Neuerungen in vSphere 7 und Update 1

Deutlich mehr

von Thomas Drilling

Die im April 2020 erschienene Version 7.0 von vSphere ist das größte Upgrade in der Produktgeschichte. Das betrifft nicht nur die Entwicklungszeit und damit die Lifetime des 6.7-Releases, sondern auch die Code-Menge und die Anzahl neuer Features. Die Wichtigsten davon aus den Bereichen vCenter, Sicherheit, Management und Storage stellt dieser Beitrag vor.

Quelle: monticello – 123RF

Wir betrachten in diesem Artikel nicht nur die Neuerungen der finalen Version vom April 2020, sondern auch die kaum weniger erwähnenswerten Aktualisierungen des Update 1 vom Oktober 2020, unter denen vor allem vSphere mit Tanzu hervorzuheben ist. Hat vor allem der mit Version 7 eingeführte native Kubernetes-Support im Vorfeld der Veröffentlichung die höchsten Wellen geschlagen, ist die Funktion aus Sicht des Infrastrukturverantwortlichen erst einmal wenig wahrnehmbar, adressiert doch das Cloud-Native-Thema in erster Linie Entwickler. Ganz generell wandelt sich aber die Rolle von vSphere als Einzelprodukt hin zu einem essenziellen Baustein in VMwares Philosophie des Software-defined Datacenter (SDDC).

Fokussiert auf die Cloud

So hat VMware zwar erkannt, dass cloudnativen Apps die Zukunft gehört und die Grenzen zwischen Infrastruktur- und Anwendungsbereitstellung mehr und mehr verschwinden, doch bis sich entsprechende Denk- und Sichtweisen in den Unternehmen in der Art und Weise der Anwendungsbereitstellung bemerkbar machen, mag durchaus noch Zeit ins Land gehen.

IT-Verantwortliche, die in vSphere immer noch in erster Linie ein Produkt zur Serverkonsolidierung sehen, kommen mit den neuen Möglichkeiten in vSphere kaum in Berührung. Hier ist ein deutlicher Impuls von Entwicklerseite nötig, und bevor diese von vSphere mit Kubernetes profitieren, muss der Virtualisierungs-Admin bei vSphere 7 erst für den passenden Unterbau in Form der "VMware Cloud Foundation" sorgen. Insofern blieb das Aushänge-Feature von vSphere 7 für viele IT-Verantwortliche zunächst einmal mit viel Arbeit verbunden.

Anders ist es mit vSphere 7 Udate 1 und vSphere mit Tanzu, denn dies erschließt die Cloud-Native-Welt auf Basis von Tanzu Kurbenetes Grid (TKG) auch ohne NSX-T und vSAN. Mehr zu vSphere mit Kubernetes, vSphere mit Tanzu und der Produkthistorie von den Anfängen des Pivotal Container Servives, über Zukäufe wie Heptio bis zur Tanzu-Suite in ihren diversen Editionen finden Sie in verschiedenen Beiträgen dieses Sonderhefts.

Dieser Beitrag konzentriert sich auf die Neuerungen von vSphere als Plattform zur Servervirtualisierung. Dabei klammern wir die Aktualisierungen in vSAN 7 aus, denen ebenfalls eigene Artikel gewidmet sind (ab Seite 112). Was die Neuerungen im Einzelnen angeht, überfliegen wir diese aus maximaler Reiseflughöhe und verweisen bei den Details auf die entsprechenden Artikel dieses Sonderhefts. Zur besseren Einordnung kategorisieren wir die Betrachtung unabhängig von ihrer Bedeutung und Wichtigkeit für das Gesamtprodukt in die Bereiche Management/vCenter, Host-Features, Lifecyle-Verwaltung, VM-Features, Storage-Verbesserungen, Security und Cluster. Möchten Sie sich unabhängig oder zusätzlich zu diesem Beitrag über die bisherigen und kommenden Neuerungen auf dem Laufenden halten, sollten Sie den VMware vSphere Blog [1] (Kategorien vSphere 7 und 7U1) im Auge behalten.

Neues aus dem vCenter

Die wichtigsten Neuerungen im vCenter und für das Verwalten von vSphere sind der Abschied vom Web-Client, die Einführung von vCenter-Serverprofilen, weitreichende Verbesserungen an der Content Library, die Unterstützung für ADFS und das Ende von Windows-vCenter sowie vom externen Platform Services Controller (PSC), der durch den Support des Embedded Linked Mode überflüssig wurde.

Doch der Reihe nach: In vSphere 7 steht als UI-basierter Verwaltungsclient auf vCenter-Ebene ausschließlich der auf HTML5 basierende vSphere-Client zur Verfügung, der nun sämtliche Funktionen etwaiger älterer Clients in sich vereint. Der vSphere-Web-Client ist unter anderem wegen Flash veraltet und daher nicht mehr

unterstützt [2]. Darüber hinaus stellt jeder ESXi-Host nach wie vor per Default einen ebenfalls HTML5-basierenden Host-Client zur Verfügung, der Nutzern das Verwalten einzelner ESXi-Hosts erlaubt, die kurzfristig oder generell nicht mit einem vCenter-Server verbunden sind.

Dieses wird mit vSphere 7 ausschließlich als Linux-basierende (VMware Photon Linux) virtuelle Appliance (VCSA) mit eingebetteter PostgresQL-Datenbank und PSC ausgeliefert, die sich als OVA sehr einfach auf einem ESXi-Host oder vorhandenen vCenter ausrollen lässt. Das OVA wiederrum ist in einem Linux-/Mac- oder Windows-basierenden UI-Installer eingebettet, der die Inbetriebnahme zum Kinderspiel macht. Optional stehen diverse JSON-Templates für eine CLI-basierte, unbeaufsichtigte Installation bereit. Von den Templates gibt es im Vergleich zur Vorgängerversion deutlich weniger, da der Support für den externen PSC entfällt. Das heißt, im betreffenden Ordner für Installation/Upgrade oder Migration der CLI-Variante finden sich ab sofort nur noch vier JSON-Dateien – jeweils für die eingebettete Installation auf ESXi oder vCenter mit und ohne Replikation beziehungsweise im Ordner für das Upgrade die vier Dateien für Embedded-vCSA auf ESXi/VC beziehungsweise vCSA auf ESXi/VC.

