight zum Überwachen und Kopieren der Protokolldateien an einen zentralen Speicherort. Die Konfiguration dieser Optionen hängt davon ab, welches System Sie in Ihrer Umgebung bevorzugt verwenden, und ist daher nicht Gegenstand dieses Dokuments.

Wichtig Wir empfehlen die Verwendung einer TLS-fähigen `syslog`-Infrastruktur. Das `syslog`-Standardprotokoll (UDP) bietet weder eine Verschlüsselung während der Übertragung noch eine Übertragungskontrolle bzw. -bestätigung. Ohne Verschlüsselung sind die Protokolldaten leichter auszuspionieren (die in den Protokollen enthaltenen Informationen könnten zudem für weitere Angriffe verwendet werden), und die fehlende Übertragungskontrolle könnte es einem Angreifer ermöglichen, die Protokolldaten zu manipulieren. Weitere Informationen hierzu finden Sie in Abschnitt 4 von RFC 5426.

Diagnoseprotokollierung und Protokoll-Rollover

Die Protokolldatei der Jetty-Anforderungen (*`$vcloud_home/Logs/Yyyy_mm_dd.`* `request.log`) wird vom Jetty (HTTP)-Server programmgesteuert kontrolliert, unterliegt aber keiner Größenbeschränkung. Es besteht daher das Risiko eines unbegrenzten Wachstums der Protokolldatei. Für jede von Jetty bediente HTTP-Anfrage wird der aktuellen Datei ein Protokolleintrag hinzugefügt. Aus diesem Grund wird die Verwendung von `logrotate` oder ähnlichen Methoden empfohlen, um die Größe von Protokollen und die Anzahl alter Protokolldateien zu steuern.

Die anderen Diagnoseprotokolldateien sind auf insgesamt 400 MB begrenzt. Stellen Sie sicher, dass Sie genügend freien Speicherplatz haben, um diese Dateien und die Jetty-Anforderungsprotokolle in der von Ihnen erlaubten Größe unterzubringen. Wie bereits erwähnt, sorgt die zentrale Protokollierung dafür, dass Sie keine wertvollen Diagnoseinformationen verlieren, wenn die Gesamtgröße der Protokolldateien von 400 MB erreicht wird und Dateien rotiert und gelöscht werden.

NTP und Protokolle

Das *vCloud Director-Installations- und Upgrade-Handbuch* identifiziert NTP als Voraussetzung für alle vCloud Director-Zellen. Ein Nebeneffekt der Verwendung von NTP ist, dass Protokollmeldungen aus allen Zellen synchronisierte Zeitstempel aufweisen. Sicherlich verwenden Protokollverwaltungstools und SIEM-Systeme eigene Zeitstempel, um Protokolle aus verschiedenen Quellen zu koordinieren, aber diese Zeitstempel beziehen sich auf den Empfang der Meldungen von diesen Systemen und nicht auf den Zeitpunkt, zu dem ein Ereignis ursprünglich protokolliert wurde.

Weitere Protokolle

Andere Systeme, die mit vCloud Director verbunden sind und von ihm genutzt werden, erstellen Überwachungsprotokolle, die in Ihren Überwachungsprozessen konsolidiert werden sollten. Dazu gehören Protokolle von NSX Manager, der vCloud Director-Datenbank, von vCenter Server und vSphere-Hosts. Die Details zu den Protokolldateien der einzelnen Systeme und deren Zweck sind nicht Gegenstand dieses Dokuments und können der Dokumentation zu diesen Produkten entnommen werden.

Mandantensicherheit

6

Der Dienstanbieter, die Systemadministratoren und die Organisationsadministratoren sind für die Sicherheit jeder vCloud Director-Mandantenorganisation verantwortlich.

Die Absicherung einer vCloud Director-Mandantenorganisation vor externen Angriffen ist weitgehend eine Frage der Sicherheit auf Systemebene, sodass externe Angreifer nicht auf Mandantenressourcen zugreifen können. Der Dienstanbieter muss sich auch der Möglichkeit bewusst sein, dass ein Mandant einen anderen angreifen oder einfach stören kann. Mögliche Angriffsvektoren zwischen den einzelnen Mandanten sind z. B. das Ausspionieren von Details über Computing-, Speicher- und Netzwerkressourcen auf Systemebene. Absichtliche oder unabsichtliche Störungen entstehen, wenn die Systemressourcen von den Mandanten gemeinsam verwendet werden (die gegenseitig misstrauisch sein können) und es einem Mandanten gelingt, genügend dieser Ressourcen zu verbrauchen, um anderen Mandanten den erwarteten Servicelevel zu verweigern. Diese Situation wird häufig als das „lauter Nachbar“-Problem bezeichnet.

Wie in Kapitel 3 Architektur und Sicherheitsfunktionen von vCloud Director beschrieben, ist vCloud Director so konzipiert, dass eine transparente Aufteilung der Systemressourcen unter einer großen Anzahl von Mandanten möglich ist. Im Allgemeinen steht es einem Dienstanbieter frei, Systemressourcen so einzusetzen, dass die Systemeffizienz maximiert und das Ausfallrisiko minimiert wird. Wann immer Ressourcen von Mandantenorganisationen gemeinsam verwendet werden, sollte der Dienstanbieter überlegen, wie sich eine solche Aufteilung auf verschiedene Vorgänge von Mandanten auswirken könnte und ob sie Angriffe zwischen den einzelnen Mandanten ermöglichen könnte.

Dieses Kapitel enthält die folgenden Themen:

- Netzwerksicherheit für Mandantenorganisationen
- Zuteilen und Isolieren von Systemressourcen
- Verwaltung von Benutzerkonten

Netzwerksicherheit für Mandantenorganisationen

Obwohl vCloud Director-Organisationen für ihre eigene Netzwerksicherheit verantwortlich sind, sollte der Dienstanbieter externe Netzwerke mit einer Firewall schützen.

Innerhalb des vCloud Director-Systems erzwingen VXLAN- und VLAN-Netzwerke eine Trennung des Paketdatenverkehrs, die dem entspricht, was mit separaten physischen Netzwerken erreicht werden kann. Darüber hinaus bieten sie eine Reihe von Routing- und Firewall-Optionen, mit denen Unternehmen den Zugriff auf ihre Arbeitslasten von externen Systemen und innerhalb des Unternehmens genau steuern können. Diese Funktionen sind in der vCloud Director-Dokumentation unter http://docs.vmware.com detailliert beschrieben. In den meisten Fällen muss ein Dienstanbieter, der einen effektiven Schutz für das System selbst entwickelt hat (einschließlich einer Web Application Firewall, SSL-terminierenden Lastausgleichsdiensten und ordnungsgemäß signierten digitalen Zertifikaten), keine aktive Rolle bei der Einrichtung oder Aufrechterhaltung der Sicherheit von VDC-Organisationsnetzwerken übernehmen.

Externer Zugriff auf die Mandantenarbeitslasten

Beim Konfigurieren des Zugriffs auf Organisationsarbeitslasten (vApps) aus dem Internet oder einem Unternehmensnetzwerk muss der Dienstanbieter die Firewallanforderungen für die von vCloud Directorbereitgestellte und verwendete vSphere-Infrastruktur beachten. Höchstwahrscheinlich benötigen einige vApps entweder Zugriff auf das Internet oder müssen remote aufgerufen werden, sei es über RDP, SSH usw. für die Verwaltung oder über HTTP oder andere Protokolle für Endbenutzer dieser Dienste. Aus diesem Grund werden zwei verschiedene Datennetzwerke für virtuelle Maschinen empfohlen (wie in den Architekturdiagrammen in Zuteilen und Isolieren von Systemressourcen dargestellt) für unterschiedliche Anwendungen, die jeweils einen Netzwerk-Firewallschutz erfordern.

Virtuelle Maschinen, die Zugriff von außerhalb der Cloud benötigen (z. B. aus dem Internet), werden entweder mit einem öffentlichen Netzwerk oder einem privaten NAT-Routing-Netzwerk mit Portweiterleitung für die exponierten Dienste verbunden. Für das externe Netzwerk, mit dem diese VDC-Organisationsnetzwerke verbunden sind, wäre eine schützende Firewall erforderlich, für die der vereinbarte Datenverkehr zu dieser DMZ zulässig ist. Das heißt, der Dienstanbieter sollte sicherstellen, dass nicht jeder Port und jedes Protokoll eine Verbindung zur externen DMZ aufbauen darf. Gleichzeitig muss sichergestellt werden, dass genügend Datenverkehr zugelassen wird, damit die vApps der Organisationen die Dienste bereitstellen können, für die sie bestimmt sind. Dies beinhaltet typischerweise Port 80/TCP und Port 443/TCP, kann aber auch zusätzliche Ports und Protokolle beinhalten. Der Dienstanbieter muss festlegen, wie dieses Gleichgewicht am besten erreicht werden kann, wobei er sich darüber im Klaren sein muss, dass aus Sicherheitsgründen unnötige Ports und Protokolle blockiert werden sollten.

Im Allgemeinen wird empfohlen, dass vApps, die Zugang zum und vom Internet benötigen, mit einem gerouteten VDC-Organisationsnetzwerk verbunden werden, das so konfiguriert ist, dass es nur die erforderlichen eingehenden und ausgehenden Verbindungstypen zulässt. Dadurch erhält die Organisation Kontrolle über die NSX-Firewall- und Portweiterleitungsregeln. Bei einer solchen Konfiguration ist es nach wie vor notwendig, dass eine Netzwerk-Firewall das von diesen VDC-Organisationsnetzwerken verwendete externe Netzwerk trennt, da öffentliche VDC-Organisationsnetzwerke keinen vCloud Director-Firewallschutz haben. Die separate Firewall ist erforderlich, um eine DMZ zu erstellen (diese Funktion könnte jedoch durch eine separate NSX-Edge-Instanz ausgeführt werden).

In ähnlicher Weise wird ein privates VDC-Organisationsnetzwerk mit NAT-Routing für ein Datennetzwerk einer virtuellen Maschine verwendet, das virtuellen Maschinen den Zugriff auf das Internet ermöglicht. Wie bereits erwähnt, stellt ein NSX-Edge die NAT- und Firewall-Funktionen für dieses interne VM-Datennetzwerk bereit. Auch hier sollte sich der externe Netzwerkteil dieses gerouteten Netzwerks in der DMZ befinden, sodass eine separate Netzwerk-Firewall die DMZ von der Internetverbindung selbst trennt.

