vRealize Suite - Overzicht

vRealize Suite 2017

vmware®

U vindt de recentste technische documentatie op de website van VMware:

https://docs.vmware.com/nl/

Op de VMware-website vindt u tevens de nieuwste productupdates.

Als u opmerkingen over deze documentatie heeft, kunt u uw feedback sturen naar:

docfeedback@vmware.com

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

Inhoud

Inleiding op VMware vRealize Suite

Het Overzicht van *VMware vRealize Suite* biedt een overzicht van de architectuur van vRealize Suite, naast informatie over het installeren, configureren en gebruiken van dit product.

Om u aan de slag te helpen, leiden algemene beschrijvingen van de installatie, de configuratie en het gebruik u naar de specifieke sets individuele producten voor meer gedetailleerde concepten en procedures.

Doelgroep

Deze informatie is bedoeld voor iedereen die de producten van vRealize Suite wil implementeren en gebruiken om een Software-Defined Data Center (SDDC) te controleren en te beheren. Deze informatie is geschreven voor ervaren Windows- of Linux-systeembeheerders die bekend zijn met de technologie van virtual machines en de bewerkingen in datacenters.

Woordenlijst VMware Technical Publications

VMware Technical Publications beschikt over een woordenlijst met termen die u mogelijk nog niet kent. Ga naar http://www.vmware.com/support/pubs voor een definitie van de termen die in de technische documentatie van VMware worden gebruikt.

Inleiding tot vRealize Suite 1

vRealize Suite biedt een allesomvattend cloudbeheerplatform voor de levering, de controle en het beheer van toepassingen in VMware vSphere en andere hypervisors, inclusief de fysieke infrastructuur, en particuliere en openbare clouds. vRealize Suite is beschikbaar als Standard-, Advanced- en Enterprise-editie.

Dit hoofdstuk omvat de volgende onderwerpen:

vRealize Suite - Mogelijkheden

Intelligente bewerkingen, geautomatiseerde IT, Infrastructure as a Service (IaaS) en DevOps-ready IT worden het meest gebruikt als oplossing voor cloudbeheer. Intelligente bewerkingen helpen bewerkingen van datacenters te stroomlijnen en te automatiseren. Geautomatiseerde IT, IaaS en DevOps-ready IT maken de levering van toepassings- en infrastructuurservice mogelijk.

Beheer van intelligente bewerkingen

Intelligente bewerkingen reageren proactief op de status, prestaties en het capaciteitsbeheer van IT-services in heterogene en hybride cloudomgevingen om de prestaties en beschikbaarheid van IT-services te verbeteren.

Geautomatiseerde IT tot IaaS

Geautomatiseerde IT en IaaS automatiseren de levering en het continue beheer van de IT-infrastructuur om de reactietijd voor aanvragen voor IT-bronnen te beperken en het continue beheer van ingerichte bronnen te verbeteren.

DevOps-Ready IT

DevOps-ready IT helpt u een cloudoplossing te bouwen voor ontwikkelingsteams die een complete applicatiestack kunnen leveren met deze mogelijkheden:

- De ontwikkelaarskeuze ondersteunen in de vorm van API- en GUI-toegang tot bronnen.
- Bronnen inrichten in een hybride cloud.
- Het bereik van de oplossing uitbreiden door continue levering te regelen om het leveringsproces voor toepassingen te versnellen.

vRealize Suite -edities en producten

vRealize Suite is beschikbaar als Standard-, Advanced- en Enterprise-editie. Een vRealize Suite-editie bevat afzonderlijke producten met verschillende productedities en verschillende mogelijkheden.

De standaard, geavanceerde en zakelijke edities van vRealize Suite leveren elk een verschillende set van functies, zoals hieronder in de tabel wordt weergegeven.

Tabel 1-1. Kenmerken vRealize Suite -editie

vRealize Suite-product	Kenmerk van vRealize Suite	Standard-editie	Advanced-editie	Enterprise-editie
vRealize Operations Manager (omvat vRealize Log Insight en vRealize Infrastructure Navigator)	Logboekanalyse	Ja	Ja	Ja
	Operations-platform	Ja	Ja	Ja
	Visualisatie	Ja	Ja	Ja
	Beleidsbeheer	Ja	Ja	Ja
	Controle en analyse van prestaties	Ja	Ja	Ja
	Capaciteitsbeheer	Ja	Ja	Ja
	Workload-balans	Ja	Ja	Ja
	Wijzigings-, configuratie- en nalevingsbeheer	Ja	Ja	Ja
	Toewijzing toepassingsafhankelijkheid	Ja	Ja	Ja
	Toepassingsbewaking		Ja	Ja
vRealize Business Cloud	Automatische virtuele infrastructuurmeting, kostprijsberekening en prijsstelling	Ja	Ja	Ja
	Automatische prijsstelling servicecatalogus, geïntegreerd met vRealize Automation	Ja	Ja	Ja
	Verbruiksanalyse virtuele infrastructuur	Ja	Ja	Ja
	Exporteerbare gegevensset die automatische rapportage mogelijk maakt	Ja	Ja	Ja
	Kostenvergelijking openbare cloud en virtualisatie-infrastructuur	Ja	Ja	Ja
	Kostprijsberekening, verbruiksanalyse en prijsstelling openbare cloud	Nee	Ja	Ja
	Rolgebaseerde showback in virtuele infrastructuur en openbare cloud	Nee	Ja	Ja
	Datacenter-optimalisatie, geïntegreerd met vRealize Operations Manager	Nee	Ja	Ja
	Kwantificeren van terugwinningsmogelijkheden van virtuele infrastructuur, geïntegreerd met vRealize Operations Manager	Nee	Ja	Ja

Tabel 1-1. Kenmerken vRealize Suite -editie (Vervolgd)

vRealize Suite-product	Kenmerk van vRealize Suite	Standard-editie	Advanced-editie	Enterprise-editie
	Aangepaste rapportage, visuele grafieken en API voor automatische gegevensextractie	Nee	Ja	Ja
vRealize Automation	Selfservice met uniforme servicecatalogus en API-functies	Nee	Ja	Ja
	Ondersteuning van virtuele, fysieke en openbare cloud voor meerdere leveranciers	Nee	Ja	Ja
	IaaS. Enkele en meerlagige machine-inrichtingen met omvattend levenscyclusbeheer	Nee	Ja	Ja
	IaaS. Netwerk- en beveiligingsconfiguratie	Nee	Ja	Ja
	Anything as a service (XaaS). Ontwerpen van aangepaste IT-services	Nee	Ja	Ja
	XaaS. Kan worden ingezet als een catalogusitem of Day Two-bewerking	Nee	Ja	Ja
	Toepassingsontwerp. Ontwerpen van softwareonderdelen en inrichten van toepassingsstacks	Nee	Nee	Ja
	Toepassingsontwerp. Dynamische softwarescriptverwerking en afhankelijkheidskoppelingen	Nee	Nee	Ja
	Toepassingsontwerp. Toepassingsgerichte netwerk- en beveiligingsconfiguratie	Nee	Nee	Ja

vRealize Suite -producten

VMware vRealize Suite is inclusief bepaalde producten of een subset van deze producten, afhankelijk van de vRealize Suite-editie die u aanschaft.

Tabel 1-2. Producten meegeleverd met vRealize Suite

Productnaam	Beschrijving
vRealize Suite Lifecycle Manager	Automatiseert Day 0 to Day 2-bewerkingen van de hele vRealize Suite voor een vereenvoudigde operationale ervaring. vRealize Suite Lifecycle Manager automatiseert lifecycle management met één scherm, waardoor klantbronnen worden vrijgemaakt en deze kunnen worden gebruikt voor bedrijfskritieke initiatieven, terwijl time to value, betrouwbaarheid en consistentie worden verbeterd.
vRealize Operations Manager	Verzamelt prestatiegegevens van elk object op elk niveau van uw virtuele omgeving, van afzonderlijke virtual machines en schijfstations tot complete clusters en datacenters. Bewaart en analyseert de gegevens en gebruikt deze analyse om realtime informatie te geven omtrent problemen, of mogelijke problemen, overal binnen uw virtuele omgeving.
vRealize Infrastructure Navigator	Detecteert automatisch toepassingsservices, visualiseert relaties en wijst afhankelijkheden toe van toepassingen op gevirtualiseerde reken-, opslag- en netwerkbronnen.

Tabel 1-2. Producten meegeleverd met vRealize Suite (Vervolgd)

Productnaam	Beschrijving
vRealize Log Insight	Biedt schaalbare logboeksamenvoeging en indexering voor vRealize Suite, inclusief alle edities van vSphere, met realtime zoek- en analysemogelijkheden. Log Insight verzamelt, importeert en analyseert logboeken om realtime antwoord te geven op problemen met betrekking tot systemen, services en toepassingen binnen fysieke, virtuele en cloudomgevingen.
vRealize Automation	Helpt bij het implementeren en inrichten van bedrijfsrelevante cloudservices voor particuliere en openbare clouds, fysieke infrastructuur, hypervisors en openbare cloudproviders. vRealize Automation Enterprise omvat vRealize Automation Application Services.
vRealize Orchestrator	Vereenvoudigt de automatisering van complexe IT-taken en integreert met vRealize Suite-producten voor het aanpassen en uitbreiden van de servicelevering en het operationeel beheer, terwijl effectief wordt omgegaan met de bestaande infrastructuur, tools en processen.
vRealize Business	Geeft informatie over financiële aspecten van uw cloudinfrastructuur en stelt u in staat deze bewerkingen te optimaliseren en verbeteren.

vRealize Suite -edities en de productedities

Bepaalde productedities zijn verkrijgbaar als Standard-, Advanced- en Enterprise-editie van vRealize Suite.

Tabel 1-3. vRealize Suite softwareproduct-edities in Suite-edities

vRealize-producteditie	vRealize Suite Standard-editie	vRealize Suite Advanced-editie	vRealize Suite Enterprise-editie
VMware vRealize Automation Advanced-editie	Nee	Ja	Nee
VMware vRealize Automation Enterprise-editie	Nee	Nee	Ja
VMware vRealize Operations Management Suite (Advanced)	Ja	Ja	Ja
VMware vRealize Operations Management Suite toepassingscontrole	Nee	Nee	Ja
VMware vRealize Business CloudStandard-editie	Ja	Nee	Nee
VMware vRealize Business Cloud Advanced-editie	Nee	Ja	Ja
VMware vRealize Orchestrator Advanced-editie	Nee	Ja	Nee
VMware vRealize Orchestrator Enterprise-editie	Nee	Nee	Ja
VMware vRealize Log Insight	Ja	Ja	Ja
VMware vRealize Infrastructure Navigator	Ja	Ja	Ja

Licenties voor vRealize Suite

U kunt licenties voor de producten in vRealize Suite afzonderlijk verkrijgen of als onderdeel van vRealize Suite 2017.

U verkrijgt en gebruikt een licentietype voor het licentiëren van vRealize Suite-producten.

Tabel 1-4. Licentietypen die compatibel zijn met vRealize Suite -producten.

Licentietype	Licentiemogelijkheden
Afzonderlijke productlicentie	Sommige producten zijn verkrijgbaar als standalone producten die u kunt licentiëren op basis van het aantal virtual machines door gebruik te maken van de productlicentie. Afzonderlijke productlicenties zijn bedoeld voor workloads in de openbare cloud of workloads op fysieke hardware.
Overdraagbare licentie-eenheid (Portable License Unit, PLU) voor vRealize Suite	Met een overdraagbare licentie-eenheid (Portable License Unit, PLU) kunt u workloads binnen vSphere en hybride omgevingen inrichten en beheren, inclusief openbare en particuliere cloudproviders. Een PLU is een enkele SKU die workloads meet in vSphere en hybride omgevingen, en die metingen ondersteunt voor CPU's en virtual machines. Elke PLU licentieert één CPU voor een onbeperkt aantal virtual machines of 15 besturingssysteeminstanties.