Zur Erinnerung: Der PSC bündelt sämtliche vCenter-Funktionen, die das Single Sign-on (SSO) betreffen, in einer separaten Komponente. Das betrifft neben sämtlichen SSO-Bestandteilen einschließlich Verzeichnisdienst (VMware Directory Services, vmdir) nebst SAML-basierender Token-Austausch-Infrastruktur auch die Zertifikatsdienste (VMware CA, Certificate Store), den Lizenzdienst und einen Lookup-Service.

Die mit vSphere 6.0 eingeführte Ausgliederung dieser Dienste in eine separate Infrastrukturkomponente ermöglicht es externen Zusatzlösungen von VMware und Drittanbietern, das vCenter für SSO zu nutzen. Das ist auch in vSphere 7 so, nur dass der PSC keine separate VM mehr erfordert, was den Nachteil einer Abhängigkeit vom Netzwerk-Stack beseitigt und zudem Bereitstellung und Sicherung von vCenter auf VM-Level vereinfacht. Die Bereitstellung des PSC auf einer externen VM war aber vor vSphere 7 Voraussetzung für den verknüpften vCenter-Modus (Enhanced Linked Mode; ELM).

In diesem können zwei bis 15 vCenter-Systeme beim gleichen PSC registriert sein und damit nicht nur die gleiche SSO-Domäne nutzen, sondern auch das jeweilige Inventar im eigenen vSphere-Client sehen und Funktionen wie Cross-vCenter-vMotion verwenden. Ist mehr als ein PSC vorhanden, kann sich die SSO-Domäne über alle PSCs erstrecken. Benutzer, Berechtigungen sowie Rollen werden dann zwischen mehreren PSCs repliziert. Das ist nützlich, um den PSC hochverfügbar zu halten oder das vCenter über mehrere Standorte zu verteilen. Vor vSphere 7 war ein externer PSC hierzu zwingende Voraussetzung, in vSphere 7 funktioniert der hier ausschließlich unterstützte "Embedded Linked Mode" (ELM) mit den stets eingebetteten PSCs.

Verbesserung im Netz und bei IP-Adressen

Ebenfalls neu ist die mit vCenter 7 erstmals eingeführte Möglichkeit, den sogenannten PNID (Primary Network Identifier) des vCenter-Servers auch nach der Bereitstellung ändern und damit bei Bedarf den DNS-Hostnamen und die IP-Adresse nachträglich anpassen zu können. Das war vor vSphere 7 schlichtweg nicht oder nur mit großem Aufwand möglich, denn der Systemname ist unter anderem im SSL-Zertifikat des Systems verschlüsselt und vCenter-Server-Core sowie PSC kommunizieren stets unter Verwendung des Systemnamens miteinander. Jetzt sind IP-Adresse und Systemname im Applicance Management Interface (VAMI) anpassbar.

Bei der Gelegenheit sei zudem erwähnt, dass vCenter 7 erstmals Multihooming unterstützt und sich mit bis zu vier virtuellen Netzwerkkarten ausstatten lässt. So sind vCenter-Systeme problemlos aus mehreren unterschiedlichen IP-Subnetzen heraus verwaltbar. Alle vier von Multihoming unterstützten NIC-Konfigurationen bleiben während des Upgrades, der Sicherung und der Wiederherstellung erhalten. In vSphere 7 ist darüber hinaus die primäre MAC-Adresszuweisungsmethode außer für VMs nicht mehr OUI-basiert (VMware Organizationally Unique Identifier). Standard ist nun die präfixbasierte MAC-Adresszuweisung.

Schließlich wurde die seit Version 6.5 im VAMI eingebaute Möglichkeit der dateibasierten Sicherung von vCenter-Konfiguration, -Inventar und -Datenbank (Statistiken, Events und Tasks) von Version zu Version von VMware sukzessive weiter

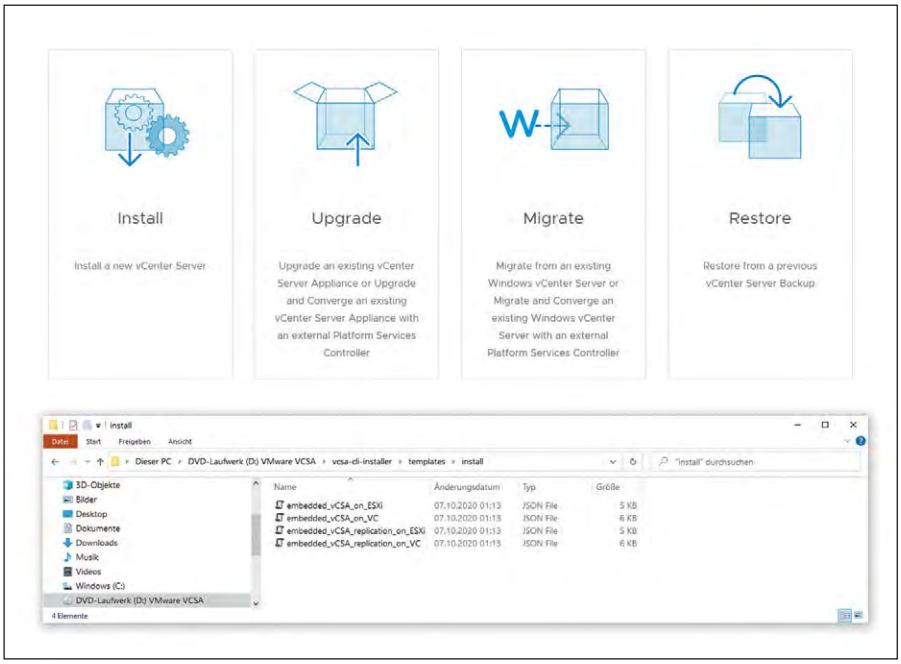

Bild 1: Die vCenter-Bereitstellung erfolgt OVA-basiert verpackt in einem UI- oder CLI-basierenden Installer.