Zuteilen und Isolieren von Systemressourcen

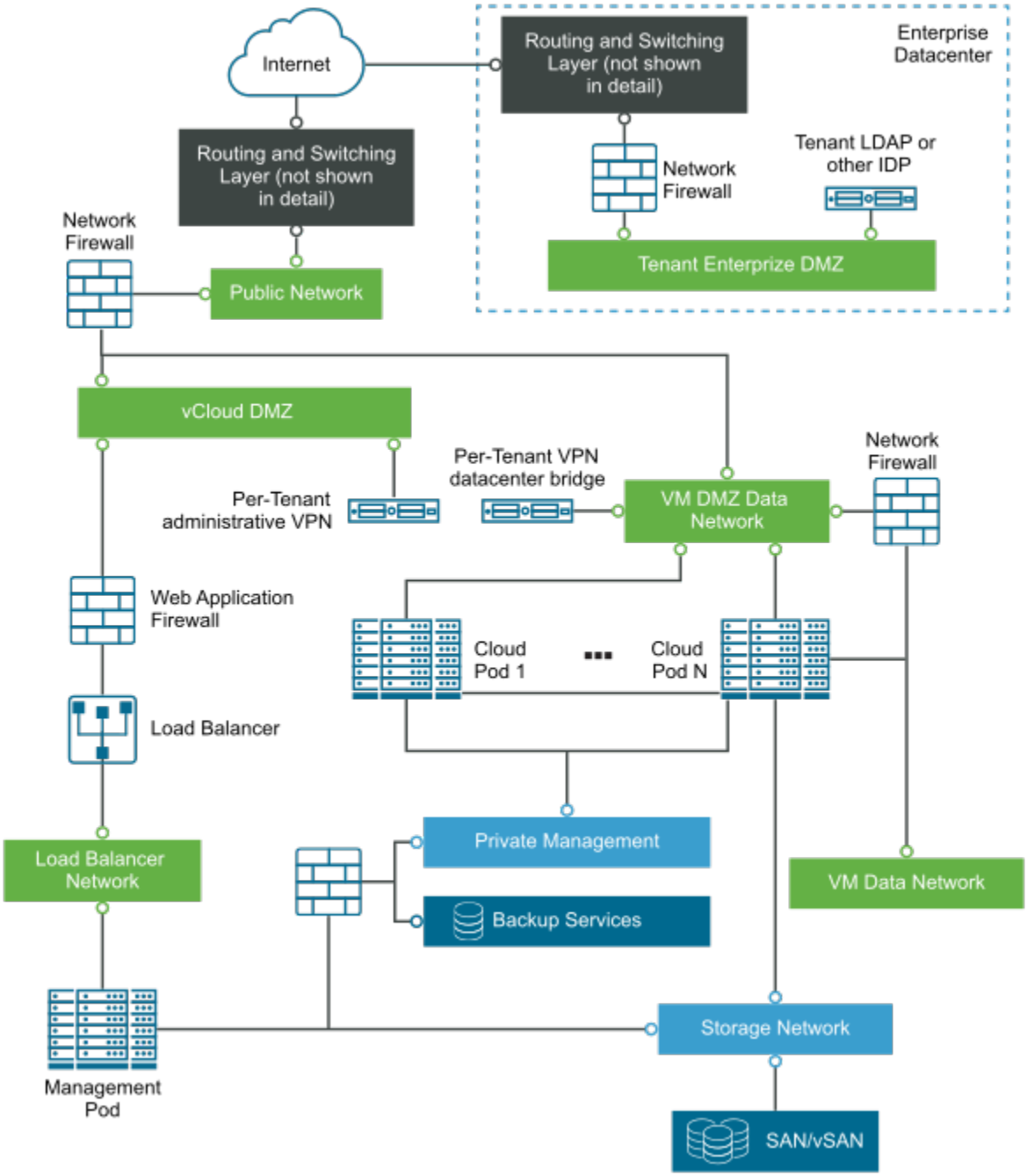
Die standardmäßige Bereitstellung von vCloud Director durch Dienstanbieter sieht die gemeinsame Nutzung von vSphere-Ressourcen durch mehrere Mandantenorganisationen vor. Dies bietet den Organisationen ein Höchstmaß an Flexibilität und dem Anbieter eine maximale Auslastung der bereitgestellten Computing-, Netzwerk- und Speicherressourcen. Beispiele für logische und physikalische Bereitstellungsdiagramme finden Sie weiter unten.

Der Rest dieses Unterabschnitts beschreibt die Komponenten auf hohem Niveau, während die folgenden Unterabschnitte spezifische Empfehlungen bezüglich der Ressourcenpools, Datenspeicher, Netzwerke und der Konfiguration anderer Komponenten beschreiben.

Bereitstellung gemeinsam genutzter Ressourcen

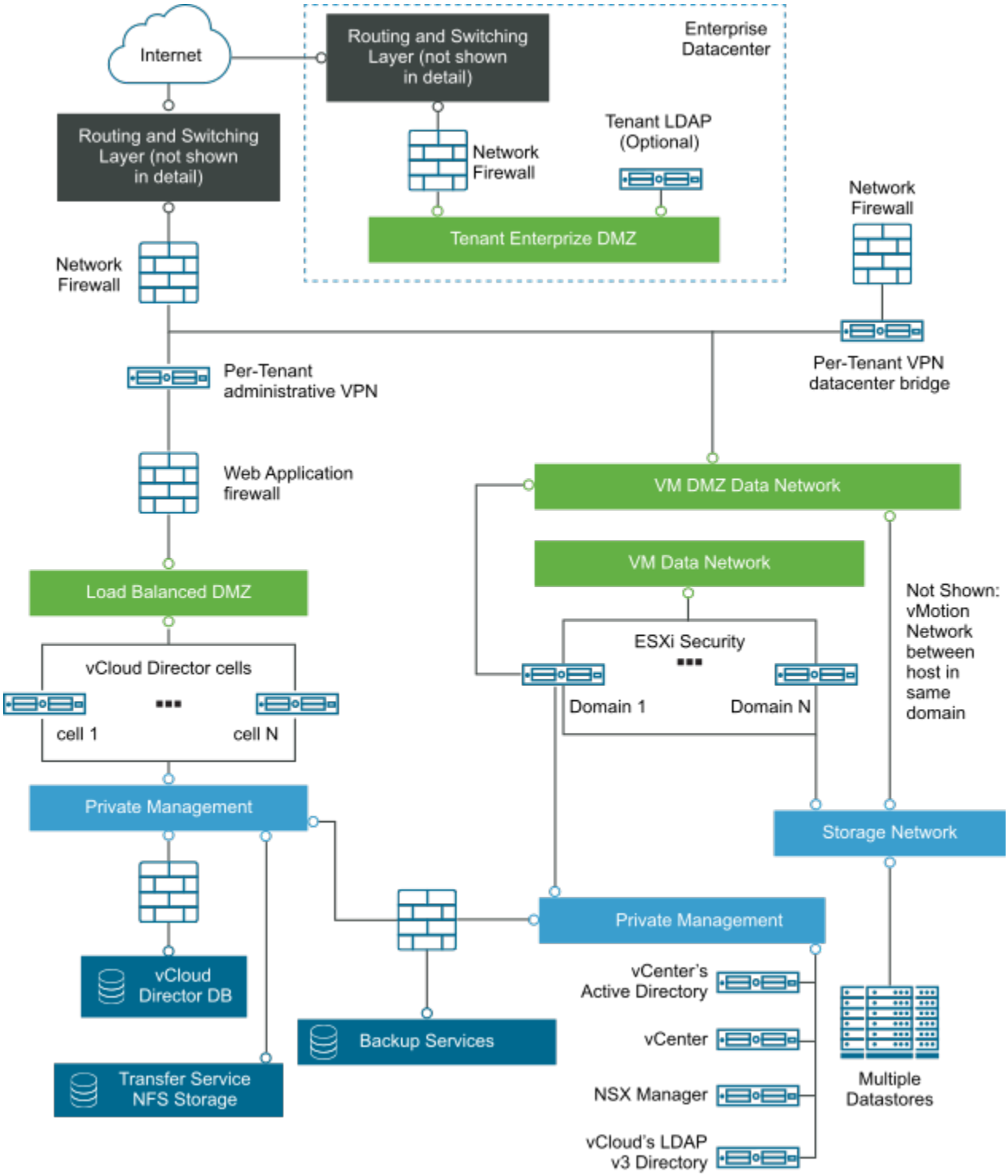
Abbildung 6-1. Diagramm für physische Bereitstellung und Abbildung 6-2. Diagramm für logische Bereitstellung sind zwei Ansichten derselben vCloud Director-Installation. In diesen Abbildungen verwenden wir den Begriff „Pod“, um eine Gruppe von Ressourcen (physische oder virtuelle Maschinen) zu bezeichnen, die entweder der Systemverwaltung („Verwaltungs-Pod“) oder den Arbeitslasten der Mandanten („Cloud-Pod“) gewidmet sind.

Abbildung 6-1. Diagramm für physische Bereitstellung



Bei der Betrachtung von Abbildung 6-2. Diagramm für logische Bereitstellung zeigt die linke Seite die vCloud Director-Zellen in einer DMZ mit Lastausgleich. Die DMZ enthält auch eine WAF und optional ein administratives VPN pro Mandant. Dieses VPN kann von einem Dienstanbieter für jede Organisation so konfiguriert werden, dass die Benutzer und IP-Adressen, die auf die über die WAF zugänglichen Dienste zugreifen können, strenger eingeschränkt werden. Darüber hinaus kann ein Mandant ein VPN konfigurieren, um seine lokalen Arbeitslasten und Daten mit VMs in der Cloud zu verbinden. Die Konfiguration solcher VPNs ist nicht Gegenstand dieses Dokuments.

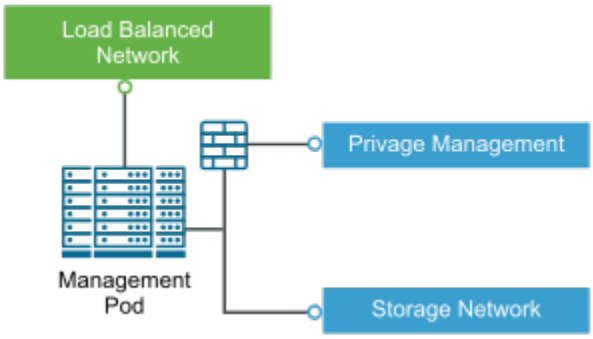
Abbildung 6-2. Diagramm für logische Bereitstellung



Hinter den Zellen befinden sich die von vCloud Director benötigten privaten Verwaltungselemente. Dazu zählen vCenter, NSX, die vCloud Director-Datenbank usw. Ihre Verbindungen werden durch die Firewalls im Diagramm streng kontrolliert, da diese Dienste nicht von anderen Maschinen in der DMZ oder direkt aus dem Internet erreichbar sein sollten.