Zie Licentieverlening, prijzen en verpakking van VMware vRealize Suite en vCloud Suite voor meer informatie over PLU's.

Overzicht van de vRealize Suite - architectuur 2

In de architectuur wordt beschreven hoe vRealize Suite-producten met elkaar en met systemen in het datacenter samenwerken om een Software-Defined Data Center (SDDC) te leveren.

Dit hoofdstuk omvat de volgende onderwerpen:

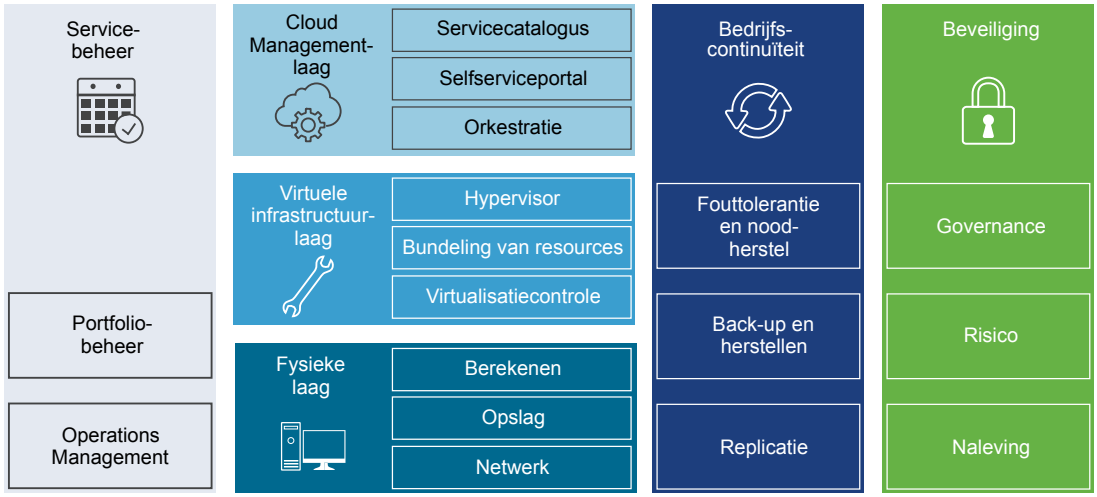
Software-Defined Data Center

Het Software-Defined Data Center (SDDC) biedt verschillende typen mogelijkheden, met meer complexe functies die voortbouwen op de onderliggende structuur. Als u alle vRealize Suite-functies wilt inschakelen, moet u een reeks installatie- en configuratiebewerkingen uitvoeren.

Het leveren van volledige operationele mogelijkheden van vRealize Suite aan uw organisatie of klanten is een gestructureerd proces. In een grote organisatie moeten mogelijk meerdere cycli van beoordeling, ontwerp, kennisoverdracht en oplossingsvalidatie worden doorlopen. Afhankelijk van uw organisatie moet u een uitgebreid proces plannen waarvoor mogelijk meerdere rollen nodig zijn.

Niet elke omgeving heeft alle vRealize Suite-mogelijkheden op elk moment nodig. Begin met het implementeren van de kerninfrastructuur voor het datacenter, zodat u mogelijkheden kunt toevoegen wanneer uw organisatie die nodig heeft. Mogelijk moet u voor elk van de SDDC-lagen een afzonderlijk implementatieproces plannen en uitvoeren.

Figuur 2-1. Lagen van het SDDC



Fysieke laag

De laagste laag van de oplossing omvat reken-, netwerk- en opslagonderdelen. Het rekenonderdeel bevat de x86-gebaseerde servers waarop de workloads voor het beheer, de rand en de tenant worden uitgevoerd. De opslagonderdelen bieden de fysieke basis voor het SDDC en de IT-automatiseringscloud.

Virtuele infrastructuurlaag

De virtuele infrastructuurlaag bevat het virtualisatieplatform met de hypervisor, bronpooling en virtualisatiebediening. VMware-producten in deze laag zijn vSphere, VMware NSX, ESXi en vCenter Server. Deze producten brengen een robuuste gevirtualiseerde omgeving tot stand waarin alle oplossingen kunnen worden geïntegreerd. Door bronnen te scheiden van de fysieke laag, beschikt u over de basis voor de integratie van VMware-oplossingen voor orkestratie en controle. Extra processen en technologieën bouwen voort op de infrastructuur om Infrastructure as a Service (IaaS) en Platform as a service (PaaS) mogelijk te maken.

Cloudbeheerlaag

De cloudbeheerlaag bevat de servicecatalogus die plaats biedt aan de voorzieningen die moeten worden geïmplementeerd, orkestratie, die de workflows levert om catalogusitems te implementeren, en de selfserviceportal waarmee eindgebruikers het SDDC kunnen gebruiken. vRealize Automation levert het portal en de catalogus, en ingesloten vRealize Orchestrator-mogelijkheden helpen bij het beheer van de workflows om complexe IT-processen te automatiseren.

Servicebeheer

Maak gebruik van servicebeheer om de werking van meerdere gegevensbronnen in het verspreide SDDC te volgen en te analyseren. Implementeer vRealize Operations Manager en vRealize Log Insight op meerdere knooppunten voor continue beschikbaarheid en snellere gegevensopname in logboeken.

Bedrijfscontinuïteit

Gebruik bedrijfscontinuïteit om back-uptaken te maken in vSphere Data Protection voor vRealize Operations Manager, vRealize Log Insight, VMware NSX en vRealize Automation. Als een hardwarefout optreedt, kunt u de onderdelen van deze producten herstellen vanuit de opgeslagen back-ups.

Beveiliging

VMware levert het Compliance Reference Architecture Framework en het Compliance Capable, Audit Ready-platform. Klanten gebruiken het platform om te voldoen aan nalevingsvereisten voor gevirtualiseerde workloads en om bedrijfsrisico's te beheren. VMware-producten en compatibele partnerproducten worden zorgvuldig toegewezen om te voldoen aan de vereisten van gezaghebbende bronnen zoals PCI DSS, HIPAA, FedRAMP en CJIS. De kerndocumenten voor het Compliance Reference Architecture Framework zijn:

- Handleidingen voor de toepasbaarheid van producten bevatten beschrijvingen van VMware-productsuites per product waarbij voorschriften, samen met voorschriftcontroles gerelateerd aan productkenmerken, worden besproken.
- Handleidingen voor architectuurontwerpen bevatten overwegingen voor het bouwen van een veilige, compatibele VMware vRealize-omgeving die voldoet aan de betreffende voorschriften.
- Documenten voor gevalideerde referentie-architectuur bieden bevindingen ter staving van de voorschriften op basis van een controlestudie die u kunt toepassen op uw omgeving.

Navigeer naar VMware Solution Exchange en selecteer Compliance Solutions voor toegang tot de documenten.

U kunt uw vRealize Suite-omgeving uitbreiden door extra VMware-producten en services te integreren. Deze producten hebben mogelijkheden zoals noodherstel naar de cloud, Software-Defined Storage en Software-Defined Networking.

Conceptontwerp van een vRealize Suite -omgeving

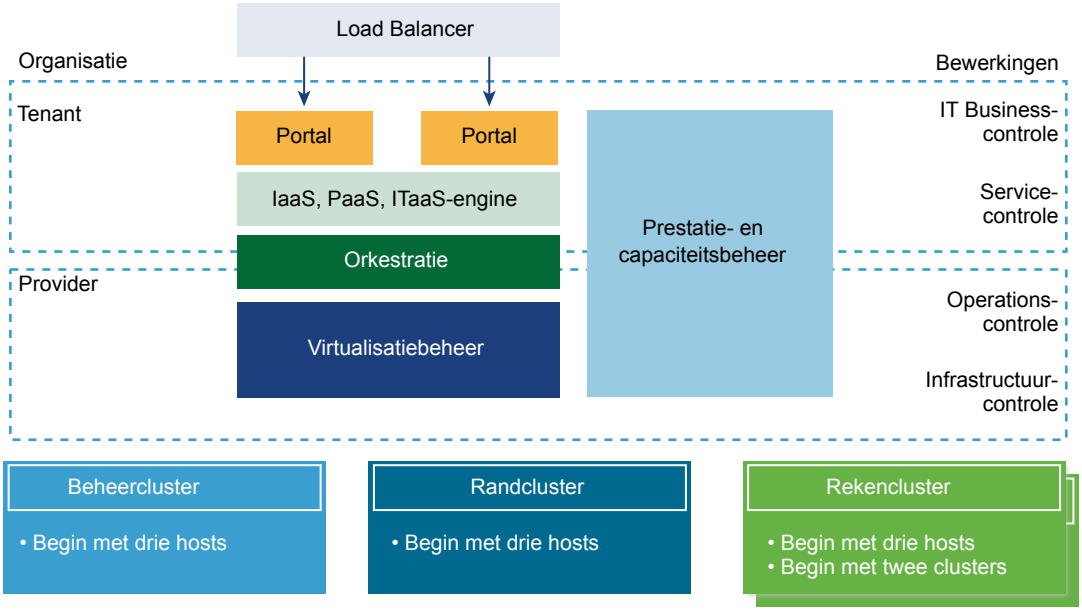
Als u wilt beginnen met het implementeren van vRealize Suite, hebt u slechts een beperkt aantal fysieke hosts nodig. De beste en veiligste basis voor het schalen van uw omgeving is het distribueren van uw hosts in beheer-, rand- en payloadclusters om de basis tot stand te brengen voor een implementatie die later kan worden geschaald naar tienduizenden virtual machines.

De clusters voeren de hele vRealize Suite-infrastructuur uit, inclusief de workloads van klanten.

Voor de implementatie en het gebruik van vRealize Suite moet een technologische en operationele transformatie plaatsvinden. Wanneer nieuwe technologieën worden geïmplementeerd in het datacenter, moet uw organisatie ook geschikte processen toepassen en de nodige rollen toewijzen. Zo hebt u mogelijk processen nodig om nieuwe informatie te verwerken die wordt verzameld. Elk beheerproduct heeft een of meer beheerders nodig, waarvan sommigen mogelijk andere toegangsniveaus hebben.

In het diagram ziet u technologische mogelijkheden en organisatorische constructies.

Figuur 2-2. Conceptontwerp van een vRealize Suite -omgeving



De clusters, elk met minimaal drie hosts, vormen de basis voor uw vRealize Suite-implementatie.

Beheercluster

De hosts in het beheercluster voeren de beheeronderdelen uit die vereist zijn voor ondersteuning van het SDDC. Voor elke fysieke locatie is één beheercluster vereist. U installeert handmatig de ESXi-hosts die het beheercluster uitvoeren en configureert ze om lokale harde schijven te gebruiken om op te starten.

Een beheercluster isoleert de bronnen. Productietoepassingen, testtoepassingen en overige typen toepassingen kunnen geen gebruikmaken van de clusterbronnen die zijn voorbehouden voor beheer, controle en infrastructuurservices. Het isoleren van de bronnen helpt om het prestatieniveau van de beheer- en infrastructuurservices te optimaliseren. Een apart cluster kan tegemoetkomen aan het beleid van de organisatie om een fysieke scheiding te hebben tussen de hardware voor beheer- en klantpayloads.

Randcluster

Het randcluster ondersteunt netwerkapparaten die zorgen voor de interconnectiviteit tussen omgevingen. Het biedt de beschermde capaciteit waarmee interne datacenternetwerken via gateways verbinding maken met externe netwerken. Netwerkrandservices en netwerkverkeerbeheer vinden plaats in het cluster. Alle extern gerichte netwerkconnectiviteit eindigt in dit cluster.

Een toegewezen vCenter Server-instantie die is gekoppeld met VMwareNSX, beheert de ESXi-hosts in het randcluster. Dezelfde vCenter Server-instantie beheert de payloadclusters die toegang nodig hebben tot externe netwerken.

Het randcluster hoeft niet groot te zijn en kan bestaan uit ESXi-hosts met minder capaciteit dan die in de beheer- en payloadclusters.