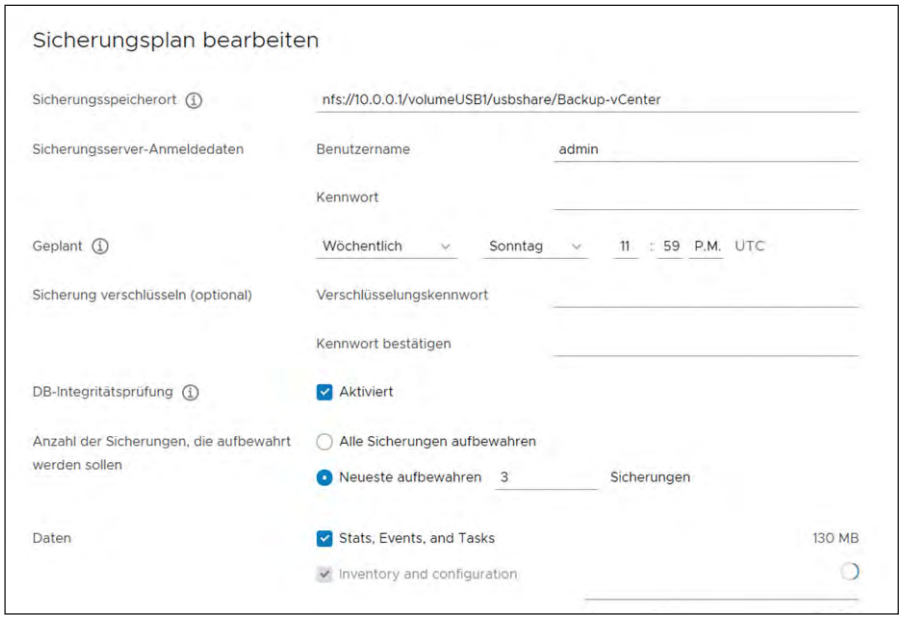

Bild 2: Die dateibasierte Sicherungsfunktion im Appliance-Management wurde um neue Optionen erweitert.

ausgebaut und unterstützt in Version 7 nun auch die Protokolle NFSv3 und höher sowie Samba (SMBv2 und neuer).

Flexiblere Möglichkeiten mit der Content Library

Die mit vSphere 6.0 eingeführte Funktion der Inhaltsbibliothek (Content Library) hat VMware über die Jahre allmählich ausgebaut. Fand das Feature anfangs weniger Beachtung, ist es in Version 7 auch für kleine Unternehmen ohne verteilte Standorte interessant. Bemerkenswert ist einerseits, dass Inhaltsbibliotheken inzwischen die Content-Typen "VM-Template", "OVA/OVF" und "ISO-Image" unterstützen und der Administrator sogar die Wahl hat, ob dieses als VM-Template oder als OVF-Datei abgelegt wird.

Darüber hinaus lassen sich Templates nun versionieren. Dabei können IT-Verantwortliche ein Template aus der Bibliothek "auschecken", um dieses im Rahmen einer Rekonvertierung in eine VM aktualisieren zu können, während es gleichzeitig in der Bibliothek für andere Benutzer sichtbar bleibt, die daraus im Zweifel zur gleichen Zeit ebenfalls VMs auschecken können. VMware nennt das im Hintergrund auf der Linked-Clone-Technologie basierende Feature "VM Template In-Place Update". Es vereinfacht den Vorgang einer Template-Aktualisierung erheblich.

Zertifikatsmanagement per GUI

Neu ist in vSphere 7 auch die Zertifikatsverwaltung im grafischen vSphere-Client. Bekanntlich verwendet vSphere Zertifikate zum Verschlüsseln der Kommunikationen zwischen Knoten, etwa vCenter-Server- und ESXi-Host, zum Authentifizieren von vSphere-Diensten sowie zum Durchführen interner Aktionen wie das Signieren von Token.

Mussten vSphere-Administratoren bei früheren Versionen wie vSphere 5.5 und älter zahlreiche verschiedene Zertifikate verwalten, was einen erheblichen Aufwand etwa beim Erneuern verursachte, reduzierte VMware die Komplexität des Themas von Version zu Version. Dies erfolgte zum Beispiel durch Verkleinern der Anzahl der erforderlichen Zertifikate und die fast vollständige Integration der vSphere-7-Zertifikatsverwaltung in den HTML5-Client.

Zwar kommt der Admin nicht in jedem Fall um den CLI-basierten Certificate Manager (unter "/usr/lib/vmware-vmca/bin/certificate-manager") herum, mit der neuen Zertifikatsverwaltung im vSphere-Client kann er aber nun sehr komfortabel die vertrauenswürdigen Root-Zertifikate und Maschinen-SSL-Zertifikate anzeigen, verlängern oder ersetzen und eine benutzerdefinierte Zertifikatsignier-Anforderung (CSR) für ein Maschinen-SSL-Zertifikat generieren, beziehungsweise dieses ersetzen, wenn es die Zertifizierungsstelle zurückgibt.

vCenter-Profile zur Konfiguration

Eine weitere neue Funktion in vSphere 7 ist der Support für vCenter-Profile. Diese haben nichts mit Hostprofilen für ESXi zu tun, die in Verbindung mit einer Enterprise-Plus-Lizenz schon seit Jahren eine konsistente Hostkonfiguration ermöglichen, haben aber einen ähnlichen Zweck. Mit ihnen können Admins vCenter-Konfigurationen auf mehrere Systeme verteilen, vorhandene Systeme auf Konformität prüfen und gegebenfalls Konfigurationen wiederherstellen.