Der Fokus in der Abbildung Abbildung 6-3. Verwaltungs-Pod-Netzwerke liegt ausschließlich auf dem Verwaltungs-Pod. Sie zeigt, dass mindestens zwei, wenn nicht sogar drei getrennte physische Netzwerke benötigt werden, die mit diesem Pod verbunden sind. Dazu gehören die DMZ mit Lastausgleich, das private Verwaltungsnetzwerk und ein optionales dediziertes Speichernetzwerk mit einer anbieterspezifischen Konfiguration.

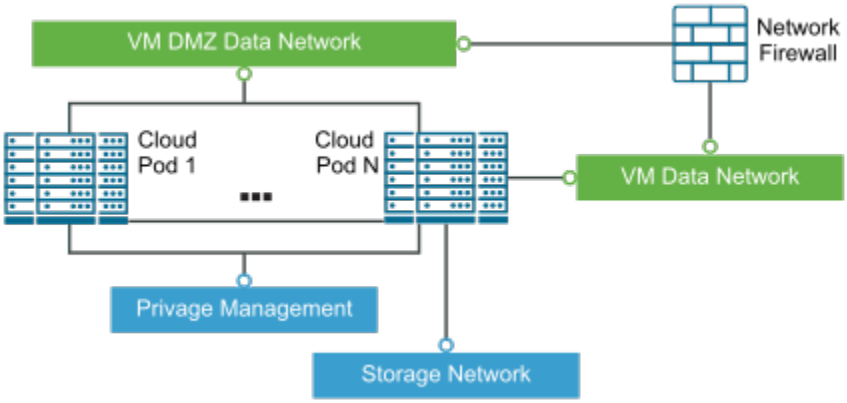
Abbildung 6-3. Verwaltungs-Pod-Netzwerke



In Bezug auf die vSphere-Hosts, die in verschiedenen Sicherheitsdomänen gruppiert sind, verfügen sie jeweils über externe Netzwerke, die als ein Datennetzwerk für eine VM-DMZ für die Verwendung als öffentliche VDC-Organisationsnetzwerke sowie als VM-Datennetzwerke für private VDC-Organisationsnetzwerke bereitgestellt werden und zu einem externen Netzwerk geroutet werden können.

Der Fokus der Abbildung Abbildung 6-4. Cloud-Pod-Netzwerke liegt auf den Cloud-Pods. Es zeigt vier physische Netzwerke; das Speichernetzwerk ist jedoch spezifisch für die gewählte Hardware und Speichertechnologie. Wenn Ressourcenpools sich nicht über Cluster erstrecken, müssen Sie möglicherweise kein physisches VM-Datennetzwerk bereitstellen. Andernfalls (wenn sich Ressourcenpools über Cluster erstrecken) wird in diesem Dokument ein separates physisches Netzwerk für den vMotion-Datenverkehr empfohlen.

Abbildung 6-4. Cloud-Pod-Netzwerke



Es wird auch davon ausgegangen, dass typische Sicherheitstechnologien für Rechenzentren wie IDS/IPS, SIEM, Systeme für Konfigurationsverwaltung, Patchverwaltung, Schwachstellenverwaltung und Virenschutz sowie GRC-Verwaltungssysteme sowohl auf vCloud Director, den zugehörigen Systemen, vSphere und den zugehörigen Systemen sowie auf die sie unterstützende Netzwerk- und Speicherinfrastruktur angewendet werden. Details zu diesen Systemen sind ebenfalls nicht Gegenstand dieses Dokuments.

Empfehlungen zur gemeinsamen Nutzung und Isolierung von Ressourcen

Unter normalen Bedingungen kann ein Dienstanbieter Computing-, Speicher- und Netzwerkressourcen für mehrere Mandantenorganisationen freigeben. Das System erzwingt die Isolierung über Abstraktion, eine sichere technische Praxis im Hypervisor und den vCloud Director-Software-Stack.

Mandantenorganisationen verwenden die zugrunde liegenden Ressourcenpools, Datenspeicher und externen Netzwerke gemeinsam, die über ein einziges Anbieter-VDC zugänglich sind, ohne Ressourcen zu beeinträchtigen (oder gar zu kennen), die sie nicht besitzen. Die ordnungsgemäße Verwaltung von vApp Speicher- und Laufzeit-Leases, vApp-Quoten, Beschränkungen für ressourcenintensive Vorgänge und Zuweisungsmodelle für Organisations-VDCs können sicherstellen, dass ein Mandant den Dienst für einen anderen nicht versehentlich oder absichtlich verweigern kann. Beispielsweise würde eine sehr konservative Konfiguration alle Organisations-VDCs unter dem Zuweisungsmodell des Reservierungspools einrichten und Ressourcen nie überbelegen. Der vollständige Optionsumfang wird in diesem Dokument nicht behandelt; einige Punkte werden jedoch in den folgenden Unterabschnitten erläutert.

Sicherheitsdomänen und Anbieter-VDCs

Trotz der richtigen Isolierung in der Software und der richtigen Organisationskonfiguration können Situationen eintreten, in denen Mandantenorganisationen nicht möchten, dass unterschiedliche Arbeitslasten auf bestimmten Computing-, Netzwerk- oder Speicherressourcen ausgeführt oder gespeichert werden. Dies führt nicht dazu, dass das System insgesamt zu einer „Hochsicherheitsumgebung“ wird (Erläuterungen dazu würden den Rahmen dieses Dokuments sprengen), sondern dass die Cloud in mehrere Sicherheitsdomänen segmentiert werden muss. Konkrete Beispiele für Arbeitslasten, die eine solche Behandlung erfordern, sind unter anderem:

- Daten, die den Datenschutzgesetzen unterliegen, die eine Speicherung und Verarbeitung innerhalb der vorgeschriebenen geographischen Grenzen vorschreiben.
- Daten und Ressourcen im Besitz von Ländern oder Organisationen, die trotz des Vertrauens in die Isolierung der Cloud aus Gründen der Vorsicht und Verteidigung in der Tiefe verlangen, dass ihre VDCs keine Ressourcen mit bestimmten anderen Mandanten teilen können – zum Beispiel einem konkurrierenden Unternehmen.

In diesen und anderen Szenarien sollten Ressourcenpools, Netzwerke und Datenspeicher in verschiedene „Sicherheitsdomänen“ unter Verwendung verschiedener Anbieter-VDCs segmentiert werden, wobei vApps mit ähnlichen Anliegen gruppiert (oder isoliert) werden können. Beispielsweise können Sie bestimmte Anbieter-VDCs eindeutig als Speicher- und Verarbeitungsdaten in bestimmten Ländern identifizieren.

Ressourcenpools

Innerhalb eines einzigen Anbieter-VDCs können Sie mehrere Ressourcenpools haben, die CPU- und Speicherressourcen, die von der zugrunde liegenden vSphere-Infrastruktur bereitgestellt werden, aggregieren. Die Segmentierung verschiedener Organisationen über verschiedene Ressourcenpools hinweg ist aus Sicht der Vertraulichkeit und Integrität nicht notwendig. Aus der Sicht der Verfügbarkeit kann es jedoch Gründe dafür geben. Dieses Ressourcenmanagementproblem hängt von den VDC-Zuteilungsmodellen der Organisation, den zu erwartenden Arbeitslasten, Quoten und Beschränkungen für diese Organisationen und der Geschwindigkeit ab, mit der zusätzliche Computing-Ressourcen vom Anbieter online gestellt werden können. Dieses Handbuch definiert nicht die verschiedenen Ressourcenzuweisungsmodelle und deren Auswirkungen auf die Nutzung eines Ressourcenpools durch die einzelnen Organisationen, außer zu sagen, dass immer dann, wenn Sie die Überbelegung von Ressourcen in einem Pool, der von mehr als einer Organisation genutzt wird, zulassen, das Risiko besteht, dass die Servicequalität für eine oder mehrere Organisationen abnimmt. Eine angemessene Überwachung der Service Levels ist unerlässlich, um zu vermeiden, dass Denial of Service von einer Organisation verursacht wird, aber die Sicherheit schreibt keine spezifische Trennung der Organisationen vor, um dieses Ziel zu erreichen.

Begrenzen des gemeinsamen Verbrauchs von gemeinsam genutzten Ressourcen

In der Standardkonfiguration können viele vCloud Director-Computing- und -Speicherressourcen von allen Mandanten in unbegrenzter Menge verbraucht werden. Das System bietet dem Systemadministrator mehrere Möglichkeiten, den Verbrauch dieser Ressourcen zu verwalten und zu überwachen. Die sorgfältige Prüfung der folgenden Bereiche ist ein wichtiger Teil dafür, die Möglichkeiten für einen „lauten Nachbarn“ zu beschränken, den Servicelevel zu beeinflussen, den vCloud Director bietet.

Begrenzen von ressourcenintensiven Vorgängen	Informationen hierzu finden Sie unter Konfigurieren der Systembegrenzung im *vCloud Director-Administratorhandbuch*.
Festlegen sinnvoller Kontingente	Informationen hierzu finden Sie unter Konfigurieren von Einstellungen für Leases, Quoten und Beschränkungen und (zum Begrenzen der Anzahl der VDCs, die ein Mandant erstellen kann, sowie zum Begrenzen der Anzahl gleichzeitiger Verbindungen pro VM) Konfigurieren der Systembegrenzung im *vCloud Director-Administratorhandbuch*.
Verwalten von Speicher- und Laufzeit-Leases	Leases bieten die Möglichkeit, die Nutzung von Speicher- und Computing-Ressourcen zu steuern. Die Begrenzung der Zeit, die eine vApp eingeschaltet bleiben kann oder die eine abgeschaltete vApp Speicher nutzen kann, ist ein wesentlicher Schritt bei der Verwaltung gemeinsamer Ressourcen. Informationen hierzu finden Sie unter Grundlegende Informationen zu Leases im *vCloud Director-Administratorhandbuch*.