Payloadcluster

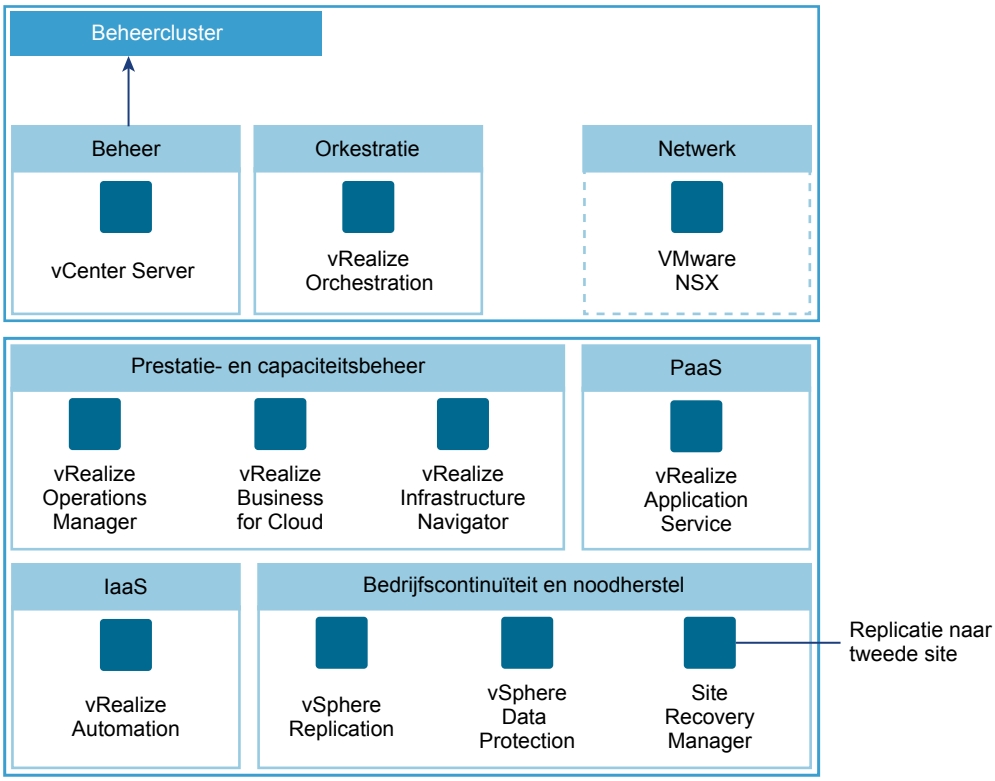
Het payloadcluster ondersteunt de levering van alle andere workloads voor niet-randclients. Het cluster blijft leeg tot een consument van de omgeving dit begint te vullen met virtual machines. U kunt opschalen door meer payloadclusters toe te voegen.

Wanneer het datacenter groeit, kunt u nieuwe rand- en payloadclusters maken, opschalen door bronnen toe te voegen of uitschalen door hosts toe te voegen.

vRealize Suite -producten in het beheercluster

Het aantal vRealize Suite-producten in het beheercluster neemt toe wanneer u mogelijkheden toevoegt. Een beheercluster moet een minimum set producten bevatten. U kunt de set producten uitbreiden wanneer u extra mogelijkheden nodig hebt.

Figuur 2-3. VMware-producten in het beheercluster



Minimum set beheerclusterproducten

Het beheercluster bevat altijd een vCenter Server-instantie. Als u de omgeving wilt voorbereiden voor IaaS- en PaaS-mogelijkheden, kunt u een vRealize Orchestrator-applicatie als vRealize Suite-product implementeren in een vroege fase.

vRealize Suite bevat standaard geen VMware-netwerkoplossingen. NSX for vSphere kan worden gebruikt voor de netwerkfuncties van het vRealize Suite-beheercluster. NSX biedt netwerkvirtualisatie van laag 2 tot laag 7, met beveiligingsbeleidsregels die workloads in het datacenter volgen voor snellere netwerkinrichting en beheer. U kunt NSX for vSphere met korting kopen als add-on.

Opmerking vCloud Networking and Security was een onderdeel van de vorige versie van vRealize Suite, en kon worden gebruikt voor de netwerkfuncties van het beheercluster. vCloud Networking and Security maakt niet langer deel uit van vRealize Suite.

Uitgebreide set producten

Als de complexiteit van de omgeving toeneemt, installeert u en configureert u extra producten. Zo bieden vRealize Operations Manager en gerelateerde producten bijvoorbeeld geavanceerde controlefuncties. vRealize Automation is het sleutelelement van uw IaaS-oplossing omdat u hiermee snel servers en desktops kunt modelleren en inrichten in virtuele en fysieke, privé en openbare, of hybride cloudinfrastructuren. Een vCenter Site Recovery Manager-instantie kan replicatie bieden aan een tweede site voor noodherstel.

SDDC-kerninfrastructuur

De SDDC-kerninfrastructuur bestaat uit vSphere- en vRealize Suite-producten zoals vRealize Operations Manager en vRealize Log Insight voor controle, vRealize Automation en vRealize Orchestrator voor beheerworkflows en vRealize Business Cloud voor kostenbepaling.

De kerninfrastructuur bevat de fysieke laag, de virtuele infrastructuurlaag en de cloudbeheerlaag. De kernvisualisatie maakt deel uit van de virtuele infrastructuurlaag, en de servicecatalogus en orkestratieservices zijn onderdeel van de cloudbeheerlaag. Met de virtuele infrastructuurlaag kunt u onderliggende fysieke bronnen consolideren en poolen. De cloudbeheerlaag biedt de orkestratiemogelijkheden en reduceert de kosten voor het gebruik van een intern datacenter. De servicebeheerlaag biedt controlemogelijkheden om potentiële problemen proactief te identificeren en op te lossen met voorspellende analyse en slimme waarschuwingen, zodat de prestaties en beschikbaarheid van toepassingen en infrastructuur worden geoptimaliseerd.

De vRealize Suite-producten van de SDDC-infrastructuur helpen u de prestaties, beschikbaarheid en capaciteit van bronnen in een virtuele en hybride cloudomgeving op effectieve wijze te beheren. De kerninfrastructuur helpt bij het beheer van hybride en heterogene cloudomgevingen, intern of extern, op basis van vSphere of andere technologieën van derden.

Wanneer de SDDC-infrastructuur tot stand is gebracht, kunt u deze uitbreiden om Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) te bieden aan consumenten van IT-bronnen binnen of buiten de organisatie. IaaS en PaaS vervolledigen het SDDC-platform en bieden meer uitbreidingsmogelijkheden. Met IaaS en PaaS verhoogt u de flexibiliteit van IT- en ontwikkelaarsactiviteiten.

Figuur 2-4. Bouwfasen voor de SDDC-infrastructuur

Virtualisatie en beheer van vRealize Suite -infrastructuur

De verschillende VMware-producten die deel uitmaken van de vRealize Suite bieden de virtualisatie- en beheermogelijkheden die zijn vereist voor de vRealize Suite-basis. Als u een robuuste basis voor uw datacenter tot stand wilt brengen, installeert en configureert u vCenter Server, ESXi en ondersteunende onderdelen.

Hybride cloudimplementatie

Met vRealize Suite kunnen ondernemingen workloads van de particuliere cloud uitbreiden naar de openbare cloud, profiteren van de implementatie van eindpunten (op aanvraag, zelfondertekend en flexibel) en tegelijk voordeel halen uit dezelfde beheeromgeving, betrouwbaarheid en prestaties van de door vRealize Suite aangedreven particuliere cloud.

Met vRealize Automation en vRealize Orchestrator in de cloudbeheerlaag van een SDDC kunnen ondernemingen VM's en eindpunten inrichten die verder reiken dan vSphere-omgevingen, en dus ook omgevingen die niet zijn gebaseerd op vSphere. De niet-vSphere omgevingen die niet zijn gebaseerd op vSphere, kunnen zich bevinden in particuliere datacenters of bij serviceproviders van openbare clouds. De servicebeheerlaag van SDDC staat controle van vSphere-eindpunten en eindpunten die niet zijn gebaseerd op vSphere toe. vRealize Operations Manager en vRealize Log Insight zijn de voornaamste producten van de servicebeheerlaag die ondernemingen helpen om analytische informatie te bieden over de VM's.

Ontwerpoverwegingen voor ESXi en vCenter Server

Ontwerpbesluiten voor virtualisatie van het SDDC moeten beantwoorden aan de specifieke implementatie- en ondersteuningskenmerken van ESXi en vCenter Server.

Overweeg de volgende ontwerpbesluiten wanneer u de implementatie van ESXi-hosts plant.

ESXi

- Gebruik een tool zoals VMware Capacity Planner om de prestaties en het gebruik van bestaande servers te analyseren.
- Gebruik ondersteunde serverplatformen die in de lijst staan in de Compatibiliteitshandleiding voor VMware.
- Verifieer of uw hardware voldoet aan de minimale systeemvereisten om ESXi uit te voeren.
- Als u variabiliteit wilt elimineren en een beheerbare en ondersteunde infrastructuur tot stand wilt brengen, standaardiseert u de fysieke configuratie van de ESXi-hosts.
- U kunt ESXi-hosts handmatig implementeren, of hiervoor een geautomatiseerde installatiemethode zoals vSphere Auto Deploy gebruiken. Een geldige benadering is het handmatig implementeren van het beheercluster en vervolgens vSphere Auto Deploy te gebruiken naarmate uw omgeving groeit.

vCenter Server

- U kunt vCenter Server implementeren als een op Linux gebaseerde virtuele applicatie of op een 64-bits fysieke of virtual machine met Windows.

  Opmerking vCenter Server op Windows kan worden opgeschaald om tot 10.000 ingeschakelde virtual machines te ondersteunen. De vCenter Server-applicatie is een alternatieve keuze die vooraf is geconfigureerd, en implementatie versnelt en licentiekosten voor het besturingssysteem reduceert. Wanneer u een externe Oracle-database gebruikt, kan de vCenter Server-applicatie tot 10.000 virtual machines ondersteunen.

- Zorg voor voldoende virtuele systeembronnen voor vCenter Server.

- Implementeer de vSphere Web Client en de vSphere Client voor gebruikersinterfaces in de omgeving. Implementeer de vSphere Command Line Interface (vCLI) of vSphere PowerCLI voor opdrachtregel- en scriptverwerkingsbeheer. vCLI en vSphere SDK for Perl zijn opgenomen in de vSphere Management Assistant.

Overwegingen voor het netwerkontwerp

Naarmate virtualisatie en cloud computing populairder worden in het datacenter, vindt er een verschuiving plaats in het traditionele drielaagse netwerkmodel. Het traditionele model core-aggregate-access wordt vervangen door het leaf-spine-ontwerp.

Het netwerk moet zodanig zijn ontworpen dat dit voldoet aan de uiteenlopende behoeften van verschillende entiteiten binnen een organisatie. Deze entiteiten omvatten toepassingen, services, opslag, beheerders en gebruikers.

- Gebruik waar nodig gecontroleerde toegang en isolatie om een passend beveiligingsniveau te bieden.
- Gebruik een leaf-spine-ontwerp om de netwerkarchitectuur te vereenvoudigen.
- Configureer algemene poortgroepnamen voor hosts ter ondersteuning van de migratie en failover van virtual machines.
- Scheid de netwerken voor de belangrijkste services van elkaar om een betere beveiliging en betere prestaties te realiseren.