Mit vCenter-Server-7-Profilen lässt sich die vCenter-Konfiguration im Bereich Management, Netzwerk, Benutzer und Berechtigungen über eine REST-API importieren und exportieren. Der Export speichert die Konfiguration in einer JSON-Datei, die sich auf bis zu 100 weitere vCenter-7-Server übertragen lässt. Das Feature ist derzeit jedoch nur über die Rest-API verfügbar. Admins können damit in der Praxis beispielsweise auf einem "Referenz-vCenter" sämtliche erforderlichen Konfigurationen und Einstellungen einrichten und dieses System später als eine Art Golden-Master für weitere zu konfigurierenden vCenter-Systeme verwenden.

Das Anpassen kann auch selektiv erfolgen und etwa bei einigen vCenter-Systemen lediglich die Appliance- und Netzwerkkonfigurationen betreffen, während der Adminstrator auf anderen vCenter-Systemen sämtliche Konfigurationseinstellungen, also etwa auch die Benutzerkonfigurationen überträgt.

vCenter-Updates besser planen

Neu im vSphere-Client ist auch der vCenter Update Planner. Er zeigt sowohl als Nachricht in der Ereignisanzeige als auch im dafür vorgesehenen "Updates"-Menü bei im Inventar markiertem logischen vCenter-Objekt die jeweils verfügbaren vCenter-Updates mit allen erforderlichen Detailinformationen an. Dazu zählen auch ein Link auf die Release-Notes sowie eine praktische Schaltfläche, um nahtlos

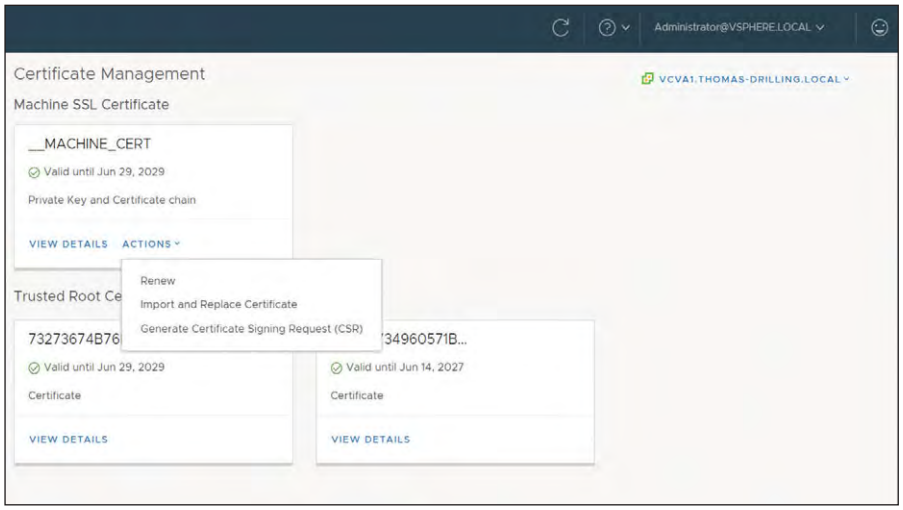

Bild 3: Die Zertifikatsverwaltung ist zum großen Teil in den vSphere-Client gewandert.

zur Update-Rubrik im Appliance-Management-Interface zu wechseln. Außerdem kann der Admin die potenziellen Auswirkungen eines geplanten Updates im Voraus prüfen und erfährt bei Erfolg sogar, wie lange die vCenter-Downtime beim Update wäre.

Darüber hinaus bietet der Update Planner bei im Inventar markierten vCenter-Objekten praktische Interoperabilitätsberichte im Menü "Monitor / Interoperability" an. Mit deren Hilfe kann der Admin – vorausgesetzt er hat bei der Bereitstellung dem "Customor Experience Improvement Program" (CEIP) zugestimmt – die Auswirkungen des Updates auf angeflanschte Produkte wie Operations Manager prüfen und das Ergebnis der Prüfung bei Bedarf als Report exportieren.

vCenter-Server-Identitätsanbieterverbund

Das oben erwähnte Single Sign-on umfasst im vCenter einen Security Token Service (STS), einen Verwaltungsserver, den erwähnten vCenter-Lookup-Service und den Verzeichnisdienst VMware Directory Service (vmdir), alle bereitgestellt am PSC. Zudem wird der VMware-Verzeichnisdienst wie oben beschreiben auch für die Zertifikatverwaltung verwendet. Im Verlauf einer Standardinstallation werden der STS, der Verwaltungsserver, der Identitätsverwaltungsdienst und der Verzeichnisdienst automatisch bereitgestellt und konfiguriert. Dieser speichert die vCenter-SSO-Informationen und die Zertifikatsinformationen.

Dabei stehen dem Admin verschiedene Identitätsquellen zur Verfügung, um vCenter-SSO eine oder mehrere Domänen hinzuzufügen. Unter einer Domäne versteht vSphere ein Repository für Benutzer und Gruppen, das dem vCenter-Single-Sign-on-Server zur Benutzerauthentifizierung dient. Benutzer können sich nur am vCenter-Server anmelden, wenn sie Teil einer Domäne sind, die vCenter-SSO als Identitätsquelle kennt. Neben der VMware-eigenen Identitätsquelle, die der VMware-Verzeichnisdienst bereitstellt, ist hierfür seit Version 5.1 auch das Microsoft Active Directory als Identitätsquelle geeignet. In beiden Fällen finden Überprüfung und Authentifizierung aber auf dem vCenter statt.

Neu in vSphere 7 ist, dass IT-Verantwortliche in der Lage sind, auch einen vCenter-Server-Identitätsanbieterverbund über den vSphere-Client oder die API zu konfigurieren. Im Augenblick besteht allerdings nur Unterstützung für die Active Directory Federation Services (AD FS) als externen Identitätsanbieter, weitere sollen aber folgen.

Im Gegensatz zur Möglichkeit, dem vCenter-SSO das AD als Identitätsquelle hinzuzufügen, verlagert der neue vCenter-Server-Identitätsanbieterverbund den Prozess der Authentifizierung komplett auf das externe System. Voraussetzung hier ist, dass ADFS für Windows Server 2016 oder höher läuft und ADFS mit dem Active Directory verbunden ist. Ferner gilt es, auf dem Domaincontroller eine Anwendungsgruppe für vCenter-Server im Rahmen des Konfigurationsvorgangs in ADFS zu erstellen.