Externe Netzwerke

Ein Dienstanbieter erstellt externe Netzwerke bereit und macht diese für Mandanten zugänglich. Ein externes Netzwerk kann sicher von mehreren öffentlichen Netzwerken gemeinsam verwendet werden, da diese per Definition öffentlich sind Mandanten sollten daran erinnert werden, dass der Datenverkehr in externen Netzwerken abgefangen wird, und sie sollten die Sicherheit auf Anwendungsebene oder auf Transportebene in diesen Netzwerken nutzen, um bei Bedarf Vertraulichkeit und Integrität zu gewährleisten.

Private geroutete Netzwerke können diese externen Netzwerke unter den gleichen Umständen gemeinsam verwenden – wenn sie für die Verbindung zu einem öffentlichen Netzwerk verwendet werden. In manchen Fällen kann ein externes Netzwerk von einem VDC-Netzwerk einer Organisation dazu genutzt werden, zwei verschiedene vApps und deren Netzwerke zu verbinden oder ein vApp-Netzwerk wieder mit dem Unternehmensdatencenter zu verbinden. In diesen Fällen sollte das externe Netzwerk nicht von mehreren Organisationen gemeinsam genutzt werden.

Sicherlich kann man nicht erwarten, für jede Organisation ein eigenes physisches Netzwerk zu haben. Stattdessen wird empfohlen, ein gemeinsames physisches Netzwerk mit einem einzigen externen Netzwerk zu verbinden, das eindeutig als DMZ-Netzwerk gekennzeichnet ist. So wissen Unternehmen, dass es keinen Vertraulichkeitsschutz bietet. Für die Kommunikation, die ein externes Netzwerk durchläuft, aber Vertraulichkeitsschutz erfordert (zum Beispiel eine Verbindung von den vApps zum Datencenter des Unternehmens oder eine vApp-vApp-Brücke über ein öffentliches Netzwerk), kann ein VPN bereitgestellt werden. Dies liegt daran, dass eine vApp in einem privaten gerouteten Netzwerk nur dann erreichbar ist, wenn sie die Weiterleitung von IP-Adressen über eine in diesem externen Netzwerk verfügbare IP-Adresse nutzt. Jede andere vApp, die sich mit diesem physischen Netzwerk verbindet, kann Pakete an diese vApp senden, selbst wenn es sich um eine andere Organisation handelt, die mit einem anderen externen Netzwerk verbunden ist. Um dies zu verhindern, kann ein Dienstanbieter NSX Distributed Firewall und Distributed Logical Routing verwenden, um die Trennung des Datenverkehrs von mehreren Mandanten in einem einzigen externen Netzwerk zu erzwingen. Informationen hierzu finden Sie unter NSX Distributed Firewall und Logical Routing im *VMware vCloud® Architecture Toolkit™ for Service Providers* (vCAT-SP)

VDC-Organisationsnetzwerke verschiedener Mandanten können das gleiche externe Netzwerk gemeinsam nutzen (als ein Uplink aus einem Edge-Gateway), solange sie nicht mit NAT und IP-Maskierung den Zugriff auf das interne Netzwerk zulassen.

Wichtig vCloud Director Die Funktion „Erweitertes Netzwerk“ ermöglicht Mandanten und Dienstanbietern den Einsatz von dynamischen Routing-Protokollen wie OSPF. Der OSPF-Mechanismus für automatische Erkennung könnte, wenn er ohne Authentifizierung verwendet wird, Peering-Beziehungen zwischen Edge-Gateways verschiedener Mandanten herstellen und mit dem Austausch von Routen beginnen. Um dies zu verhindern, aktivieren Sie OSPF nicht für öffentlich freigegebene Schnittstellen, es sei denn, Sie aktivieren die OSPF-Authentifizierung, um das Peering mit nicht authentifizierten Edge-Gateways zu verhindern.

Netzwerkpools

Ein einzelner Netzwerkpool kann von mehreren Mandanten genutzt werden, sofern alle Netzwerke im Pool entsprechend isoliert sind. VXLAN-gestützte Netzwerkpools (Standardeinstellung) basieren auf der Konfiguration der physischen und virtuellen Switches, um die Konnektivität innerhalb eines VXLANs und die Isolation zwischen verschiedenen VXLANs zu ermöglichen. Auf Portgruppen basierte Netzwerkpools müssen mit voneinander isolierten Portgruppen konfiguriert werden. Diese Portgruppen konnte physisch über VXLANs isoliert werden.

Von den drei Arten von Netzwerkpools (portgroup, VLAN und VXLAN) ist es am einfachsten, einen vCloud Director-VXLAN-Netzwerk-Pool gemeinsam zu nutzen. VXLAN-Pools unterstützen viel mehr Netzwerke als die auf VLAN oder portgroup basierten Netzwerkpools, und die Isolierung wird auf der vSphere-Kernelebene erzwungen. Während die physischen Switches den Datenverkehr nicht ohne den Einsatz des VXLAN isolieren, ist VXLAN auch nicht anfällig für fehlerhafte Konfigurationen auf der Hardwareebene. Wie oben bereits erwähnt, bietet keines der Netzwerke in einem Netzwerkpool Vertraulichkeitsschutz für abgefangene Pakete (z. B. auf der physischen Ebene).

Speicherprofile

vCloud Director-Speicherprofile aggregieren Datenspeicher auf eine Weise, die es dem Dienstanbieter ermöglicht, Speicherfunktionen nach Kapazität, Leistung und anderen Attributen abgestuft anzubieten. Mandantenorganisationen können nicht auf einzelne Datenspeicher zugreifen. Stattdessen kann ein Mandant eine Auswahl aus einer Reihe von durch den Dienstanbieter angebotenen Speicherprofilen treffen. Wenn die zugrunde liegenden Datenspeicher so konfiguriert sind, dass sie nur über das vSphere-Verwaltungsnetzwerk zugänglich sind, ist das Risiko bei der gemeinsamen Nutzung von Datenspeichern, wie bei Computing-Ressourcen, auf die Verfügbarkeit beschränkt. Eine Organisation kann am Ende mehr Speicherplatz verbrauchen als erwartet, wodurch die Menge des verfügbaren Speichers für andere Organisationen begrenzt wird. Dies gilt insbesondere für Organisationen, die das Pay-As-You-Go-Zuweisungsmodell und die Standardeinstellung „unbegrenzter Speicher“ verwenden. Wenn Sie Datenspeicher gemeinsam nutzen, sollten Sie daher einen Speichergrenzwert festlegen, wenn möglich Thin Provisioning aktivieren und die Speichernutzung sorgfältig überwachen. Sie sollten ebenfalls Ihre Speicher-Leases sorgfältig verwalten, wie in Begrenzen des gemeinsamen Verbrauchs von gemeinsam genutzten Ressourcen angegeben. Wenn Sie keine Datenspeicher freigeben, müssen Sie den Speicher für die Speicherprofile, die Sie jeder Organisation zur Verfügung stellen, ordnungsgemäß reservieren und verschwenden so möglicherweise Speicherplatz, indem Sie ihn Organisationen zuweisen, die ihn nicht benötigen.

vSphere-Datenspeicherobjekte sind die logischen Volumes, in denen VMDKs gespeichert sind. Während vSphere-Administratoren die physischen Speichersysteme sehen können, aus denen diese Datenspeicher erstellt werden, erfordert dies Rechte, die dem vCloud Director-Administrator oder -Mandant nicht zur Verfügung stehen. Mandantenbenutzer, die vApps erstellen und hochladen, speichern die VMDKs der vApps einfach auf einem der in ihrer Organisation verfügbaren Speicherprofile.

Aus diesem Grund sehen virtuelle Maschinen niemals Speicher außerhalb des von ihren VMDKs verbrauchten Speichers, es sei denn, sie verfügen über eine Netzwerkverbindung zu diesen Speichersystemen. In diesem Handbuch wird diese Vorgehensweise nicht empfohlen. Ein Anbieter könnte den Zugriff auf externen Speicher für vApps als Netzwerkdienst bereitstellen, aber er muss von den LUNs getrennt sein, die den vSphere-Hosts zugeordnet sind, die die Cloud unterstützen.

Ebenso sehen Mandantenorganisationen nur die in ihren VDCs verfügbaren Speicherprofile, und selbst diese Ansicht ist auf die vCloud Director-Abstraktion beschränkt. Sie können die Datenspeicher des Systems nicht durchsuchen. Sie sehen nur, was in Katalogen veröffentlicht oder von den von ihnen verwalteten vApps verwendet wird. Wenn die VDC-Speicherprofile der Organisation keine Datenspeicher gemeinsam nutzen, können sich die Organisationen nicht gegenseitig beeinflussen (außer vielleicht, indem sie zu viel Netzwerkbandbreite für Storage I/O verwenden). Selbst wenn sie das tun, sorgen die oben genannten Einschränkungen und Abstraktionen für eine angemessene Isolierung zwischen den Organisationen. vCloud Director-Administratoren können vSphere Storage I/O Control auf bestimmten Datenspeichern aktivieren, um die Fähigkeit eines Mandanten einzuschränken, eine übermäßige Menge an Storage I/O-Bandbreite zu verbrauchen. Informationen hierzu finden Sie unter Konfigurieren der Unterstützung für Storage I/O in einem Anbieter-VDC im *vCloud Director-Administratorhandbuch*.

Verwaltung von Benutzerkonten

Die Verwaltung der Benutzer und ihrer Anmeldedaten ist wichtig für die Sicherheit eines jeden Systems. Da die gesamte Authentifizierung bei und innerhalb des vCloud Director-Systems über Benutzername und Kennwort erfolgt, ist es wichtig, die besten Verfahren zur Verwaltung der Benutzer und ihrer Kennwörter zu befolgen.

Dieses Thema zielt darauf ab, die Möglichkeiten und Grenzen der Verwaltung von Benutzern und Kennwörtern in vCloud Director zu definieren und gibt Empfehlungen, wie diese angesichts dieser Einschränkungen sicher verwaltet und verwendet werden können.

Einschränkungen von lokalen Benutzerkonten

vCloud Director bietet einen unabhängigen Identitätsanbieter für Benutzerkonten, die erstellt und in der Datenbank vCloud Director erstellt und verwaltet werden. Obwohl diese Konten in einem System mit eingeschränktem Netzwerkzugriff auf die Datenbank nicht von Natur aus anfällig sind (siehe Konfiguration des Verwaltungsnetzwerks), bieten sie nicht die Art von Kennwortverwaltungsfunktionen, die von bestimmten Branchen (wie dem PCI-Datensicherheitsstandard) gefordert werden. Um Brute-Force-Angriffen vorzubeugen, sollte die Anzahl der Versuche für die wiederholte Kennworteingabe beschränkt sein. Zudem sollten Kontosperrungsrichtlinien angewendet werden.