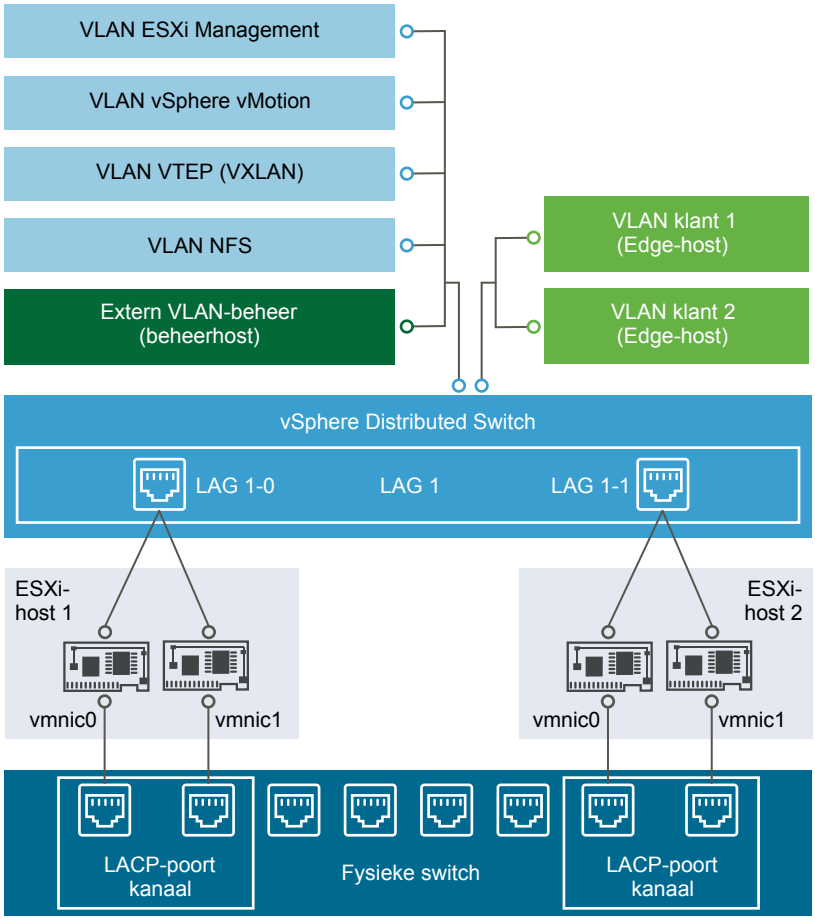
Netwerkisolatie wordt vaak beschouwd als 'best practice' in het datacenter. In een vRealize Suite-omgeving kunnen er meerdere belangrijke VLAN's zijn die twee of meer fysieke clusters omvatten.

In de volgende illustratie maken alle hosts deel uit van het ESXi-beheer, vSphere vMotion, VXLAN en NFS VLAN's. De beheerhost is ook verbonden met het externe VLAN, en elke Edge-host maakt verbinding met het klantspecifieke VLAN.

In dit geval gebruiken verbindingen het Link Aggregation Control Protocol (LACP) dat wordt aangeboden door een vSphere Distributed Switch voor het samenvoegen van de bandbreedte van fysieke NIC's op ESXi-hosts die zijn aangesloten op LACP port-kanalen. U kunt meerdere Link Aggregation Groups (LAG's) maken op een gedistribueerde switch. Een LAG omvat twee of meer poorten en sluit fysieke NIC's aan op de poorten. LAG-poorten worden in de LAG samengevoegd voor redundantie en het netwerkverkeer wordt gelijkmatig verdeeld over de poorten door middel van een LACP-algoritme.

Zie LACP-ondersteuning op een vSphere Distributed Switch.

Figuur 2-5. Verschillende typen ESXi-hosts maken verbinding met verschillende VLAN's



Ontwerpoverwegingen voor gedeelde opslag

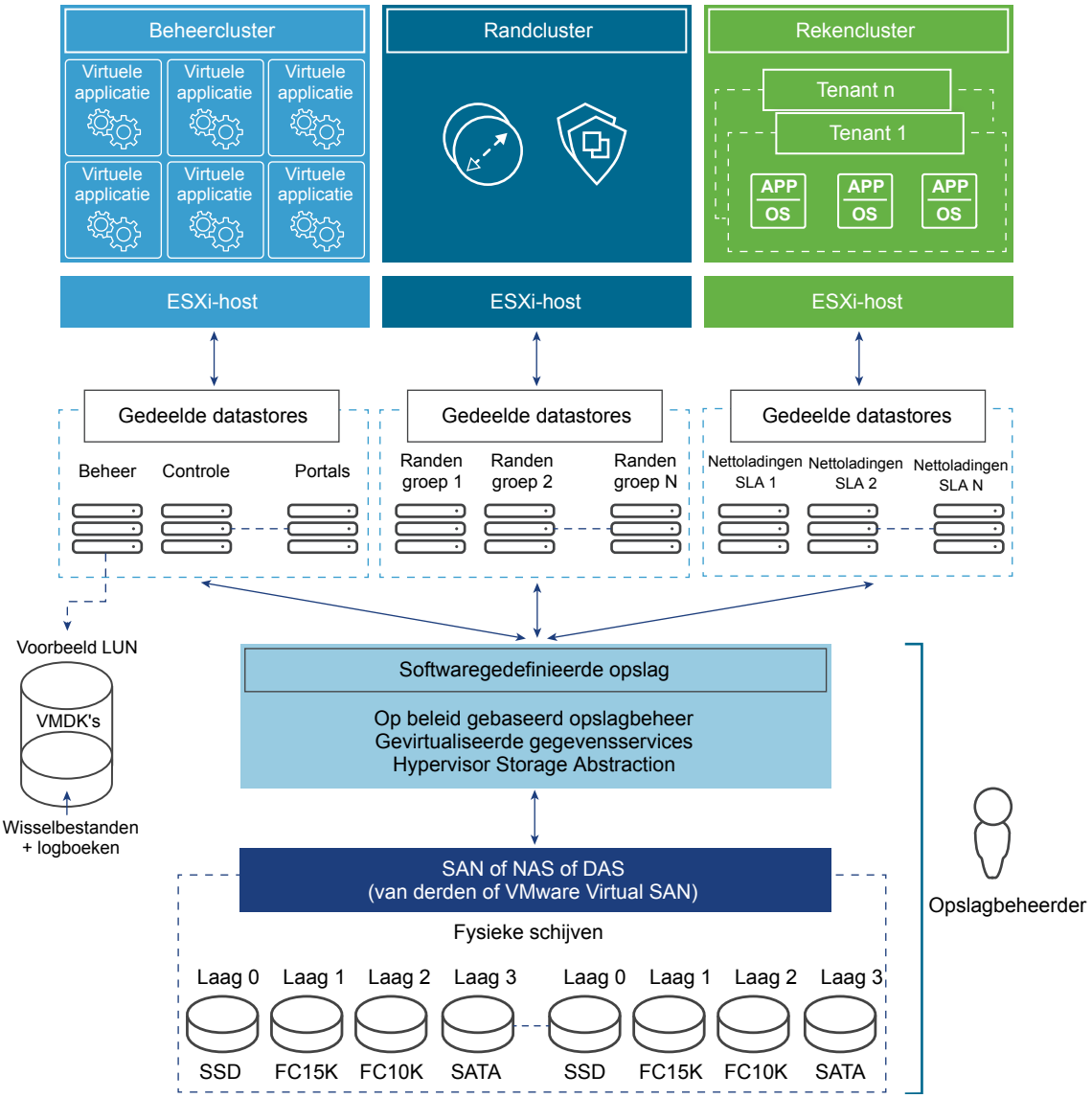
Een goed opslagontwerp is de basis voor een goed presterend virtueel datacenter.

- Het opslagontwerp moet zijn geoptimaliseerd om te voldoen aan de uiteenlopende behoeften van toepassingen, services, beheerders en gebruikers.
- Opslaglagen hebben verschillende prestatie-, capaciteits- en beschikbaarheidskenmerken.
- Het ontwerpen van verschillende opslaglagen is kostenbesparend omdat niet elke toepassing dure, hoogwaardige, goed beschikbare opslag vereist.
- Fibre Channel, NFS en iSCSI zijn volwassen en rendabele opties voor de ondersteuning van de behoeften van virtual machines.

De volgende afbeelding laat zien hoe verschillende typen hosts gebruikmaken van verschillende opslagarrays. Hosts in het beheercluster hebben opslag nodig voor beheer, controle en portals. Hosts in het randcluster hebben opslag nodig die voor de klant toegankelijk is. Een host in het nettolading-cluster heeft toegang tot klantspecifieke opslag. Verschillende nettolading-clusterhosts hebben toegang tot verschillende opslag.

De opslagbeheerder kan alle opslag beheren, maar de opslagbeheerder heeft geen toegang tot de gegevens van klanten.

Figuur 2-6. Opslag ter ondersteuning van de verschillende hosts



vRealize Suite -kerninfrastructuur beheren

Het beheer van een SDDC omvat veel, vaak repetitieve, bewerkingen. In vRealize Suite kunt u vRealize Orchestrator gebruiken om complexe processen te beheren door middel van werkstromen.

Met de cloudbeheerlaag kunt u macro-achtige werkstromen creëren voor het automatiseren van handmatige processen. Orkestratie maakt het inrichten van herhaalbare bewerkingen mogelijk.

Binnen de cloudbeheerlaag kunnen werkstromen automatisch of handmatig worden geactiveerd.

- vRealize Automation kan vRealize Orchestrator-werkstromen activeren.
- U kunt ook werkstromen publiceren in uw servicecatalogus en deze handmatig activeren.

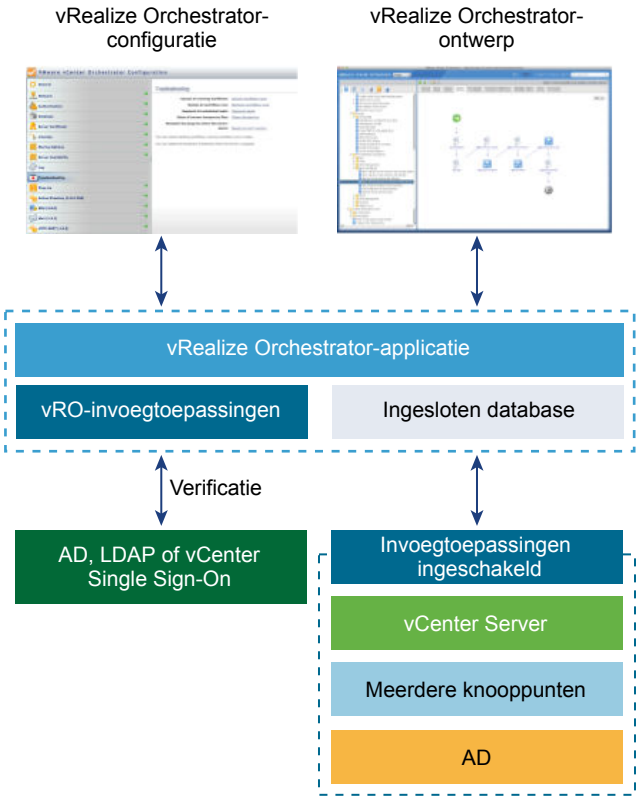
Door de orkestratie-engine vroegtijdig in het proces in te richten profiteren klanten van alle niveaus hiervan en wordt de basis gelegd voor de rest van de oplossing. Implementeer minimaal één vCenter Server-exemplaar voor elk vCenter Server-systeem in uw omgeving, afhankelijk van uw schaalvereisten.

De orkestratielaag bevat de volgende belangrijke elementen.