Neue Partitionen auf dem Host

Die wichtigste vSphere-7-Neuerung auf Hostebene ist sicherlich die native Kubernetes-Integration in den Hypervisor. Diese ist auch die Hauptursache dafür, dass VMware für den VM-Kernel ein komplette Überarbeitung des Code vornehmen musste und damit unter anderem der Grund für die lange Lebenszeit des Vorgänger-Releases.

Weitere Änderungen gab es aber auch am Standard-Partitionslayout von ESXi. Das ursprüngliche FAT-basierende Partitionslayout sah hier bekanntlich neben der 4 MByte großen System-Boot-Partition und den beiden 250 MByte großen identischen Boot-Bank-Partitionen (jeweils unter "/bootbank" und "/altbootbank" im ESXi-Dateisystem eingebunden) auch eine 110 MByte große Dump-Partition (für Systemabsturz-Abbilder) sowie eine 285

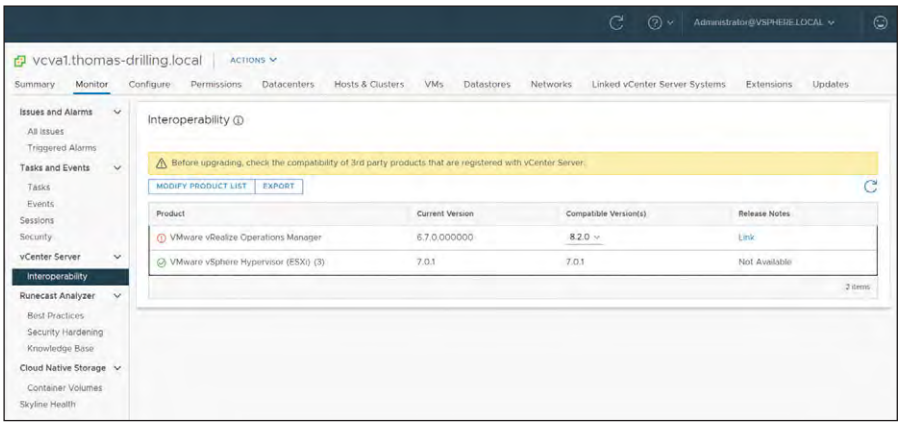

Bild 4: Der vCenter Update Planner prüft bei Bedarf die Update-Auswirkungen auf Drittanbietersoftware.

MByte umfassende, unter "/store" gemountete Partition für persistente Daten wie Downloads oder VMware-Tools-ISOs vor. Schließlich existiert – sofern genügend Platz auf dem Boot-Medium vorhanden ist – eine 4 GByte große Scratch-Partition für die Logdateien des Kernels unter "/scratch". Ein Installationsmedium wie zum Beispiel ein USB-Stick benötigte hier im Minimalfall nicht mehr als 5 GByte Platz. Handelte es sich dagegen beim Boot-Medium beispielsweise um eine SAS-Platte (jedenfalls nicht um ein Flash-Medium) wurde auf dieser, sofern noch mindestens 4 GByte nicht zugeordneter Festplattenplatz vorhanden war, zusätzlich eine VMFS-Partition für virtuelle Maschinen angelegt.

Wegen der I/O-Empfindlichkeit von USB- und SD-Geräten erstellt das Installationsprogramm nur eine Locker-Partition auf diesen Geräten, um VM-Tools- und Core-Dump-Dateien zu speichern, keine Scratch-Partition. Die Scratch-Partition befindet sich dann in einer RAM-Disk, die unter "/tmp" eingebunden ist.

Faktisch entscheidet also lediglich die Anbindung (USB) über die Bereitstellung von ESXi im Embedded- oder Installable-Modus. Generell gilt nach wie vor, dass sich ESXi auf Flash-Devices (USB-Sticks, SD-Cards), einer separaten Boot-Festplatte oder einem virtuellen Laufwerk eines RAID-Controllers installieren lässt. Beim Installieren von ESXi 7 wird das Bootmedium stets mit einer GPT-Partitionstabelle mit vier (Embedded) oder fünf Partitionen (Installable) beschrieben. Neu am vSphere-7-Partitionslayout ist die sogenannte ESX-OSData-Partition.

So benötigen Sie für die Installation von ESXi 7.0 nun ein Startgerät mit mindestens 8 GByte (bei USB- oder SD-Geräten) plus eine 32-GByte-Festplatte für die neue OSData-Partition. Diese führt die ursprünglichen Partitionen "small-core-dump", "large-core-dump", "locker" und "scratch" zu einer Partition vom Typ VMFS-L zusammen. Das wirkt sich auf ein ESXi-Upgrade aus, indem es das Startgerät neu partitioniert und die ursprünglichen Core-Dump-, Locker- und Scratch-Partitionen in das ESX-OSData-Volume konsolidiert.

War der Syslog-Dienst vorher zum Speichern von Logs auf der lokalen 4-GByte-VFAT-Scratch-Partition konfiguriert, migrieren Logs nun ins Verzeichnis "var/run/log" des ESX-OSData-Volumes. Ferner verschwinden die VMware-Tools von der ursprünglichen Locker-Partition und diese wird dann gelöscht. Ebenso Adieu sagen die Core-Dump-Partition und die auf der Scratch-Partition gespeicherten Core-Dump-Dateien. Ist kein benutzerdefiniertes Core-Dump-Ziel konfiguriert, kommt als Core-Dump-Speicherort per Default eine Datei auf dem ESX-OSData-Volume zum Einsatz. Bei einer Neuinstallation von ESXi haben Admins nun im Prinzip drei Möglichkeiten (abgesehen von Auto Deploy):

- Ein USB- oder SD-Gerät mit 8 GByte plus eine zusätzliche lokale Festplatte mit 32 GByte, wobei sich die ESXi-Startpartitionen dann auf dem USB- oder SD-Gerät und das ESX-OSData-Volume auf der lokalen Festplatte befindet.
- Bei einem Installationsmedium mit mindestens 32 GByte enthält diese Festplatte die Startpartitionen und das ESX-OSData-Volume.
- Hat die lokale Festplatte mehr als 142 GByte, wird auf dieser noch eine VMFS-Partition für VMs angelegt.