Dienstanbieter sollten die Vorteile und Risiken der weiteren Verwendung lokaler Konten für Systemadministratoren sorgfältig abwägen und sorgfältig kontrollieren, welche Quell-IP-Adressen sich über die Cloud-URL eines Unternehmens authentifizieren können, wenn lokale Systemadministratorkonten konfiguriert sind. Es wird dringend empfohlen, die Verwendung dieses Identitätsanbieters für Systemadministratorkonten zu unterbinden oder zumindest einzuschränken.

Eine neue Installation von vCloud Director erstellt ein Konto für den lokalen Systemadministrator. In der Standardkonfiguration muss in vCloud Director mindestens ein Systemadministratorkonto lokal bleiben. Ein Dienstanbieter, der es der Systemorganisation ermöglicht hat, den vSphere-SSO-Dienst (ein SAML-Identitätsanbieter) oder LDAP zu verwenden, kann den Betrieb von vCloud Director ohne lokale Systemadministratorkonten konfigurieren, indem er die folgenden Schritte ausführt:

1 Erstellen eines oder mehrerer Konten für die Systemadministratoren im vSphere-SSO-Dienst (ein SAML-Identitätsanbieter) oder LDAP.

2 Importieren Sie dieses bzw. diese Konten in die Systemorganisation.

3 Ausführen des Befehls `manage-config` im Zellenverwaltungstool, um das System so zu konfigurieren, dass keine lokalen Systemadministratorkonten erforderlich sind und sich kein Systemadministrator mit einem lokalen Konto beim System authentifizieren kann.

```
./cell-management-tool manage-config -n local.sysadmin.disabled -v true
```

Beachten Sie, dass dadurch lokale Konten für andere Organisationen nicht deaktiviert werden.

Hinweis In einem System, das nicht über lokale Systemadministratorkonten verfügt, müssen die Befehle des Zellenverwaltungstools, die die Angabe von Systemadministrator-Credentials erfordern, stattdessen die Option `-i --pid` verwenden und die Prozess-ID der Zelle in *pid* angeben. Informationen dazu finden Sie in der Zellenverwaltungstool-Referenz im *vCloud Director-Administratorhandbuch*.

4 Sie können diese Änderung mit einer ähnlichen Befehlszeile im Zellenverwaltungstool rückgängig machen, die den Zugriff für Systemadministratoren mit lokalen Konten wieder ermöglicht.

```
./cell-management-tool manage-config -n local.sysadmin.disabled -v false
```

Kennwortverwaltung

Die meisten LDAP-, OAUTH- und SAML-Identitätsanbieter bieten Funktionen oder lassen sich in Systeme integrieren, um die Situation zu bewältigen, in der ein Benutzer sein Kennwort vergessen hat. Diese Situationen sind nicht Gegenstand dieses Dokuments. Das vCloud Director-Zellenverwaltungstool enthält einen Befehl `recover-password`, mit dem ein verlorenes Systemadministratorkennwort wiederhergestellt werden kann. vCloud Director verfügt nicht über integrierte Funktionen, diese Situation für andere lokale Benutzer zu bewältigen. Es wird empfohlen, dass alle lokalen Kontokennwörter in einer von Ihrer IT-Sicherheitsabteilung genehmigten Weise gespeichert werden. Einige Organisationen sperren Kennwörter in einem Tresor. Andere verwenden kommerziell oder frei verfügbare Programme zur Kennwortspeicherung. In diesem Dokument wird keine bestimmte Methode empfohlen.

Kennwortstärke

Die Stärke der Kennwörter von Identitätsanbieter-Benutzern hängt von den Steuerelementen ab, die von diesem Identitätsanbieter bereitgestellt werden, bzw. von den Tools, die zur Verwaltung der Benutzer innerhalb des Verzeichnisses verwendet werden. Beispiel: Wenn Sie vCloud Director mit Active Directory verbinden, werden die Steuerelemente für die Länge, die Komplexität und den Verlauf von Active

Directory-Standardkennwörtern, die mit Microsoft Active Directory verbunden sind, durch das Verzeichnis selbst erzwungen. Andere Identitätsanbieter neigen dazu, ähnliche Funktionen zu unterstützen. Die Details der Steuerung der Kennwortstärke sind verzeichnisspezifisch und werden hier nicht näher erläutert.

In vCloud Director müssen die Kennwörter der lokalen Benutzer mindestens sechs Zeichen beinhalten. Diese Anforderung ist nicht konfigurierbar, und es sind keine anderen Kennwortkomplexitäts- oder Verlaufssteuerelemente verfügbar. Es wird empfohlen, dass alle Benutzer, insbesondere System- und Organisationsadministratoren, ihre Kennwörter sorgfältig auswählen, um sich vor Brute-Force-Angriffen zu schützen (Probleme mit der Kontosperre werden weiter unten erläutert).

Schutz von Benutzerkennwörtern

Die Anmeldedaten von Benutzern, die von einem IDP verwaltet werden, werden niemals in der vCloud Director-Datenbank gespeichert. Sie werden mit der vom Identitätsanbieter gewählten Methode übertragen. Weitere Informationen zum Sichern dieses Informationskanals finden Sie unter Konfigurieren von Identitätsanbietern .

Die Kennwörter der lokalen Benutzer werden verschlüsselt, bevor sie in der vCloud Director-Datenbank gespeichert werden. Das Klartext-Kennwort kann nicht aus der Datenbank wiederhergestellt werden. Lokale Benutzer werden authentifiziert, indem sie das angezeigte Kennwort mit dem Inhalt ihres Kennwortfeldes in der Datenbank vergleichen.

Andere Kennwörter

Neben den Anmeldedaten für lokale Benutzer speichert die vCloud Director-Datenbank Kennwörter für verbundene vCenter-Server und NSX-Manager. Änderungen an diesen Kennwörtern werden im System nicht automatisch aktualisiert. Sie müssen diese manuell mit dem vCloud Director-Konfigurationsskript (für das vCloud Director-Datenbankkennwort) oder der Web-Benutzeroberfläche für vCenter und NSX ändern.

Wie oben erwähnt, verwaltet vCloud Director auch Kennwörter für den Zugriff auf die privaten Schlüssel, die mit seinen TLS/SSL-Zertifikaten verbunden sind, sowie die Kennwörter für die vCloud Director-Datenbank, die vCenter-Server und die NSX-Manager-Server. Diese Kennwörter werden mit einem eindeutigen Schlüssel pro vCloud Director-Installation verschlüsselt und in der Datei `$VCLOUD_HOME/etc/global.properties` gespeichert. Wie bereits in Schützen von vertraulichen Dateien nach der Installation erläutert, schützen Sie alle Sicherungen, die diese Datei enthalten.

Rollenbasierte Zugriffssteuerung

vCloud Director implementiert ein rollenbasiertes Autorisierungsmodell. In diesem Abschnitt werden die unterschiedlichen Identitätsquellen, Benutzertypen, Authentifizierungssteuerelemente, Rollen und Rechte in vCloud Director behandelt. Ein Verständnis dieser Informationen ist erforderlich, um das System ordnungsgemäß abzusichern und den richtigen Zugang zu den richtigen Personen zu gewährleisten.

Eine vCloud Director-Mandantenorganisation kann über eine beliebige Anzahl an Benutzern und Gruppen verfügen. Benutzer können lokal vom Organisationsadministrator erstellt oder von einem externen Verzeichnisdienst (LDAP) oder Identitätsanbieter (OAUTH, SAML) importiert werden. Importierte Benutzer können Mitglieder einer oder mehrerer Gruppen sein. Einem Benutzer, der Mitglied mehrerer Gruppen ist, werden alle diesen Gruppen zugeordneten Rollen zugewiesen. Jede Organisation wird mit einem Standardsatz von Rechten und einem Satz von vordefinierten Rollen erstellt, die Kombinationen dieser Rechte enthalten. Ein Systemadministrator kann einer Organisation zusätzliche Rechte zuweisen, und Organisationsadministratoren können diese Rechte verwenden, um benutzerdefinierte Rollen zu erstellen, die für die Organisation lokal sind. Die Berechtigungen innerhalb einer Organisation werden durch Zuweisung von Rechten und Rollen zu Benutzern und Gruppen gesteuert.

Nicht authentifizierte Benutzer dürfen nicht über die Webkonsole, das Mandantenportal oder die vCloud-API auf vCloud Director-Funktionen zugreifen. Jeder Benutzer authentifiziert sich mit einem Benutzernamen und einem Kennwort. Richtlinien für die wiederholte Eingabe von Kennwörtern und für die Kontosperrung können global und pro Organisation konfiguriert werden.

Rollen sind Gruppierungen von Rechten, die dem Benutzer, dem diese Rolle zugewiesen wurde, Funktionen zur Verfügung stellen. Vordefinierte Rollen umfassen:

- Systemadministrator
- Organisationsadministrator
- Katalogautor
- vApp-Autor
- vApp-Benutzer
- Nur Konsolenzugriff

Im *vCloud Director-Administratorhandbuch* wird ebenfalls aufgeführt, welche Rechte jeder Rolle zugewiesen sind. Dieser Abschnitt soll Ihnen helfen, die richtige Rolle für jeden Benutzertyp auszuwählen. Beispielsweise kann die vApp-Benutzerrolle für einen Administrator geeignet sein, der virtuelle Maschinen ein- und ausschalten muss, aber wenn er auch den einer virtuellen Maschine zugewiesenen Speicher bearbeiten muss, ist vApp-Autor eine geeignetere Rolle. Diese Rollen haben möglicherweise nicht genau die Rechte, die für die Organisationen Ihrer Mandanten relevant sind, sodass Organisationsadministratoren benutzerdefinierte Rollen erstellen können. Eine Beschreibung, welche spezifischen Rechte kombiniert werden können, um eine hilfreiche benutzerdefinierte Rolle zu erstellen, ist nicht Gegenstand dieses Dokuments.

Konfigurieren von Identitätsanbietern

Eine vCloud Director-Mandantenorganisation kann einen Identitätsanbieter definieren, den sie mit anderen Anwendungen oder Unternehmen gemeinsam nutzt. Benutzer authentifizieren sich beim Identitätsanbieter, um ein Token zu erhalten, mit dem sie sich dann bei der Organisation anmelden können. Eine solche Strategie kann einem Unternehmen den Zugriff auf mehrere, voneinander unabhängige Dienste einschließlich vCloud Director mit einem einzigen Satz von Anmeldeinformationen ermöglichen, was oft als Single Sign-On bezeichnet wird.