- vRealize Orchestrator

- vRealize Orchestrator-invoegtoepassingen

Figuur 2-7. Ontwerp van de vRealize Suite -orkestratielaag



Tabel 2-1. Onderdelen van de vRealize Suite -orkestratielaag

Onderdeel	Beschrijving
vRealize Orchestrator-toepassing	U kunt vRealize Orchestrator implementeren als een virtuele toepassing. De vRealize Orchestrator-toepassing, uitgevoerd in standalone modus, niet in HA, is de aanbevolen benadering voor kleinere toepassingen.
Verificatie	Aangeboden door Active Directory of vCenter Single Sign-On.
vRealize Orchestrator-configuratie-interface	Gebruik de configuratie-interface op het web voor de configuratie van de toepassingsdatabase, TLS-certificaat, licentie, enzovoort.
vRealize Orchestrator-ontwerpinterface	Gebruik de ontwerpinterface op het web voor het maken en aanpassen van werkstromen.
vCenter Server-invoegtoepassing	Gebruik de vRealize Orchestrator-invoegtoepassing voor het beheren van meerdere vCenter Server-instanties. De invoegtoepassing beschikt over een bibliotheek met standaardwerkstromen voor het automatiseren van vCenter Server-bewerkingen.
Invoegtoepassing met meerdere knooppunten	Gebruik de vRealize Orchestrator-invoegtoepassing met meerdere knooppunten voor het op afstand beheren van vRealize Orchestrator en uitvoeren van werkstromen.

vRealize Suite -kerninfrastructuur controleren

De controlemogelijkheid is een vereist element voor een SDDC. Het controle-element biedt mogelijkheden voor prestatie- en capaciteitsbeheer van gerelateerde infrastructuuronderdelen, zoals vereisten, specificaties, beheer en relaties.

vRealize Suite-controleproducten omvatten diverse VMware-producten.

Tabel 2-2. Controleproducten in vRealize Suite

Controleproduct	Beschrijving
vRealize Operations Manager	Biedt informatie over de prestaties, capaciteit en status van uw infrastructuur. Gedistribueerd als virtuele applicatie die u kunt implementeren op ESXi-hosts. Configureer de virtuele applicatie en registreer deze met een vCenter Server-systeem. Raadpleeg de Informatiecentrum voor vRealize Operations Manager.
vRealize Suite Lifecycle Manager	Biedt statuscontrole voor vRealize Suite-producten in een VMware vRealize Suite Lifecycle Manager-omgeving. Statuscontrole is alleen beschikbaar voor omgevingen met vRealize Operations Manager. Zie Statuscontrole configureren voor de vRealize Suite Management Stack.
vRealize Infrastructure Navigator	Detecteert toepassingsservices, visualiseert relaties en wijst afhankelijkheden toe van toepassingen op gevirtualiseerde reken-, opslag- en netwerkbronnen. Raadpleeg de Documentatiecentrum voor vRealize Infrastructure Navigator.
vRealize Log Insight	Verzamelt en analyseert logboekgegevens om in real time antwoorden te geven op problemen gerelateerd aan systemen, services en toepassingen en om belangrijke inzichten te leveren. Raadpleeg de Documentatiecenter voor VMware vRealize Log Insight.

U kunt alle controleproducten implementeren, of slechts bepaalde producten zonder de integriteit van de oplossing te beschadigen.

Een infrastructuurservice leveren

De mogelijkheid om Infrastructure as a Service (IaaS) te leveren staat voor de technologische en organisatorische transformatie van traditionele datacenters naar de cloud. U kunt virtual machines en services modelleren en inrichten in een particuliere, openbare of hybride cloudinfrastructuur.

In het SDDC kunnen providergroepen of -organisaties bronnen isoleren en afscheiden in de vorm van infrastructuur- en toepassingsservices en ze beschikbaar maken voor tenantgroepen of -organisaties.

De cloudbeheerlaag levert een selfservicegebruikersportal dat de administratieve overhead verlaagt door het gebruik van beleidsregels om infrastructuurservices in te richten Beheerders gebruiken beleidsregels om het verbruik van services op gedetailleerde en flexibele wijze te regelen. Aan elke service kunnen goedkeuringsvereisten worden toegevoegd.

U kunt de infrastructuurservice bouwen met diverse onderdelen.

Tabel 2-3. Onderdelen van een infrastructuurservice

Sectie van een infrastructuurservice	Ontwerponderdelen
vRealize Automation virtuele applicatie	■ vRealize Automation-portalwebserver of -appserver ■ vRealize Automation vPostgreSQL-database
vRealize Automation IaaS	■ vRealize Automation IaaS-webserver ■ vRealize Automation IaaS Manager-services

Tabel 2-3. Onderdelen van een infrastructuurservice (Vervolgd)

Sectie van een infrastructuurservice	Ontwerponderdelen
Distributed Execution Manager	vRealize Automation Distributed Execution Managers bestaan uit DEMOrchestrator-instanties en DEM-werkerinstanties.
Integratie	vRealize Automation-agentmachines
Kostenbewaking	vRealize Business Cloud
Inrichtingsinfrastructuur	■ vSphere-omgeving ■ vRealize Orchestrator-omgeving ■ Andere ondersteunde fysieke, virtuele of cloudomgeving
Ondersteunende infrastructuur	■ Microsoft SQL-databaseomgeving ■ LDAP- of Active Directory-omgeving ■ SMTP- en e-mailomgeving

Een infrastructuurservice wordt in meerdere fasen geïmplementeerd.

Figuur 2-8. Fasen van een IaaS-implementatie

Raadpleeg de vRealize Automation-informatie over Infrastructure as a Service (IaaS) voor een gedetailleerde beschrijving van de voornaamste IaaS-concepten.

Selfserviceportal vRealize Automation biedt een veilig portal waar bevoegde beheerders, ontwikkelaars en zakelijke gebruikers nieuwe IT-services kunnen aanvragen.

Infrastructuuronderdelen Als u vRealize Automation wilt implementeren, configureert u bepaalde VMware-producten zoals vSphere en vCloud Air en configureert u vRealize Automation-onderdelen zoals fysieke eindpunten, materiaalgroepen en blueprints.

Services en tenants De servicecatalogus biedt een geïntegreerd selfserviceportal voor het gebruik van IT-services. Gebruikers kunnen door de catalogus bladeren om items aan te vragen, hun aanvragen volgen en de voor hen ingerichte items beheren.

Kostenbewaking Oplossingen die integreren met vRealize Automation, zoals vRealize Business Cloud, ondersteunen kostenverkenning en -bewaking.

Platform as a Service leveren

Gebruik Platform as a Service (PaaS) om toepassingen te modelleren en in te richten in particuliere, openbare en hybride cloudinfrastructuren.

PaaS is een type computingservice in de cloud die een computingplatform en een set oplossingen als een service biedt. Samen met Software as a Service (SaaS) en Infrastructure as a service (IaaS) is PaaS een servicemodel voor computing in de cloud waarmee u kunt gebruikmaken van hulpprogramma's en bibliotheken die door de provider wordt geleverd om een toepassing of service te maken. U hebt controle over instellingen voor de implementatie en de configuratie van de software. De provider levert de netwerken, servers, opslag en overige services die nodig zijn om uw toepassing te hosten.

Inrichting van toepassingen automatiseren

Een belangrijk eigenschap van PaaS is de mogelijkheid om de inrichting van toepassingen te automatiseren. vRealize Automation is een op modellen gebaseerde oplossing voor het inrichten van toepassingen die het maken en standaardiseren van topologieën voor de implementatie van toepassingen in cloudinfrastructuren vereenvoudigt. Toepassingsarchitecten kunnen met functies voor slepen en neerzetten topologieën voor de implementatie van toepassingen, toepassingsblueprints genoemd, maken. Toepassingsblueprints definiëren de structuur van de toepassing, maken het gebruik van gestandaardiseerde infrastructuuronderdelen van toepassingen mogelijk en bevatten installatieafhankelijkheden en standaardconfiguraties voor aangepaste en standaardbedrijfstoepassingen. U kunt de vooraf ingevulde en uitbreidbare catalogus met standaard logische sjablonen, toepassingsinfrastructuurservice, onderdelen en scripts gebruiken om een toepassingsblueprint te modelleren. Toepassingsblueprints zijn logische implementatietopologieën die verplaatsbaar zijn tussen IaaS-clouds, zoals vRealize Automation, en tussen openbare clouds, zoals Amazon EC2.

Met vRealize Automation bepaalt u de toepassings- en servicestructuur, waarbij de onderliggende cloudinfrastructuur de nodige computing-, netwerk- en opslagvereisten levert. U kunt de vRealize Automation-blueprints implementeren in elke particuliere of openbare cloud die is gebaseerd op VMware vSphere. Dankzij dit inrichtingsmodel voor toepassingen hoeven ontwikkelaars en toepassingsbeheerders niet langer infrastructuur-, OS- en middlewareconfiguratietaken uit te voeren en kan uw bedrijf de aandacht richten op het aanbieden van bedrijfswaarde met uw toepassingen.

Zakelijke gebruikers kunnen complexe toepassingen in dynamische cloudomgevingen standaardiseren, implementeren, configureren, bijwerken en schalen. Dit kunnen eenvoudige webtoepassingen zijn tot zelfs complexe aangepaste toepassingen en gebundelde toepassingen. Met de catalogus van standaardonderdelen, of services, automatiseert en beheert vRealize Automation Application Services de updatelevenscyclus van implementaties voor meerlagige bedrijfstoepassingen in hybride cloudomgevingen.

Prestaties van toepassingen controleren

Controle biedt mogelijkheden voor prestatiebeheer gerelateerd aan toepassingen.

Vooraf gebrouwde toepassingsonderdelen

VMware Cloud Management Marketplace biedt blueprints, services, scripts en invoegtoepassingen die u kunt downloaden en gebruiken om uw eigen toepassingsservices te ontwikkelen. Toonaangevende leveranciers van middleware, netwerken, beveiliging en toepassingen leveren vooraf gemaakte onderdelen die gebruikmaken van herbruikbare en flexibele configuraties die u kunt invoegen in elk plan voor het inrichten van meerlagige toepassingen.

Beveiligingsoverwegingen voor vRealize Suite

Elk vRealize Suite-product moet voldoen aan de beveiligingseisen. U moet rekening houden met verificatie en autorisatie voor elk product, verzekeren dat certificaten voldoen aan de bedrijfsvereisten, en netwerkisolatie implementeren.

Documentatie voor productfamilies of individuele producten kan u helpen uw omgeving te beveiligen. Dit document is met name gericht op aanvullende stappen die u kunt nemen om de productsuite te beveiligen.

Tabel 2-4. Beveiligingsdocumentatie voor vRealize Suite -producten

Product	Documentatie
vCenter ServerESXi	Zie de vSphere-beveiliging-documentatie voor informatie over veel onderwerpen waaronder certificaatbeheer, beveiliging van ESXi en vCenter Server, en verificatie en autorisatie. Zie het technische document Beveiliging van de VMware Hypervisor voor beveiligingsinformatie voor ESXi.
vSphere	Zie de vSphere Hardening-handleidingen voor beveiliging voor uw vSphere-producten.
vRealize Automation en gerelateerde producten.	Raadpleeg Voorbereiden op installatie in het informatiecentrum van vRealize Automation voor informatie over certificaten, wachtwoordzinnen, gebruikersbeveiliging, het gebruik van beveiligingsgroepen, enzovoort. Raadpleeg de vRealize Automation Handleiding Beveiligde configuratie voor informatie over het optimaliseren van de beveiligde configuratie van uw vRealize Automation-omgeving.
vRealize Suite Lifecycle Manager	Raadpleeg de Handleiding voor hardening van vRealize Suite Lifecycle Manager-beveiliging voor informatie over het optimaliseren van de beveiligde configuratie van uw vRealize Suite Lifecycle Manager-omgeving.

Verificatie en autorisatie in vCloud Suite

Verificatie met vCenter Single Sign-On zorgt dat alleen gebruikers van ondersteunde identiteitsbronnen zich kunnen aanmelden bij vCloud Suite. Autorisatie zorgt dat alleen een gebruiker met de overeenkomende privileges informatie kan weergeven of taken kan uitvoeren. Autorisatie is van toepassing op zowel services als gebruikers.

Verificatie met vCenter Single Sign-On

vCenter Single Sign-On ondersteunt verificatie in uw beheerinfrastructuur. Alleen gebruikers die zich kunnen verifiëren bij vCenter Single Sign-On kunnen infrastructuuronderdelen weergeven en beheren. U kunt identiteitsbronnen zoals Active Directory of OpenLDAP toevoegen aan vCenter Single Sign-On.