Neuerungen gibt es auch bei der Lizenzierung von ESXi. Zwar gilt nach wie vor im Prinzip, dass die Lizenzierung nach den in den ESXi-Hosts vorhandenen CPU-Sockeln erfolgt, ein Server mit zwei CPUs also mindestens eine CPU-Lizenz-Kapazität von zwei benötigt. Neu ist aber die Begrenzung auf 32 CPU-Kerne. Spielte die Anzahl der Kerne bisher keine Rolle, benötigen Sie in vSphere 7 in jedem Fall mehr als eine Lizenz, wenn mehr als 32 Kerne vorhanden sind – auch bei nur einer CPU.

Genauere Uhrzeit

ESXi-Hosts akzeptieren neben dem uralten NTP-Protokoll nun auch das um Größenordnungen genauere Precision Time Protocol (PTP) als Zeitgeber, um Uhrzeit und Datum des Hosts mit einem Zeitserver zu synchronisieren. Dieses bietet insbesondere Finanzanwendungen auf virtuellen Maschinen eine akzeptable Taktung, da sich nun auch VMs mit einer virtuelle Precision Clock ausstatten lassen. Diese umgeht für eine bessere Zeitsynchronisation den virtuellen Netzwerk-Stack und den Gastnetzwerk-Stack und ermöglicht dem Gastbetriebssystem, eine Taktgenauigkeit im Bereich von einer Millisekunde zu erreichen.

Außerdem ist es nun auch möglich, VMs mit einem virtuellen Watchdock Timer (WDT) auszurüsten. Damit lassen sich künftig auch Hochverfügbarkeitslösungen wie Red Hat High Availability oder Microsoft-SQL-Failover-Cluster auf Basis von virtuellen Maschinen realisieren.

Trusted Authority schützt Infrastruktur

Die mit Version 7 ebenfalls eingeführte vSphere Trust Authority (vTA) soll sicherstellen, dass die ESXi-Infrastruktur selbst sicher ist beziehungsweise repariert wird, falls ihre Sicherheit fraglich ist. Das Feature verwendet eine Hardware-Vertrauensbasis, um die Umgebung zu schützen, erzeugt Berichte über die Software, die auf einem Host läuft und misst beziehungsweise attestiert Systeme mithilfe eines Trusted Platform Module (TPM). TPMs fungieren als kryptografischer Prozessor, speichern Informationen wie Schlüssel, Zertifikate und Signaturen und können ermitteln, ob die Integrität eines Systems intakt ist, indem eine "Attestierung" erfolgt.

VMware verwendet TPMs für Remote-Bestätigungen von ESXi-Hosts, um beispielsweise die Echtheit der gestarteten Software zu bestätigen. Ferner integriert vTA einen Key-Provider-Dienst, der als Schnittstelle zum für Verschlüsselung obligatorischen Key Management Server (KMS) fungiert. Solche Bestätigungen stellen sicher, dass auf den jeweiligen ESXi-Hosts "echte" VMware-Software oder von VMware signierte Partnersoftware läuft. Bestätigungen fußen auf Messungen, die sich in einem auf dem ESXi-Host installierten TPM-2.0-Chip befinden. So kann unter vSphere mit Trust Authority ein ESXi-Host nur dann auf Verschlüsselungsschlüssel zugreifen und Kryptografievorgänge durchführen, wenn er bestätigt wurde.

vSphere 6.7 konnte eine Attestierung lediglich anzeigen und abgesehen von einem Alarm hatte eine fehlgeschlagene At-

testierung keine weitere Auswirkung, Sie konnte also auch nicht verhindern, dass ein ursprünglich sicherer Workload, der die VM-Verschlüsselung nutzt, durch den Distributed Resource Scheduler (DRS) wieder auf einen nicht kryptografisch sicheren Host verschoben wurde. Zudem löst Trust Authority in vSphere 7 das Problem, dass die Verschlüsselungsschlüssel in vSphere 6.7 selbst anfällig sind, weil der vCenter-Server, der in Version 6.5/6.7 alle diese Keys für einen Cluster verarbeitet, sich nicht selbst verschlüsseln lässt. Bei vSphere 7 befindet sich das vCenter nicht mehr im kritischen Pfad für die Schlüssel, da nun der Attestierungs-Cluster neben seiner Aufgabe als Bestätigungsdienst die Verteilung der Keys übernimmt. Somit ist der vCenter-Server selbst verschlüsselbar. Am Workflow ändert sich dadurch nichts.

Lastenausgleich jetzt in den VMs

Änderungen gab es in vSphere 7 auch am DRS-Lastausgleich-Algorithmus. Frühere Versionen von DRS aggregieren die Rechenkapazität für die Cluster-Last, treffen also ihre Lastausgleichsempfehlung, die letztendlich einen oder mehrere vMotion-Vorgänge verursacht, auf Hostebene.

Im Grunde stellte DRS in vSphere 6.7 und früher stets sicher, dass alle Hosts des Cluster-Ressource-Pools möglichst gleichmäßig ausgelastet sind in Bezug auf CPU, Arbeitsspeicher und Netzwerk. Dazu aggregierte DRS sämtliche Hostressourcen zu einem Cluster-Ressource-Pool und überwachte dann die Lastsituation auf den einzelnen Hosts. In vSphere 7 verlagert VMware den DRS-Algorithmus auf die VM-Ebene, um sicherzustellen, dass die Ressourcenanforderungen jeder spezifischen VM immer erfüllt sind. VMware führt dazu einen neuen DRS-Score auf VM- und Cluster-Level ein, der sämtliche Ressourcenanforderungen des Workloads berücksichtigt, einschließlich etwaiger Reservierungen.