Informationen zu den Identitätsanbietern

vCloud Director unterstützt die folgenden Arten von Identitätsanbietern:

OAuth	Eine Organisation kann einen externen Identitätsanbieter definieren, der die OAuth-Authentifizierung gemäß RFC 6749 (http://tools.ietf.org/html/rfc6749) unterstützt.
SAML	Eine Organisation kann einen externen Identitätsanbieter definieren, der den Standard Security Assertion Markup Language (SAML) 2.0 unterstützt.
Integriert	Der integrierte Identitätsanbieter ist ein vCloud Director-Dienst, der Benutzer authentifiziert, die lokal erstellt oder aus LDAP importiert werden.

OAuth

In einer OAuth-Implementierung fallen die meisten Sicherheitsentscheidungen auf der OAuth-Autorisierungsserverebene. vCloud Director hat die Rolle eines Ressourcenservers. Dies ist ein Verbraucher des Tokens, der nur dafür verantwortlich ist, die Integrität des Tokens zu überprüfen.

Um Ihre vCloud Director-Sitzungen und die zugrunde liegenden vertraulichen Assets zu schützen, muss der OAuth-Autorisierungsserver sicher eingerichtet werden und die neuesten Sicherheits-Patches installiert haben.

Wenn der OAuth-Autorisierungsserver so eingerichtet werden kann, dass Benutzer an eine beliebige, von einem Abfrageparameter angegebene URL weitergeleitet werden können, muss der OAuth-Autorisierungsserver für die Validierung von URLs eingerichtet werden, um zu verhindern, dass Angreifer Umleitungen an Drittanwendungen kontrollieren. Eine Whitelist der berechtigten Anwendungen muss für die Validierung verwendet werden, sofern vorhanden.

LDAP

Der integrierte Identitätsanbieter von vCloud Director unterstützt mehrere gebräuchliche LDAP-Dienste.

Eine Liste der unterstützten LDAP-Dienste finden Sie in dem Dokument *vCloud Director-Versionshinweise*.

vCloud Director ermöglicht es dem Systemadministrator, einen systemweiten LDAP-Dienst zu definieren, der von allen Mandanten genutzt werden kann. Die Benutzerkonten der Mandanten werden in die vCloud Director-Datenbank importiert, wo ihnen vCloud Director-Rollen zugewiesen werden. Die Kennwörter der LDAP-Benutzer werden im LDAP-Verzeichnis verwaltet und gepflegt, und die Authentifizierung für dieses Verzeichnis erfolgt mit den im LDAP-Konfigurationsbildschirm angegebenen Einstellungen. Alle Kontrollmechanismen des LDAP-Verzeichnisses in Bezug auf Authentifizierung und Kennwörter bleiben erhalten, einschließlich Authentifizierungsfehlersperren, Kennwortablauf, Änderungsverlauf, Komplexität usw., und sind spezifisch für den gewählten LDAP-Dienst. Wenn eine Organisation für die Verwendung des System-LDAP-Dienstes konfiguriert ist, stammen die Benutzer aus der Organisationseinheit (OU), die in den vCloud Director-Einstellungen des System-LDAP-Dienstes speziell für diese Organisation konfiguriert ist.

Cloud-Anbieter können festlegen, dass Mandantenorganisationen eine OU innerhalb des System-LDAP-Dienstes verwenden oder ihren eigenen LDAP-Verzeichnisdienst hosten können. In beiden Fällen muss ein entsprechender Verwaltungszugriff auf dieses Verzeichnis ermöglicht werden, damit die Benutzer vom Organisationsadministrator verwaltet werden können. Das Fehlen einer derartigen Kontrolle würde einen zusätzlichen Arbeitsaufwand für den Systemadministrator mit sich bringen und die Organisation daran hindern, den Zugriff auf ihre VDCs ordnungsgemäß und bequem zu steuern. In Ermangelung solcher Verwaltungskontrollen sollte eine Organisation nur ein privates LDAP-Verzeichnis verwenden, das sie selbst hostet und verwaltet.

vCloud Director-Zellen müssen Verbindungen zum System-LDAP-Server und zu allen Organisations-LDAP-Servern herstellen können, damit die Software die Benutzer ordnungsgemäß authentifizieren kann. Wie in diesem Dokument empfohlen, muss sich der System-LDAP-Server im privaten Verwaltungsnetzwerk befinden, das durch eine Firewall von der DMZ getrennt ist. Was die erforderlichen LDAP-Server auf Organisationsebene angeht, so werden diese von einigen Cloud-Anbietern und den meisten IT-Organisationen in eigener Regie betrieben, und auch sie würden sich in einem privaten Netzwerk und nicht in der DMZ befinden. Alternativ könnte ein Organisations-LDAP-Server auch außerhalb der Umgebung des Cloud-Anbieters und unter der Kontrolle der Organisation gehostet und verwaltet werden. In diesem Fall muss er den vCloud Director-Zellen zugänglich gemacht werden, möglicherweise über die DMZ des unternehmenseigenen Datencenters.

In all diesen Fällen müssen die entsprechenden Ports in den verschiedenen Firewalls auf dem Weg von den Zellen zum LDAP-Server geöffnet werden, wie unter LDAP over TLS/SSL (sicheres LDAP) beschrieben. Zudem entsteht ein Problem, wenn die Organisation ihren eigenen LDAP-Server hostet und ihn über ihre DMZ zur Verfügung stellt. Da es sich nicht um einen Dienst handelt, der für die breite Öffentlichkeit zugänglich sein muss, sollten Schritte unternommen werden, um den Zugriff auf die vCloud Director-Zellen zu beschränken. Eine einfache Möglichkeit besteht darin, den LDAP-Server und/oder die externe Firewall so zu konfigurieren, dass der Zugriff nur von IP-Adressen aus möglich ist, die den vom Cloud-Anbieter gemeldeten vCloud Director-Zellen zugeordnet sind. Weitere Optionen sind Systeme wie organisationsbezogene Site-to-Site-VPNs, die diese beiden Systemgruppen miteinander verbinden, gehärtete LDAP-Proxies, virtuelle Verzeichnisse oder andere Optionen, die alle nicht Gegenstand dieses Dokuments sind.

Umgekehrt sollten sich Cloud-Anbieter bewusst sein, dass von Organisationen gehostete LDAP-Server, die von skrupellosen Kunden verwaltet werden, als Teil eines Angriffs auf andere Organisationen eingesetzt werden können. Beispielsweise könnte man sich vorstellen, dass eine Organisation einen Organisationsnamen anfordert, der mit einem häufig falsch geschriebenen Namen einer anderen Organisation identisch ist, und die ähnlich aussehende Anmelde-URL bei einem Phishing-Angriff verwendet. Der Anbieter kann Maßnahmen ergreifen, um sich gegen diese und ähnliche Angriffe zwischen Mandanten zu schützen, indem er sowohl die Quell-IP-Adressen von Anfragen nach Möglichkeit einschränkt, um Anmeldeversuche zwischen Organisationen zu vermeiden, als auch sicherstellt, dass die von ihm vergebenen Organisationsnamen nicht zu ähnlich sind.

LDAP over TLS/SSL (sicheres LDAP)

Es wird dringend empfohlen, ein LDAPv3-Verzeichnis für die Benutzerauthentifizierung zu konfigurieren. vCloud Director muss für die Verbindung zu LDAP-Servern unter Verwendung von SSL konfiguriert sein, um die zu validierenden Kennwörter beim Zugriff auf diese Server ordnungsgemäß zu schützen. Weitere Informationen hierzu finden Sie unter „Konfigurieren einer LDAP-Verbindung“ im *vCloud Director-Administratorhandbuch*. Die sicherste LDAP-Konfiguration wird durch Auswahl von **SSL verwenden** ermöglicht und erfordert ein vom LDAP-Dienst bereitgestelltes SSL-Zertifikat.

Wenn das signierte Zertifikat des LDAP-Servers nicht verfügbar ist, muss das Zertifikat der CA, die das LDAP-Server-Zertifikat signiert, in den JCE-Keystore (JCEKS) des Systems oder der Organisation importiert werden. LDAP-Konfigurationen, die einen JCE-Keystore spezifizieren, sind ebenfalls sicher. Allerdings kann eine große Anzahl von vertrauenswürdigen CA-Zertifikaten (oder sogar eine große Anzahl spezifischer Server-Zertifikate) zu Fehlkonfigurationen führen. Darüber hinaus ist es besser, einen LDAP-Anbieter zu wählen, der die Kerberos-Authentifizierung unterstützt.

Eine Verbindung zum LDAP-Server ist erforderlich. Während einfaches LDAP (ohne SSL) über den TCP-Port 389 läuft, verwenden Server, die LDAP over SSL unterstützen, standardmäßig den TCP-Port 636. Dieser Port ist jedoch auch konfigurierbar. In diesem Zusammenhang ist zu beachten, dass vCloud Director den veralteten LDAPS (LDAP over SSL)-Ansatz unterstützt und daher keine Unterstützung für einen TLS-Handshake innerhalb einer LDAP-Verbindung mit dem Befehl StartTLS bietet.

Schließlich sei noch erwähnt, dass der LDAP-fähige Verzeichnisserver ordnungsgemäß mit einem SSL-Zertifikat konfiguriert werden muss. Wie das geschieht, geht über den Rahmen dieses Dokuments hinaus.

Importieren von Gruppen

Der Zweck des Imports von Gruppen in vCloud Director besteht darin, den manuellen Import einzelner Benutzer mit derselben Rolle zu vermeiden. Wenn sich LDAP-Benutzer anmelden, werden ihrer Sitzung die Rollen zugewiesen, die den Gruppen zugeordnet sind, denen sie angehören. Sobald sich die Gruppenzugehörigkeit von Benutzern aufgrund von Änderungen ihrer Aufgaben innerhalb ihrer Organisation ändert, ändern sich auch die diesen Benutzern zugewiesenen Rollen automatisch gemäß der Zuordnung von Gruppe zu Rolle. Auf diese Weise können Organisationen Cloud-Rollen problemlos mit internen Organisationsgruppen oder -rollen und den Systemen, die sie bereitstellen und verwalten, integrieren.