Overzicht van vCenter Single Sign-On

vCenter Single Sign-On is een verificatiebroker en uitwisselingsinfrastructuur voor beveiligingstokens voor gebruikers en gebruikers van oplossingen, die sets van VMware-services zijn. Wanneer een gebruiker of een gebruiker van een oplossing zich verifieert met vCenter Single Sign-On, ontvangt die gebruiker een SAML-token. Daarna kan de gebruiker het SAML-token gebruiken om zich te verifiëren bij vCenter Server-services. De gebruiker kan vervolgens de informatie weergeven en de acties uitvoeren waarvoor die gebruiker privileges heeft.

MetvCenter Single Sign-On kunnen de vCloud Suite-producten met elkaar communiceren via een uitwisselingsmechanisme voor beveiligingstokens, zodat elk product gebruikers niet individueel hoeft te verifiëren met een directoryservice zoals Microsoft Active Directory. Tijdens de installatie of upgrade maakt vCenter Single Sign-On een intern beveiligingsdomein, bijvoorbeeld vsphere.local, waar de vSphere-oplossingen en producten zijn geregistreerd. In plaats van dit interne beveiligingsdomein te gebruiken voor bedrijfsspecifieke verificatie-informatie, kunt u een of meer identiteitsbronnen zoals een Active Directory-domein toevoegen aan vCenter Single Sign-On.

vCenter Single Sign-On configureren

U kunt vCenter Single Sign-On configureren in de vSphere Web Client.

Vanaf vSphere 6.0 is vCenter Single Sign-On een onderdeel van Platform Services Controller. De Platform Services Controller bevat gedeelde services die vCenter Server en vCenter Server-onderdelen ondersteunen. Als u vCenter Single Sign-On wilt beheren, maakt u verbinding met de Platform Services Controller die bij uw omgeving hoort. Zie vSphere Authentication met vCenter Single Sign-On voor achtergrondinformatie en meer details over de configuratie.

Autorisatie in vCloud Suite

Autorisatie bepaalt welke gebruiker of welk proces toegang heeft of wijzigingen kan aanbrengen in welke onderdelen van uw vCloud Suite-implementatie. Verschillende producten in vCloud Suite hebben verschillende autorisatieniveaus.

Verschillende typen beheerders zijn verantwoordelijk om verschillende typen gebruikers toegang te verlenen voor verschillende producten of productonderdelen.

Autorisatie voor vCenter Server

Het vCenter Server-rechtenmodel staat beheerders toe om rollen toe te wijzen aan een gebruiker of groep voor een bepaald object in de vCenter Server-objecthiërarchie. Rollen bestaan uit een set privileges. vCenter Server heeft vooraf gedefinieerde rollen, maar u kunt ook aangepaste rollen maken.

In bepaalde gevallen moeten rechten worden gedefinieerd voor zowel een bronobject als een doelopbject. Als u bijvoorbeeld een virtual machine verplaatst, hebt u niet alleen rechten voor die virtual machine nodig, maar ook voor het bestemde datacenter.

Met algemene rechten kunt u bepaalde gebruikers privileges verlenen voor alle objecten in de vCenter-objecthiërarchie. Gebruik algemene rechten zeer zorgvuldig, in het bijzonder als u ze doorvoert in de objecthiërarchie.

Zie de vSphere-beveiligingsdocumentatie voor details en instructievideo's over vCenter Server-rechten.

Verificatie van vRealize Automation

Met vRealize Automation kunt u vooraf gedefinieerde rollen gebruiken om te bepalen welke gebruiker of groep welke taken kan uitvoeren. Anders dan bij vCenter Server kunt u geen aangepaste rollen definiëren, maar is er een set vooraf gedefinieerde rollen beschikbaar.

Verificatie en autorisatie verlopen als volgt:

1. De systeembeheerder voert de initiële configuratie van Single Sign-On en de basisinstallatie van tenants uit, inclusief het toewijzen van minimaal één identiteitsarchief en een tenantbeheerder voor elke tenant.
2. Daarna kan een tenantbeheerder extra identiteitsarchieven configureren en rollen aan gebruikers en groepen uit de identiteitsarchieven toewijzen.

   Tenantbeheerders kunnen ook aangepaste groepen binnen hun eigen tenant maken en gebruikers en groepen die in het identiteitsarchief zijn gedefinieerd, toevoegen aan aangepaste groepen. Aan aangepaste groepen, zoals identiteitsarchiefgroepen en -gebruikers, kunnen rollen worden toegewezen.
3. Beheerders kunnen vervolgens rollen toewijzen aan gebruikers en groepen, afhankelijk van hun eigen rol.
   - Er is een set systeembrede rollen, zoals systeembeheerder, IaaS-beheerder en materiaalbeheerder, vooraf gedefinieerd.
   - Er is ook een afzonderlijke reeks tenantrollen, zoals een tenantbeheeder of een catalogusbeheerder van toepassing, vooraf gedefinieerd.

Zie de documentatie bij vRealize Automation.

Federatief identiteitsbeheer

Federatief identiteitsbeheer maakt het mogelijk om elektronische identiteiten en kenmerken van één domein te accepteren en te gebruiken voor toegang tot bronnen in andere domeinen. U kunt federatief identiteitsbeheer inschakelen tussen vRealize Automation, vRealize Operations Manager en vSphere Web Client met behulp van vCenter Single Sign-On en VMware Identity Manager.

Federatieve identiteitsomgevingen delen gebruikers in in categorieën, die persona's worden genoemd, op basis van hoe ze werken met federatieve identiteitssystemen. Gebruikers gebruiken de systemen om services te ontvangen. Beheerders configureren en beheren federatie tussen de systemen. Ontwikkelaars maken services die door gebruikers worden gebruikt en kunnen die uitbreiden. In de volgende tabel beschrijven we de voordelen van federatief identiteitsbeheer waarvan deze persona gebruikmaakt.

Tabel 2-5. Voordelen voor persona

Gebruikerstypen	Voordeel van federatieve identiteit
Gebruikers	■ Handige Single Sign-On voor meerdere toepassingen ■ Minder wachtwoorden te beheren ■ Verbeterde beveiliging
Beheerders	■ Meer controle over toepassingsrechten en toegang ■ Context en authenticatie op basis van beleid
Ontwikkelaars	■ Eenvoudige integratie ■ Voordelen van meerdere tenants, gebruikers- en groepsbeheer, uitbreidbare verificatie en gedelegeerde autorisatie met een minimum aan inspanning

U kunt federatie tussen VMware Identity Manager en vCenter Single Sign-On instellen door een SAML-verbinding te maken tussen de twee partijen. vCenter Single Sign-On fungeert als de identiteitsprovider en VMware Identity Manager als de serviceprovider. Een identiteitsprovider levert een elektronische identiteit. Een serviceprovider verleent toegang tot bronnen na beoordeling en acceptatie van de elektronische identiteit.

Voor de verificatie van gebruikers door vCenter Single Sign-On moet hetzelfde account bestaan in VMware Identity Manager en vCenter Single Sign-On. De userPrinicpalName van de gebruiker moet aan beide uiteinden overeenkomen. Overige kenmerken kunnen verschillen omdat ze niet worden gebruikt om het SAML Subject te identificeren.

Voor lokale gebruikers in vCenter Single Sign-On, zoals admin@vsphere.local, moeten ook overeenkomende accounts worden gemaakt in VMware Identity Manager waarbij minimaal de userPrincipalName van de gebruiker overeenkomt. De overeenkomende accounts moeten handmatig worden gemaakt of met behulp van een script met de API's van VMware Identity Manager voor het maken van lokale gebruikers.

De volgende taken moeten worden voltooid om SAML tussen SSO2 en vIDM in te stellen.

1. Importeer het SAML-token van vCenter Single Sign-On in VMware Identity Manager voordat u de VMware Identity Manager-standaardverificatie bijwerkt.
2. Configureer in VMware Identity Manager vCenter Single Sign-On als een identiteitsprovider voor VMware Identity Manager en werk de VMware Identity Manager-standaardverificatie bij.
3. Configureer voor vCenter Single Sign-On VMware Identity Manager als serviceprovider door het VMware Identity Manager `sp.xml`-bestand te importeren.

Raadpleeg de volgende productdocumentatie:

- Zie VMware vCenter SSO 5.5 U2 gebruiken met VMware vCloud Automation Center 6.1 voor informatie over het configureren van SSO2 als identiteitsprovider voor vRealize Automation.
- Zie Uw wachtwoord voor Single Sign-On bijwerken voor VMware Identity Manager voor documentatie over vRealize Automation VMware Identity Manager.

- Zie SAML-federatie configureren tussen Beheer van folders en SSO2voor informatie over hoe u federatie tussen Beheer van directory's en SSO2 configureert.
- Zie Een Single Sign-On-bron configureren in vRealize Operations Manager voor documentatie over vRealize Operations Manager SSO.

TLS en gegevensbescherming

De verschillende vRealize Suite-producten gebruiken TLS om sessie-informatie tussen producten te versleutelen. De VMware Certificate Authority (VMCA), die deel uitmaakt van de Platform Services Controller, levert certificaten standaard aan bepaalde producten en services. Overige onderdelen worden ingericht met zelfondertekende certificaten.

Als u de standaardcertificaten wilt vervangen door uw eigen bedrijfscertificaten of CA-ondertekende certificaten, verschilt het proces voor de verschillende onderdelen.

Certificaatcontrole is standaard ingeschakeld en TLS-certificaten worden gebruikt om netwerkverkeer te versleutelen. Vanaf vSphere 6.0 wijst de VMCA certificaten toe aan ESXi-hosts en vCenter Server-systemen als onderdeel van het installatieproces. U kunt deze certificaten vervangen om VMCA te gebruiken als tussenliggende CA of u kunt aangepaste certificaten in uw omgeving gebruiken. vSphere versie 5.5 en lager gebruikt zelfondertekende certificaten en u kunt deze indien nodig gebruiken of vervangen.

U kunt certificaten van vSphere 6.0 vervangen door gebruik te maken van het hulpprogramma vSphere Certificate Manager of certificaatbeheer-CLI's. U kunt certificaten van vSphere 5.5 en lager vervangen met het Certificate Automation Tool.

Producten die VMCA gebruiken

Diverse VMware-producten ontvangen tijdens de installatie certificaten van de VMCA. Voor die producten hebt u meerdere opties.

- Behoud de certificaten voor interne implementaties of overweeg om extern gerichte certificaten te vervangen, maar intern gerichte VMCA-ondertekende certificaten te behouden.
- Maak van VMCA een tussenliggend certificaat. Gebruik in de toekomst de volledige keten om te ondertekenen.
- Vervang de VMCA-ondertekende certificaten door aangepaste certificaten.

Zie vSphere-beveiligingscertificaten.

Producten die zelfondertekende certificaten gebruiken

U kunt gebruikmaken van producten die zelfondertekende certificaten gebruiken. Browsers vragen gebruikers om een zelfondertekend certificaat bij het eerste gebruik te accepteren of te weigeren. Gebruikers kunnen op een link klikken om de certificaatgegevens te openen en te bekijken voordat ze het certificaat accepteren of weigeren. Browsers slaan geaccepteerde certificaten lokaal op en accepteren ze zonder bericht bij daaropvolgend gebruik. U kunt de acceptatiestap desgewenst vermijden door zelfondertekende certificaten te vervangen door bedrijfscertificaten of CA-ondertekende certificaten. In de productdocumentatie wordt beschreven hoe u zelfondertekende certificaten kunt vervangen.

Tabel 2-6. Zelfondertekende certificaten vervangen

Product	Documentatie
vSphere Replication	Zie Het SSL-certificaat van de vSphere Replication Appliance wijzigen.
vRealize Automation	Zie vRealize Automation-certificaten bijwerken.
vRealize Log Insight	Zie Aangepast SSL-certificaat installeren.
vRealize Orchestrator	Zie SSL-certificaten wijzigen.