Ferner arbeitet VMware weiter daran, die Abhängigkeit des DRS-Features vom vCenter zu beseitigen und führt dazu einen neuen Typ von Agenten-VM ein. Solche vSphere-Cluster-Service-Maschinen (vCLS- VMs) werden automatisch für jeden vSphere-Cluster bereitgestellt, den ein vCenter-Server in Version 7.0 Update 1 verwaltet. Hierbei handelt es sich um kompakte Agenten-VMs, die ein Cluster-Quorum bilden. Sie korrigieren sich selbst, das bedeutet vCLS versucht stets, diese Agenten-VMs automatisch zu instanziieren oder einzuschalten, wenn die erforderliche Anzahl nicht mehr verfügbar ist.

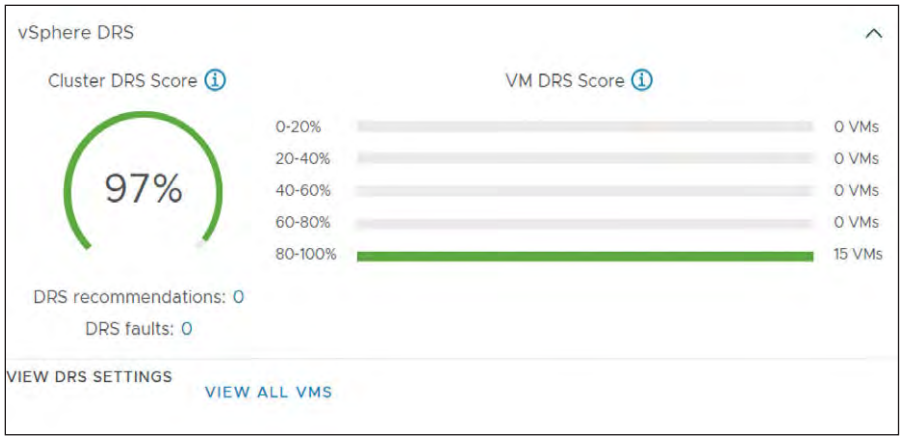

Bild 5: In vSphere 7 wird der DRS-2.0-Lastausgleichsalgorithmus jede Minute ausgeführt.

Ausgebaute Storage-Features

Auch bei der Integration neuer Storage-Technologien gehts ESXi stets mit der Zeit. So lässt sich in vSphere 7 moderner NVMe-Speicher entweder direkt über eine PCIe-Schnittstelle oder remote über verschiedene Fabric-Transport-Protokolle an einen Host anschließen. vSphere 7 unterstützt NVMe over RDMA beispielsweise in Form der RoCE-v2-Technologie (RDMA over converged Ethernet) – in VMware auch als "Shared NVMe over Fabrics" bezeichnet – optional aber auch in Form von NVMe-oF (eine Technologie, die NVMe auf dem Fibre-Channel-Protokoll abbildet). In diesem Zusammenhang hat VMware zudem die Pluggable Storage Architecture (PSA) um ein High-Performance-Plug-in (HPP) erweitert, das als Standard-Plug-in für NVMe-oF-Ziele dient. Das HPP unterstützt nur ALUA-Ziele (Active-Active und impliziter Asymetric Logical Unit Access) und verbessert die Leistung ultraschneller Flash-Geräte, die unter ESXi installiert sind.

Darüber hinaus bietet vSphere 7 iSER-Unterstützung für vSphere Virtual Volumes. Die iSCSI-Erweiterung für RDMA (iSER) erlaubt leistungsstarke iSCSI-Konnektivität für Standard-RDMA-Netzwerkkarten. Ist das iSER-Protokoll aktiviert, erlaubt dies dem iSCSI-Framework auf dem ESXi-Host den RDMA-Transport anstelle von TCP/IP zu verwenden. Weitere umfangreiche Erweiterungen im Storage-Bereich erstrecken sich auf vSAN 7 und Container-Speicher für Kubernetes, die wir an anderer Stelle im Detail betrachten.

Neu im Programm: Lifecycle Manager

In vSphere 7 hat VMware auch die Verwaltung von Updates (Patches) für Hosts und VMs sowie Upgrades in Form des Update Managers komplett überarbeitet und Letzteren durch den neuen Lifecycle Manager (vLCM) ersetzt. Mit diesem lassen sich genau wie beim vSphere Update Manager (VUM) Hosts und VMs updaten sowie Hosts upgraden. Der neue Lifecycle Manager führt allerdings darüber hinaus das Konzept des "Cluster-Image" ein.

Mit einem solchen Image kann der Admin eine deklarative "Desired State"-Philosophie bei der Lebenszyklusverwaltung der Hosts eines ESXi-7-Clusters verfolgen. Hierbei definiert er auf Cluster-Ebene ein Image, das den gewünschten Zustand des gesamten ESXi-Clusters (Basis-Image, Hersteller, Firmware- und Treiber-Add-ons sowie Komponenten) beschreibt und mit dessen Hilfe IT-Verantwortliche bei Bedarf (wie etwa einer negativen Compliance-Prüfung) einen oder alle Hosts im Cluster gegen dieses Cluster-Image standardisieren. Das Cluster-Image lässt sich zum Beispiel beim manuellen Erstellen eines neuen Clusters oder beim Verwenden des neuen Cluster-Quickstart-Assistenten direkt angeben.

Gleichwohl ist vLCM abwärtskompatibel mit VUM und beherrscht auch den tra-

ditionellen Modus mit Baselines und VIBs, verhält sich dann also exakt wie VUM. Baselines definieren eine Auswahl von VIBs, gegen die der jeweilige Host standardisiert wird. Stellen Sie allerdings erst einmal auf Cluster-Images um, gibt es kein Zurück mehr zu Baselines. Allerdings ist es derzeit noch empfehlenswert, bei Baselines zu bleiben, falls Sie planen, auch NSX-v via VUM zu verwalten. Derzeit unterstützen nur vSphere und vSAN ab Version 7 Cluster-Images. Außerdem müssen dann selbstverständlich alle ESXi-Hosts auf Version 7 sein.