Beispielsweise kann eine Organisation entscheiden, LDAP-Benutzern zunächst die Rolle „Nur Konsolenzugriff“ zuzuweisen, um die Rechte der Benutzer einzuschränken. Dazu werden alle Benutzer, die diese Basisrolle benötigen, einer einzigen LDAP-Gruppe hinzugefügt. Beim Importieren dieser Gruppe wird ihr dann vom Organisationsadministrator die Rolle „Nur Konsolenzugriff“ zugewiesen. Anschließend können Benutzer mit zusätzlichen Aufgaben anderen LDAP-Gruppen hinzugefügt und ebenfalls in vCloud Director importiert werden, wo ihnen dann Rollen mit zusätzlichen Berechtigungen zugewiesen werden. Beispielsweise können Benutzer, die Kataloge erstellen müssen, der Gruppe „Org A Katalogautor“ im LDAP-Server der Organisation hinzugefügt werden. Anschießend importiert der Organisationsadministrator für Org A die Gruppe „Org A Katalogautor“ und ordnet sie der vordefinierten Rolle „Katalogautor“ in vCloud Director zu. Dabei verfährt er gemäß der Anleitung im *vCloud Director-Benutzerhandbuch* zum Importieren einer Gruppe.

Checkliste

7

In dieser Checkliste sind die wichtigsten in diesem Dokument beschriebenen Aufgaben zur Sicherheitskonfiguration zusammengefasst.

- Neben den Orientierungshilfen in diesem Dokument gibt es noch die Sicherheitshinweise unter http://www.vmware.com/security/advisories/, deren Beachtung wir empfehlen. Über das Formular auf dieser Seite können Sie sich anmelden, um per E-Mail auf dem Laufenden gehalten zu werden. Zusätzliche Anleitungen und aktuelle Sicherheitshinweise bezüglich vCloud Director werden dort veröffentlicht.
- Administratoren sollten die Schritte ausführen, die in den Dokumenten *vSphere Security* (https://docs.vmware.com/de/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html), *Securing VMware NSX for vSphere* (https://communities.vmware.com/docs/DOC-27674) und *NSX-v 6.3.x Security Configuration Guide* (https://communities.vmware.com/docs/DOC-28142) empfohlen werden, um sicherzustellen, dass diese Produkte sicher installiert sind.
- Wenden Sie vor der Installation aktuelle Sicherheitspatches auf die Linux-Zellenplattform, die vCloud Director-Datenbank und die virtuelle Infrastruktur an. Die fortlaufende Überwachung dieser Komponenten ist ebenfalls wichtig, um sie auf einem aktuellen Patch-Stand zu halten.
- Auf die Linux-Zellenplattform sollten standardmäßige Sicherheitshärtungsverfahren angewendet werden, einschließlich Deaktivieren unnötiger Netzwerkdienste, Entfernen unnötiger Pakete, Einschränken des Remote-Root-Zugriffs und Durchsetzung starker Kennwortrichtlinien. Verwenden Sie nach Möglichkeit einen zentralisierten Authentifizierungsdienst wie Kerberos. Erwägen Sie die Installation von Überwachungs- und Intrusion Detection-Tools.
- Sie können zusätzliche Anwendungen installieren und zusätzliche Benutzer auf der Linux-Zellenplattform bereitstellen, dies wird jedoch nicht empfohlen. Die Erweiterung des Zugriffs auf das Zellenbetriebssystem kann die Sicherheit beeinträchtigen.
- Ermöglichen Sie den Zugriff auf die Datei `responses.properties` nur denjenigen, die ihn benötigen. Wenn sie genutzt wird (z. B. beim Hinzufügen von Zellen zu einer Servergruppe), schützen Sie den für alle Zielrechner zugänglichen Speicherort durch Platzierung entsprechender Zugriffssteuerungen. Alle erstellten Backups sollten sorgfältig kontrolliert und auch verschlüsselt werden, wenn Ihre Sicherungssoftware dies unterstützt. Sobald die Software auf allen Server-Hosts installiert ist, sollten alle Kopien der Datei `responses.properties` an den zugänglichen Stellen gelöscht werden.

- Die Dateien `responses.properties` und `global.properties` sind durch Zugriffssteuerungen für den Ordner `$VCLOUD_ HOME/etc` und die Dateien selbst geschützt. Nehmen Sie keine Änderungen an den Berechtigungen für die Dateien oder den Ordner vor.
- Der physische und logische Zugriff auf die vCloud Director-Server muss strikt auf diejenigen beschränkt sein, die sich anmelden müssen, und sollte nur die minimal erforderlichen Zugangsberechtigungen gewähren. Dies beinhaltet die Einschränkung der Nutzung des Root-Kontos durch `sudo` und andere Best Practices. Alle Backups der Server müssen streng geschützt und verschlüsselt sein, wobei die Schlüssel getrennt von den Backups selbst verwaltet werden müssen.
- Informationen zu den datenbankspezifischen Sicherheitserfordernissen finden Sie in den Sicherheitsleitfäden der von Ihnen gewählten vCloud Director-Datenbanksoftware.
- Benutzer der vCloud Director-Datenbank sollten keine Berechtigungen bezüglich anderer Datenbanken auf diesem Server oder sonstige Systemadministrationsberechtigungen erhalten.
- Stellen Sie sicher, dass alle Anmeldeinformationen, die für den administrativen Zugriff auf die Zelle, die verbundenen vCenter Server-Instanzen, die vCloud Director-Datenbank, Firewalls und andere Geräte verwendet werden, den Standards für die Kennwortkomplexität entsprechen.
- Ein wichtiger Punkt im Sinne einer Tiefenverteidigung ist die Variation der administrativen Kennwörter für die verschiedenen Server in der vCloud Director-Umgebung einschließlich der Zellen, der vCloud Director-Datenbank der vCenter Server-Instanzen und NSX.
- Informieren Sie sich unter https://docs.vmware.com/de/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-779A011D-B2DD-49BE-B0B9-6D73ECF99864.html über die Vorgehensweise beim Erstellen und Ersetzen von Zertifikaten, die von vCenter und ESXi verwendet werden. Diese Lektüre wird dringend empfohlen.
- vCenter-Zertifikate sollten ein Common Name (CN)-Feld aufweisen, dessen Inhalt dem vollqualifizierten Domänennamen (FQDN) des Servers, auf dem vCenter installiert ist, entspricht.
- Konfigurieren Sie vCloud Director für die Überprüfung von vCenter-Zertifikaten.
- vCenter-Zertifikate sollten von einer CA signiert sein und ein CN-Feld aufweisen, dessen Inhalt dem FQDN des Hosts entspricht, auf dem die Zelle installiert ist.
- Der empfohlene Ansatz für die Bereitstellung von vCloud Director-Diensten für die Außenwelt besteht darin, die Zellen in einer DMZ zu platzieren, wobei eine Netzwerk-Firewall das Internet von den vCloud Director-Zellen in der DMZ trennt. Der einzige Port, der von der Firewall internetseitig freigegeben werden muss, ist der TCP-Port 443.
- Da sich die vCloud Director-Zellen in der DMZ befinden, sollte ihr Zugriff auf die benötigten Dienste auch über eine Netzwerk-Firewall vermittelt werden. Insbesondere wird empfohlen, dass der Zugriff auf die vCloud Director-Datenbank, vCenter Server, vSphere-Hosts, IDPs (einschließlich LDAP) und alle Backup- oder ähnlichen Dienste auf der anderen Seite einer Firewall erfolgen, die die DMZ vom internen Netzwerk trennt.

- Virtuelle Maschinen, die von externer Seite außerhalb der Cloud (z. B. vom Internet aus) zugänglich sein müssen, wären entweder mit einem öffentlichen Netzwerk oder einem privaten Netzwerk mit NAT-Routing und Port-Weiterleitung für die bereitgestellten Dienste verbunden. Für das externe Netzwerk, mit dem diese VDC-Organisationsnetzwerke verbunden sind, wäre eine schützende Firewall erforderlich, für die der vereinbarte Datenverkehr zu dieser DMZ zulässig ist.
- Generell wird empfohlen, vApps, die über das Internet erreichbar sein müssen, in einem privaten gerouteten Netzwerk zu platzieren. Dies ermöglicht dem Mandanten die Kontrolle über die von NSX zur Verfügung gestellten Firewall und Portweiterleitungsregeln. Diese und andere Regeln können standardmäßig von der Netzwerk-Firewall angewendet werden, die Sie bereitstellen möchten. In der Dokumentation zu Ihrer Firewall finden Sie genaue Konfigurationsanweisungen und Standardfunktionen.
- Eine Verteidigung in der Tiefe erfordert, dass JMX (TCP-Port 8999) und JMS (TCP-Ports 61611 und 61616) von der Netzwerk-Firewall blockiert werden, welche die DMZ schützt, mit der die Zellen verbunden sind.
- So legen Sie die öffentliche Web-URL, die öffentliche Konsolen-Proxy-Adresse und die öffentliche REST-API-Basis-URL für eine mehrzellige Cloud hinter einer Webanwendungs-Firewall (WAF) oder einem Lastausgleichsdienst fest.
- Vor den vCloud Director-Zellen sollte eine Webanwendungs-Firewall (WAF) bereitgestellt werden.
- Es wird empfohlen, bei derartigen Bereitstellungen die WAF so zu konfigurieren, dass sie eine Inspektion und eine ordnungsgemäße Blockierung des schädlichen Datenverkehrs ermöglicht. Dies geschieht in der Regel mithilfe von TLS- oder SSL-Terminierung.
- Beim Konfigurieren der TLS- oder SSL-Terminierung ist es wichtig, nicht nur ein CA-signiertes Zertifikat in der Webanwendungs-Firewall (WAF) zu installieren, damit Clientanwendungen der vCloud-API und der Webkonsole sich der Identität des Servers vergewissern können, sondern auch ein CA-signiertes Zertifikat in den Zellen zu verwenden, obwohl diese nur für die WAF sichtbar sind.
- Wenn der Lastausgleichsdienst unabhängig von der WAF ist, sollte auch er ein CA-signiertes Zertifikat verwenden.
- Es wird empfohlen, sofern möglich die Generierung des `X-Forwarded-For`-Headers in der Firewall zu aktivieren.
- Wenn der vCloud Director-Server über eine dritte IP-Adresse verfügt, die ihm ausschließlich für Verwaltungszwecke zugewiesen wurde, binden Sie JMX direkt an diese IP-Adresse. Der JMX-Connector von vCloud Director wird standardmäßig an die bei der Konfiguration angegebenen primären IP-Adressen gebunden. Diese Standardeinstellung kann durch Einfügen der folgenden Eigenschaft in /opt/vmware/vcloud-service-director/etc/global.properties überschrieben werden: `vcloud.cell.ip.management=`*`IP-Adresse oder Hostname für das Verwaltungsnetzwerk, an das sich der JMX-Connector binden soll.`*.
- Die empfohlene und sicherere Konfiguration beinhaltet die Anbindung des JMX-Connectors an die localhost-Adresse: `vcloud.cell.ip.management=127.0.0.1`. Wenn JMX nur dem localhost zugänglich

ist, erfolgt die Sicherung der JMX-Kommunikation durch den Einsatz von SSH als Tunneling-Mechanismus für jeden Zugriff auf JMX. Wenn Ihre Verwaltungsanforderungen die Verwendung dieser Art von localhost-Konfiguration nicht zulassen und JMX außerhalb des vCloud Director-Servers verfügbar sein muss, sollte JMX mit TLS oder SSL gesichert werden.