Tabel 2-6. Zelfondertekende certificaten vervangen (Vervolgd)

Product	Documentatie
vRealize Operations Manager	Zie Een aangepast certificaat toevoegen aan vRealize Operations Manager.
vRealize Business for Cloud Standard	Zie Het SSL-certificaat wijzigen of vervangen van vRealize Business for Cloud.

De fysieke laag beveiligen

Het beveiligen van de fysieke laag omvat het beveiligen of 'hardening' van de hypervisor, het instellen van het fysieke netwerk voor maximumbeveiliging en het beveiligen van uw opslagoplossing.

Standaard-switchpoorten beveiligen

Net als fysieke netwerkadapters kan een virtuele netwerkadapter frames verzenden die van een andere machine afkomstig lijken of een andere machine imiteren. En net als fysieke netwerkadapters kan een virtuele netwerkadapter ook zodanig worden geconfigureerd dat deze frames ontvangt die bedoeld zijn voor andere machines.

Als een standaardswitch wordt gemaakt, worden poortgroepen toegevoegd om een beleidsconfiguratie te maken voor de virtual machines en opslagsystemen die aan de switch zijn gekoppeld. Virtuele poorten worden gemaakt via de vSphere Web Client of de vSphere Client.

Als onderdeel van het toevoegen van een poort of standaardpoortgroep aan een standaardswitch, configureert de vSphere Client een beveiligingsprofiel voor de poort. De host kan vervolgens voorkomen dat een van de virtual machines andere machines op het netwerk imiteert. Het gastbesturingssysteem dat verantwoordelijk is voor de imitatie, detecteert niet dat de imitatie is voorkomen.

Het beveiligingsprofiel bepaalt hoe strikt de host beveiligt tegen imitatie en aanvallen op virtual machines. Om de instellingen in het beveiligingsprofiel goed te gebruiken, moet u de basisprincipes begrijpen van hoe virtuele netwerkadapters overdrachten controleren en hoe aanvallen op dit niveau worden georganiseerd.

Elke virtuele netwerkadapter heeft een MAC-adres dat bij het creëren van de adapter is toegewezen. Dit adres wordt het initiële MAC-adres genoemd. Hoewel het initiële MAC-adres van buiten het gastbesturingssysteem opnieuw kan worden geconfigureerd, kan het niet worden gewijzigd door het gastbesturingssysteem. Daarnaast heeft elke adapter een effectief MAC-adres voor het uitfilteren van binnenkomend netwerkverkeer met een bestemmings-MAC-adres anders dan het effectieve MAC-adres. Het gastbesturingssysteem is verantwoordelijk voor het instellen van het effectieve MAC-adres en koppelt het effectieve MAC-adres gewoonlijk aan het initiële MAC-adres.

Bij het versturen van pakketten zet een besturingssysteem normaliter het effectieve MAC-adres van de eigen netwerkadapter in het bron-MAC-adresveld van het Ethernet-frame. Tevens wordt het MAC-adres voor de ontvangende netwerkadapter in het bestemmings-MAC-adresveld gezet. De ontvangende adapter accepteert pakketten alleen wanneer het bestemmings-MAC-adres in het pakket overeenkomt met het eigen effectieve MAC-adres.

Bij het aanmaken zijn het effectieve MAC-adres en initiële MAC-adres van een netwerkadapter hetzelfde. Het besturingssysteem van de virtual machine kan het effectieve MAC-adres op elk gewenst moment aanpassen. Als een besturingssysteem het effectieve MAC-adres wijzigt, dan ontvangt de netwerkadapter netwerkverkeer dat is bestemd voor het nieuwe MAC-adres. Het besturingssysteem kan te allen tijde frames versturen met een geïmiteerd bron-MAC-adres. Dit houdt in dat een besturingssysteem aanvallen kan plannen op de apparaten in een netwerk door het imiteren van een netwerkadapter die autorisatie heeft van het ontvangende netwerk.

Op hosts kunnen standaardbeveiligingsprofielen voor switches worden gebruikt om tegen dit type aanvallen te beschermen door het instellen van drie opties. Als standaardinstellingen voor een poort worden gewijzigd, moet het beveiligingsprofiel worden aangepast door de standaard-switchinstellingen te bewerken in de vSphere Client.

iSCSI-opslag beveiligen

De voor een host geconfigureerde opslag kan een of meer Storage Area Networks (SAN's) omvatten die iSCSI gebruiken. Als iSCSI op een host is geconfigureerd, kunnen beheerders verschillende maatregelen treffen om beveiligingsrisico's te minimaliseren.

iSCSI is een toegangsmethode voor SCSI-apparaten en dient voor het uitwisselen van gegevensrecords via TCP/IP via een netwerkpoort in plaats van via een directe verbinding met een SCSI-apparaat. Bij iSCSI-transacties worden blokken onbewerkte SCSI-gegevens ingesloten in iSCSI-records en verzonden aan het apparaat of de gebruiker die de aanvraag heeft gedaan.

Een manier om iSCSI-apparaten te beveiligen tegen ongewenste indringing, is te vereisen dat de host of initiator wordt geverifieerd door het iSCSI-apparaat of doel wanneer de host toegang probeert te krijgen tot gegevens op het doel-LUN. Verificatie bewijst dat de initiator toegangsrechten heeft voor een doel,

ESXi en iSCSI ondersteunen Challenge Handshake Authentication Protocol (CHAP), wat de legitimiteit verifieert van initiators die doelen op het netwerk benaderen. Gebruik de vSphere Client of vSphere Web Client om te bepalen of er verificatie plaatsvindt en om de verificatiemethode te configureren. Voor informatie over het configureren van CHAP voor iSCSI, zie de vSphere-documentatie CHAP-parameters configureren voor iSCSI-adapters.

ESXi-beheerinterfaces beveiligen

De beveiliging van de ESXi-beheerinterface is cruciaal voor de bescherming tegen ongeautoriseerde indringing en misbruik. Als een host op bepaalde manieren wordt geschaad, worden de virtual machines waarmee interactie plaatsvindt mogelijk ook geschaad. Om het risico van een aanval via de beheerinterface tot een minimum te beperken, wordt ESXi beschermd door een ingebouwde firewall.

Om de host te beschermen tegen ongeautoriseerde indringing en misbruik, legt VMware beperkingen op aan verschillende parameters, instellingen en activiteiten. Beperkingen kunnen worden versoepeld om te voldoen aan de configuratie-eisen, maar wanneer dit gebeurt moeten er maatregelen worden getroffen voor de bescherming van het netwerk als geheel en de apparaten die zijn verbonden met de host.

Houd rekening met de volgende aanbevelingen bij het evalueren van de beveiliging en het beheer van de host.

- Om de beveiliging te verbeteren moet gebruikerstoegang tot de beheerinterface worden beperkt en moet toegangsbeveiligingsbeleid worden ingesteld zoals het instellen van wachtwoordbeperkingen.
- Geef alleen vertrouwde gebruikers aanmeldingstoegang tot ESXi Shell. De ESXi Shell heeft toegangsbevoegdheid voor bepaalde delen van de host.
- Voer indien mogelijk alleen de essentiële processen, services en agents uit zoals virusscanners en back-up van virtual machines.
- Gebruik indien mogelijk het netwerkbeheerprogramma van vSphere Web Client of derden voor het beheren van ESXi-hosts in plaats van als rootgebruiker te werken via de opdrachtregelinterface. Als u de vSphere Web Client gebruikt, dan maakt u altijd verbinding met de ESXi-host via een vCenter Server-systeem.

De host voert verschillende pakketten van derden uit voor de ondersteuning van beheerinterfaces of taken die een operator moet uitvoeren. VMware ondersteunt het upgraden van deze pakketten alleen via een VMware-bron. Als een download of patch van een andere bron wordt gebruikt, dan kunnen de beveiliging of functies van de beheerinterface mogelijk worden geschaad. Controleer de sites van externe leveranciers en de VMware-kennisbank regelmatig op beveiligingswaarschuwingen.

Naast het implementeren van de firewall, kunt u risico's voor ESXi-hosts beperken door middel van andere methoden.

- Zorg ervoor dat alle firewallpoorten die niet specifiek nodig zijn voor beheertoegang tot de host zijn gesloten. Poorten moeten specifiek worden geopend als er andere services vereist zijn.
- Vervang de standaardcertificaten en gebruik geen zwakke versleutelingen. Standaard zijn zwakke versleutelingen uitgeschakeld en wordt alle communicatie van clients beveiligd door TLS. De exacte algoritmen die voor de beveiliging van het kanaal worden gebruikt, zijn afhankelijk van de TLS-handshake. Standaardcertificaten die zijn gemaakt op ESXi gebruiken SHA-1 met RSA-codering als handtekeningalgoritme.
- Installeer beveiligingspatches. VMware controleert alle beveiligingswaarschuwingen die invloed kunnen hebben op de beveiliging van ESXi, en brengt indien nodig een patch uit.
- Onbeveiligde services zoals FTP en Telnet worden niet geïnstalleerd en de poorten voor deze services zijn gesloten. Omdat veiligere services zoals SSH en SFTP eenvoudig beschikbaar zijn, moeten deze veiligere alternatieven altijd worden gebruikt in plaats van onveilige services. Als u onbeveiligde services moet gebruiken, implementeer dan voldoende bescherming voor de ESXi-hosts en open de betreffende poorten.

U kunt ESXi-hosts in lockdownmodus zetten. Als de lockdownmodus is ingeschakeld, kan de host alleen worden beheerd vanaf vCenter Server. Alleen vpxuser heeft verificatiemachtigingen, en directe verbindingen met de host worden geweigerd.

vCenter Server -systemen beveiligen

Het beveiligen van vCenter Server omvat het verzekeren van de veiligheid van de machine waarop vCenter Server wordt uitgevoerd, conform de 'best practices' voor het toewijzen van rechten en rollen, en het verifiëren van de integriteit van de clients die verbinding maken met vCenter Server.

Beheer de beheerdersbevoegdheden voor vCenter Server uiterst streng voor een optimale beveiliging van het systeem.

- Verwijder volledige beheerdersrechten voor vCenter Server van de account van de lokale Windows-beheerder, en wijs deze alleen toe aan een speciale lokale vCenter Server-beheerdersaccount. Geef alleen volledige beheerdersrechten voor vSphere aan de beheerders voor wie dit noodzakelijk is. Geef deze rechten niet aan een groep waarvan het lidmaatschap niet strikt wordt gecontroleerd.
- Sta gebruikers niet toe direct bij het vCenter Server-systeem aan te melden. Sta toegang alleen toe aan gebruikers die legitieme taken moeten uitvoeren en verzeker dat hun acties worden gecontroleerd.
- Installeer vCenter Server met behulp van een serviceaccount in plaats van een Windows-account. Voor het uitvoeren van vCenter Server kan een serviceaccount of Windows-account worden gebruikt. Door gebruik te maken van een serviceaccount is Windows-verificatie bij SQL Server mogelijk, wat een betere beveiliging biedt. De serviceaccount moet een beheerder zijn op de lokale machine.
- Controleer of bevoegdheden opnieuw worden toegewezen bij het opnieuw starten van vCenter Server. Als de gebruiker of gebruikersgroep die de beheerdersrol heeft voor de hoofdmap van de server niet kan worden geverifieerd als een geldige gebruiker of groep, dan worden de beheerdersbevoegdheden verwijderd en toegewezen aan de lokale groep Windows-beheerders.

Geef de vCenter Server-databasegebruiker minimale bevoegdheden. De databasegebruiker heeft slechts bevoegdheden nodig die specifiek zijn voor toegang tot de database. Daarnaast zijn sommige bevoegdheden vereist die alleen nodig zijn voor installatie en upgrades. Deze kunnen worden verwijderd nadat het product is geïnstalleerd of geüpgraded.

De virtuele lagen beveiligen

Naast het beveiligen van de fysieke lagen die de hardware, switches, enzovoort omvatten, moet u de virtuele lagen beveiligen. Beveilig de virtual machines, inclusief het besturingssysteem en de virtuele netwerklaag.