Neue Konfigurationsmaxima und virtuelle Hardwareversion

Schließlich erhöhen sich mit jeder neuen ESXi-Version die unterstützten Konfigurationsmaxima und jedes neue Major-Release geht zudem mit einer Aktualisierung der virtuellen Hardwareversion für VMs einher. Da sich die Vollvirtualisierung von VMware insbesondere im Layer der virtuellen Hardware von der Paravirtualisierung bei Hyper-V und Xen unterscheidet, kommt dem Level der virtuellen Hardware bei VMware eine große Bedeutung zu.

Die aktuellen Versionen 17 (vSphere 7) und 18 (vSphere 7 Update 1) lassen sich für jede VM über den Lifecycle Manager aktualisieren. Da eine Beschreibung von Konfigurationsmaxima und unterstützen virtuellen Hardwaregeräten sowie auf Hostebene neu unterstützte Hardware eher referenziellen Charakter hat, verweisen wir hierzu auf die Dokumentation [3] und greifen nur einige Beispiele heraus.

Bei den Konfigurationsmaxima unterstützen Hosts mit vSphere 7 nun bis zu 768 logische CPUs und 256 vCPUs für jede virtuelle Maschine. Hosts können über bis zu 16 TByte RAM verfügen, eine einzelne VM darf maximal 6 TByte besitzen. Hosts erlauben nun bis zu 12 TByte NVMe-Speicher, eine einzelne VM bis zu 6 TByte. Jedes vCenter mit Version 7 kann bis zu 45.000 registrierte VMs verwalten, davon 40.000 eingeschaltete. Im Embedded Linked Mode lassen sich bis zu 15 vCenter-System verknüpfen. Ein vSphere-Cluster ist auf 64 Hosts beschränkt und kann bis zu 8000 VMs aufnehmen.

Im Kontext neu unterstützter virtueller Hardware ist neben Precision Clock und WDT der Support für Intels Software-Guard-Extensions-(SGX)-Technologie erwähnenswert. Allgemein können Anwendungen mit Intel SGX private Speicherbereiche erstellen, sogenannte "Enklaven". Auf Daten in Enklaven haben dann nur die dazu vorgesehenen Programme Zugriff, das heißt die Enklaven-Region ist von anderen Programmen, Betriebssystemen und sogar dem Hypervisor (sollte dieser kompromittiert sein) isoliert. Virtual SGX setzt dann Intel-SGX-VMs aus, die in einer vSphere-Umgebung laufen.

Darüber hinaus unterstützten ESXi-Hosts in vSphere 7 die Kommunikation zwischen PVRDMA-Geräten. VMware führt dabei das Konzept nativer Endpunkte ein. Hierbei geht es um die Kommunikation zwischen PVRDMA-Geräten mit Nicht-PVRDMA-Devices, also solchen, die zwar RDMA-fähig sind, selbst aber keine PVRDMA-Geräte sind. In vSphere 7 können die nativen Endpunkte mit PVRDMA-Geräten kommunizieren, dann allerdings ohne vSphere-vMotion-Support.

Apropos vMotion: Hier hat VMware den Algorithmus grundlegend überarbeitet, sodass vMotion eine deutliche Verbesserung der Performance bei Datenbanken beziehungsweise "Monster-VMs" – also im Wesentlichen bei unternehmenskritischen Anwendungen – ermöglicht.

Neu ist hierbei auch die erweiterte vMotion-Kompatibilität für vSGA-GPUs. Dies ist ein erneuter Ausbau der vorhandenen erweiterten vMotion-Kompatibilitätsarchitektur, die ebenfalls eine gemeinsame Basislinie von GPU-Funktionssätzen in einem Cluster definiert. Features, die nicht in der angewendeten Baseline enthalten sind, werden maskiert und sind nicht für VMs verfügbar. Das Feature unterstützen sowohl Hardware-GPUs als auch Software-GPU-Renderer.

VMK-Treiber abgelöst

vSphere 7 ist die erste Version ist, die zugunsten eines nativen Treiber-Stacks vollständig auf VMKlinux-Treiber verzichtet. Das ist bemerkenswert, denn obwohl es sich beim VMkernel um eine Eigenentwicklung von VMware handelt, weist der monolithische Kernel Ähnlichkeiten mit Linux auf. Das war im Hinblick auf die Treiberversorgung von der ersten Version an bedeutsam, denn der VMkernel nutzt seit den ersten ESX-Tagen von Linux abgeleitete Treibermodule, um möglichst eine Vielzahl von Hardwaregeräten zu unterstützen.

ESX punktete so vom Start weg mit hoher Hardwarekompatibilität, allerdings auf Kosten der Einführung einer zusätzlichen Ebene zur Treiberemulation. Die Paravirtualisierung bei Hyper-V kennt das Problem nicht, da Gastgeräte aus einem modifizierten Gast-Kernel via Hyper-Calls direkt auf die von der Parent-Partition unterstützen Gerätetreiber zugreifen können.

Diese Übersetzungsschicht braucht ESXi, um die Kommunikation zwischen dem VMkernel und den Linux-Treiber-Modulen zu ermöglichen. Diese Ebene wird auch VMKlinux genannt. Seit vSphere 5.5 arbeitet VMware nun daran, einen nativen ESXi-Treiber-Stack einzuführen, um den VMKlinux-Treiber-Stack nach und nach aufzulösen, was nun mit vSphere 7 erstmals vollständig der Fall ist.

Fazit

Tanzu und die Kubernetes-Integration fanden im Vorfeld der Veröffentlichung von vSphere 7 die meiste Aufmerksamkeit, waren sie doch strategische Entscheidungen von VMware, die den vSphere-Code grundlegend verändern. Doch dieser Überblick zeigt, dass auch die Standardfeatures zur Virtualisierung deutliche Veränderungen und Verbesserungen erfahren haben. Wie Sie diese in der Praxis einsetzen und verwalten, legen wir Ihnen im Rest dieses Sonderhefts dar. *(jp)*

Link-Codes

[1] VMware-vSphere-Blog
ls111

[2] Ende des Web-Clients
ls112

[3] vSphere-Konfigurationsmaxima
ls113