- Hinter den Zellen befinden sich die von vCloud Director benötigten privaten Verwaltungselemente: die Datenbank, NSX, vCenter Server, ggf. der System-LDAP-Server, der von vCenter verwendete Active Directory-Server und die Verwaltungsschnittstellen der vSphere-Hosts. Ihre Verbindungen werden streng durch Firewalls kontrolliert, da diese Dienste nicht von anderen VMs in der DMZ oder direkt aus dem Internet erreichbar sein sollten.
- Außerdem wird vorausgesetzt, dass typische Sicherheitstechnologien für Datencenter wie z. B. IDS/IPS, SIEM, Konfigurationsmanagement, Patch-Management, Schwachstellen-Management, Virenschutz- und GRC-Management-Systeme sowohl auf vCloud Director und vSphere sowie die jeweils zugehörigen Systeme als auch auf die sie unterstützenden Netzwerke und Speicherinfrastrukturen angewendet werden.
- Eine ordnungsgemäße Verwaltung der Leases, Kontingente, Grenzwerte und Zuteilungsmodelle kann sicherstellen, dass eine Mandantenorganisation einer anderen nicht zufällig oder absichtlich den Dienst verweigern kann.
- In diesen und anderen Szenarien sollten Ressourcenpools, Netzwerke und Datenspeicher in verschiedene Sicherheitsdomänen unter Verwendung verschiedener Anbieter-VDCs segmentiert werden, damit vApps mit ähnlichen Problemen gruppiert (oder isoliert) werden können.
- Wenn Sie die Überbelegung von Ressourcen in einem Pool zulassen, der von mehr als einer Mandantenorganisation genutzt wird, laufen Sie Gefahr, dass sich die Servicequalität für andere Mandanten verschlechtert. Eine ordnungsgemäße Überwachung der Service Levels ist unerlässlich, um zu vermeiden, dass Denial of Service durch einen „lauten Nachbarn“ verursacht wird. Unter dem Aspekt der Sicherheit ist jedoch keine Trennung der Mandanten in einzelne Ressourcenpools erforderlich, um dieses Ziel zu erreichen.
- In manchen Fällen kann ein externes Netzwerk von einem VDC-Netzwerk einer Organisation dazu genutzt werden, zwei verschiedene vApps und deren Netzwerke zu verbinden oder ein vApp-Netzwerk wieder mit dem Unternehmensdatencenter zu verbinden. In diesen Fällen sollte das externe Netzwerk nicht von mehreren Mandantenorganisationen gemeinsam genutzt werden.
- Für Kommunikationsvorgänge, die ein externes Netzwerk durchqueren und auch Vertraulichkeitsschutz erfordern (z. B. eine vApp-Unternehmensdatencenter-Verbindung oder eine vApp-vApp-Brücke), wird empfohlen, eine NSX Edge-Appliance oder eine andere virtuelle VPN-Appliance im VDC-Netzwerk des Unternehmens bereitzustellen.
- Wenn die Netzwerkpools von Mandanten gemeinsam genutzt werden müssen, ist es am sichersten, einen VXLAN-gestützten Pool zu teilen, der viel mehr Netzwerke unterstützt als ein VLAN-gestützter Pool und die Isolierung auf der ESXi-Kernel-Ebene erzwingt.
- Wenn Sie Datenspeicher speicherprofilübergreifend gemeinsam nutzen, sollten Sie einen Speichergrenzwert festlegen, ggf. Thin Provisioning aktivieren und die Speichernutzung sorgfältig überwachen. Auch die vApp-Speicher-Leases sollten sorgfältig überwacht werden.

- Virtuelle Maschinen erkennen keinen Speicher außerhalb ihrer VMDKs, es sei denn, sie verfügen über eine Netzwerkverbindung zu diesen Speichersystemen. Dieser Leitfaden empfiehlt, ihnen diese Möglichkeit nicht zu verschaffen. Ein Anbieter könnte den Zugriff auf externen Speicher für vApps als Netzwerkdienst bereitstellen, aber er muss von den LUNs getrennt sein, die den vSphere-Hosts zugeordnet sind, die die Cloud unterstützen.
- Wie in *vSphere Security* (https://docs.vmware.com/de/VMware-vSphere/6.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html) festgehalten, ist es wichtig, dass das Verwaltungsnetzwerk von den Datennetzen der virtuellen Maschinen getrennt ist.
- Desgleichen muss das Verwaltungsnetzwerk von der DMZ getrennt sein, die den Zugriff für Organisationsadministratoren ermöglicht.
- Die Speichernetzwerke sind auch physisch getrennt. Dies entspricht den Best Practices für vSphere und schützt Mandantenorganisationen und Anbieterspeicher vor schädlichen virtuellen Maschinen.
- vMotion ist nicht immer in einem vom Verwaltungsnetzwerk separaten Netzwerk platziert; in der Cloud ist es jedoch aus Sicht der Aufgabentrennung wichtig. vMotion arbeitet in der Regel ohne Verschlüsselung, und wenn es im Verwaltungsnetzwerk platziert wird, erlaubt dies einem Administrator des Anbieters oder einem anderen Benutzer mit Zugang zu diesem Netzwerk, den vMotion-Datenverkehr auszuspionieren, was gegen den für die Mandanten geltenden Datenschutz verstößt. Aus diesem Grund sollten Sie ein separates physisches Netzwerk für die vMotion-basierte Migration von Cloud-Arbeitslasten erstellen.
- Es gehört zur guten Sicherheitspraxis, Protokolle regelmäßig auf verdächtige, ungewöhnliche oder nicht autorisierte Aktivitäten zu untersuchen. Die routinemäßige Protokollanalyse hilft auch, Systemfehlkonfigurationen und -ausfälle zu erkennen und die Einhaltung von SLAs sicherzustellen.
- Ein Syslog-Server kann während der Installation eingerichtet werden. Wir empfehlen die Verwendung einer TLS-fähigen Syslog-Infrastruktur. Der Export von Protokollen auf einen Syslog-Server wird aus mehreren Gründen empfohlen. Es wird empfohlen, den `syslog`-Server redundant zu konfigurieren, um sicherzustellen, dass wichtige Ereignisse stets protokolliert werden. Die Sicherheitsvorgänge und der IT-Betrieb von Organisationen können ebenfalls von der zentralen Zusammenführung und Verwaltung der Diagnoseprotokolle profitieren. Es wird die Verwendung von `logrotate` oder ähnlichen Methoden empfohlen, um die Größe von Protokollen und die Anzahl alter Protokolldateien zu steuern.
- Stellen Sie sicher, dass ausreichend freier Speicherplatz für Diagnoseprotokolle und Jetty-Anforderungsprotokolle vorhanden ist. Die zentrale Protokollierung sorgt dafür, dass Sie keine wertvollen Diagnoseinformationen verlieren, wenn die Gesamtgröße der Protokolldateien von 400 MB erreicht wird und Dateien rotiert und gelöscht werden.
- Andere Systeme, die mit vCloud Director verbunden sind und von ihm genutzt werden, erstellen Überwachungsprotokolle, die in Ihren Überwachungsprozessen konsolidiert werden sollten. Dazu gehören Protokolle von NSX, der vCloud Director-Datenbank, von vCenter Server und vSphere-Hosts.

- Es wird dringend empfohlen, nach Erstellung des ersten lokalen Systemadministratorkontos alle Systemadministratorkonten unter Verwendung eines Identitätsanbieters wie LDAP oder des vSphere SSO-Dienstes zu verwalten.
- Einige Cloud-Anbieter gestatten es möglicherweise Organisationen, eine OU innerhalb des System-LDAP-Dienstes zu verwenden oder ihren eigenen LDAP-Verzeichnisdienst zu hosten. In beiden Fällen muss ein entsprechender Verwaltungszugriff auf dieses Verzeichnis ermöglicht werden, damit die Benutzer vom Organisationsadministrator verwaltet werden können. In Ermangelung solcher Verwaltungskontrollen sollte eine Mandantenorganisation nur ein privates LDAP-Verzeichnis verwenden, das sie selbst hostet und verwaltet.
- Ein weiteres Problem, das auftritt, wenn die Organisation ihren eigenen LDAP-Server hostet, ist die Offenlegung außerhalb ihrer DMZ Da es sich nicht um einen Dienst handelt, der für die breite Öffentlichkeit zugänglich sein muss, sollten Schritte unternommen werden, um den Zugriff auf die vCloud Director-Zellen zu beschränken. Eine einfache Möglichkeit besteht darin, den LDAP-Server und/oder die externe Firewall so zu konfigurieren, dass der Zugriff nur von IP-Adressen aus möglich ist, die den vCloud Director-Zellen zugeordnet sind.
- Der Anbieter kann Maßnahmen ergreifen, um sich gegen diese und ähnliche Angriffe zwischen Mandanten zu schützen, indem er sowohl die Quell-IP-Adressen von Anfragen nach Möglichkeit einschränkt als auch sicherstellt, dass die von ihm an Mandanten vergebenen Organisationsnamen nicht zu ähnlich sind.
- vCloud Director muss für die Verbindung zu LDAP-Servern unter Verwendung von SSL konfiguriert sein, um die zu validierenden Kennwörter beim Zugriff auf diese Server ordnungsgemäß zu schützen. Akzeptieren Sie beim Konfigurieren von LDAP over SSL nicht alle Zertifikate.
- Best Practices für die Verwaltung von Benutzern und deren Kennwörtern sollten verstanden und angewendet werden.
- Protokollverwaltung, SIEM (Security Information and Event Management) und andere Überwachungssysteme sollten dazu verwendet werden, Versuche zu erkennen, Kennwörter durch Brute-Force-Angriffe zu knacken.
- Es wird empfohlen, die Kennwörter von Systemadministratoren und Organisationsadministratoren in einer von Ihrer IT-Sicherheitsabteilung genehmigten Weise zu speichern.