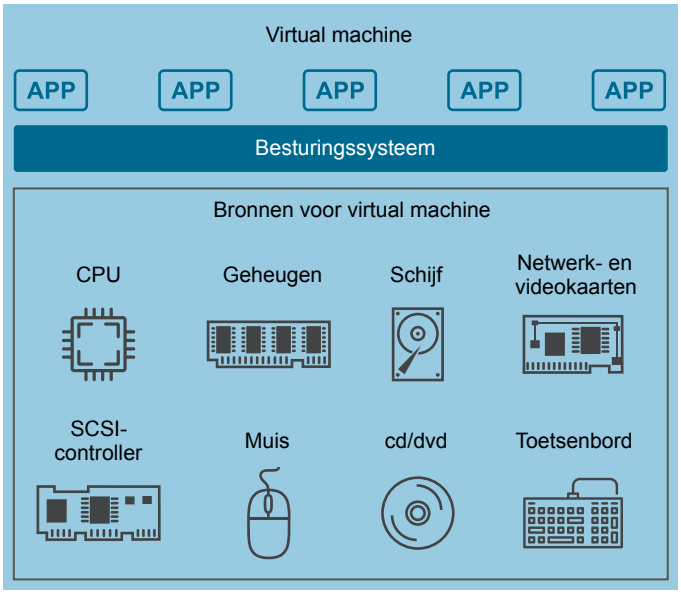
Beveiliging en virtual machines

Virtual machines zijn de logische containers waarbinnen toepassingen en gastbesturingssystemen worden uitgevoerd. Wat betreft het ontwerp zijn alle virtual machines van VMware van elkaar geïsoleerd. Deze isolatie maakt het mogelijk dat meerdere virtual machines veilig worden uitgevoerd terwijl er hardware wordt gedeeld, en staat zowel garant voor hun mogelijkheid om hardware te gebruiken als hun ononderbroken prestaties.

Zelfs een gebruiker met systeembeheerdersbevoegdheden voor het gastbesturingssysteem van een virtual machine kan deze isolatielaag niet doorbreken voor toegang tot een andere virtual machine zonder dat bevoegdheden expliciet door de ESXi-systeembeheerder zijn toegewezen. Door isolatie van virtual machines zullen, wanneer een gastbesturingssysteem dat wordt uitgevoerd op een virtual machine een storing ondervindt, andere virtual machines op dezelfde host actief blijven. Gebruikers hebben nog steeds toegang tot andere virtual machines, en de prestaties van andere virtual machines worden niet beïnvloed.

Elke virtual machine is geïsoleerd van andere virtual machines die op dezelfde hardware worden uitgevoerd. Hoewel virtual machines fysieke bronnen delen zoals CPU, geheugen en invoer-/uitvoerapparaten, kan een gastbesturingssysteem op een afzonderlijke virtual machine alleen de virtuele apparaten detecteren die u beschikbaar maakt.

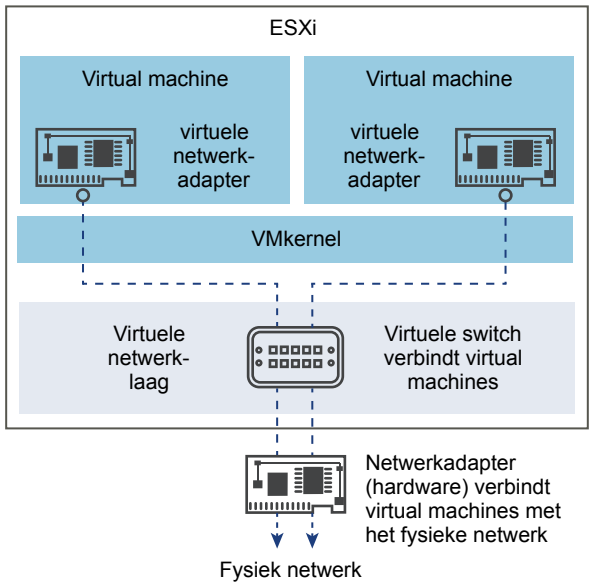
Figuur 2-9. Isolatie van virtual machines



De VMkernel bemiddelt tussen alle fysieke bronnen. Alle toegang tot fysieke hardware vindt plaats via de VMkernel en virtual machines kunnen dit isolatieniveau niet omzeilen.

Net zoals een fysieke machine via een netwerkkaart met andere machines binnen een netwerk communiceert, zo communiceert een virtual machine via een virtuele switch met andere virtual machines die op dezelfde host worden uitgevoerd. Daarnaast communiceert een virtual machine met het fysieke netwerk, inclusief andere virtual machines op andere ESXi-hosts, via een fysieke netwerkadapter.

Figuur 2-10. Virtuele netwerken via virtuele switches



Virtuele netwerken worden ook beïnvloed door de isolatie van virtual machines.

- Als een virtual machine geen virtuele switch deelt met een andere virtual machine, dan is deze volledig geïsoleerd van de virtual machines binnen de host.
- Als er geen fysieke netwerkadapter wordt geconfigureerd voor een virtual machine, dan is de virtual machine volledig geïsoleerd. Dit omvat tevens isolatie van fysieke of virtuele netwerken.
- Virtual machines zijn net zo veilig als fysieke machines wanneer u ze van het netwerk afschermt met behulp van firewalls, antivirussoftware, enzovoort.

U kunt virtual machines ook beschermen door het instellen van bronreserveringen en -limieten op de host. U kunt bijvoorbeeld brontoewijzing gebruiken om een virtual machine zodanig te configureren dat deze altijd beschikt over minimaal 10 procent en maximaal 20 procent van de CPU-bronnen van de host.

Brontoewijzingen en -limieten beschermen virtual machines tegen prestatieproblemen die het resultaat kunnen zijn van een andere virtual machine die te veel gedeelde hardwarebronnen gebruikt. Als een van de virtual machines op een host bijvoorbeeld is uitgeschakeld door een denial-of-service (DoS)-aanval, dan voorkomt een bronlimiet voor die machine dat de aanval zoveel van de hardwarebronnen gebruikt dat de andere virtual machines hierdoor ook worden beïnvloed. Op dezelfde manier zorgt een bronreservering voor elk van de virtual machines ervoor dat in het geval van een grote belasting van de bronnen door de virtual machine die het doel is van de Dos-aanval, alle andere virtual machines over voldoende bronnen beschikken om te blijven functioneren.

Standaard hanteert ESXi een vorm van bronreservering door het toepassen van een distributie-algoritme dat de beschikbare hostbronnen gelijkmatig verdeeld over de virtual machines, en tegelijkertijd een bepaald deel van de bronnen te reserveren voor andere systeemonderdelen. Dit standaardgedrag biedt een vorm van natuurlijke bescherming tegen DoS- en distributed denial-of-service (DDoS)-aanvallen. Specifieke bronreserveringen en -limieten worden op individuele basis ingesteld om het standaardgedrag zodanig aan te passen dat de distributie niet gelijkmatig is binnen de virtual-machineconfiguratie.

Beveiliging en virtuele netwerken

Als een ESXi-host wordt benaderd via vCenter Server, dan wordt vCenter Server over het algemeen beschermd door middel van een firewall. Deze firewall biedt fundamentele bescherming aan het netwerk.

Normaliter wordt een firewall ingericht op locaties die als toegangspunten van het systeem worden beschouwd. Een firewall kan zich tussen de clients en vCenter Server bevinden. vCenter Server en de clients kunnen zich ook achter de firewall bevinden voor implementatie.

Netwerken die zijn geconfigureerd met vCenter Server kunnen communicatie ontvangen via de vSphere Client of netwerkbeheerclients van derden. vCenter Server zoekt naar gegevens van de beheerde hosts en clients op aangewezen poorten. vCenter Server gaat er tevens vanuit dat de beheerde hosts zoeken naar gegevens van vCenter Server op aangewezen poorten. Firewalls tussen ESXi, vCenter Server en andere vSphere-onderdelen moeten open poorten hebben voor de ondersteuning van gegevensoverdracht.

Firewalls kunnen ook op verschillende andere toegangspunten in het netwerk worden toegevoegd, afhankelijk van hoe het netwerkgebruik is gepland en het beveiligingsniveau dat verschillende apparaten vereisen. Selecteer de locaties voor firewalls afhankelijk van de beveiligingsrisico's die zijn geïdentificeerd voor de netwerkconfiguratie.

Workloads beveiligen met VMware NSX

VMware NSX biedt Software-Defined Networking, beveiligingsservices met logisch firewallgebruik in virtuele netwerken, logisch schakelen en logische routering. Ontwerpers van virtuele netwerken stellen deze services programmatisch samen in de gewenste combinatie om unieke geïsoleerde virtuele netwerken tot stand te brengen. Deze technologie biedt een meer verfijnde beveiliging dan de traditionele hardwareapplicaties. In virtuele omgevingen kunt u deze services toepassen op vNIC-niveau. Traditionele services worden geconfigureerd op het fysieke netwerk.

Geselecteerde VMware NSX-mogelijkheden worden gedetailleerd beschreven in VMware NSX for vSphere (NSX) ontwerphandleiding voor netwerkvirtualisatie. U kunt procedures vinden om deze mogelijkheden te implenteren in de documentatie van VMware NSX for vSphere

NSX is het VMware-beveiligingsplatform voor netwerkvirtualisatie dat u kunt gebruiken om een veilige virtuele netwerkomgeving te bouwen voor uw Software-Defined Data Center. Gebruik NSX om een veilig gevirtualiseerd netwerk te maken door Software-Defined Firewalls, routers, gateways en hun beleidsregels te implementeren en te beheren. Terwijl VM's onafhankelijk zijn van het onderliggende platform en IT toestaan om fysieke hosts als een pool van rekencapaciteit te behandelen, zijn virtuele netwerken onafhankelijk van de onderliggende IP-netwerkhardware. IT kan het fysieke netwerk behandelen als een pool van transportcapaciteit die kan worden verbruikt of op aanvraag voor een nieuw doel kan worden ingesteld. Met NSX kunt u het noord-zuidrandverkeer en het oost-westverkeer tussen netwerk en stacks beschermen die de gegevensintegriteit moeten handhaven. Zo kunnen workloads van verschillende tenants bijvoorbeeld veilig worden uitgevoerd op individuele geïsoleerde virtuele netwerken, ook als ze hetzelfde onderliggende fysieke netwerk delen.

NSX -functies

NSX levert een volledige set logische netwerkelementen, boundaryprotocollen en beveiligingsservices om uw virtuele netwerken te organiseren en te beheren. Als u een NSX-invoegtoepassing installeert op vCenter Server, krijgt u centrale controle om NSX-onderdelen en -services te maken en te beheren via uw datacenter.

Zie de NSX-beheerhandleiding voor beschrijvingen van de functies en mogelijkheden van NSX.

VMware NSX Edge

Biedt centrale noord-zuidroutering tussen de logische netwerken die zijn geïmplementeerd in NSX-domeinen en de externe fysieke netwerkinfrastructuur. NSX Edge ondersteunt dynamische routeringsprotocollen zoals Open Shortest Path First (OSPF), internal Border Gateway Protocol (iBGP) en external Border Gateway Protocol (eBGP), en kan statische routering gebruiken. De routeringsoptie biedt actieve/stand-by stateful services en Equal-Cost Multipath Routing (ECMP). NSX Edge biedt ook standaardrandservices zoals Network Address Translation (NAT), taakverdeling, virtueel particulier netwerk (VPN) en firewallservices.

Logisch schakelen

NSX logische switches leveren logische netwerken op L2 waarbij isolatie van workloads op verschillende logische netwerken wordt afgedwongen. Virtueel gedistribueerde switches kunnen meerdere ESXi-hosts beslaan in een cluster over L3-materiaal door gebruik te maken van VXLAN-technologie, wat het voordeel van centraal beheer toevoegt. U kunt de omvang van de isolatie regelen door transportzones te maken met vCenter Server en waar nodig logische switches toe te wijzen aan de transportzones.

Gedistribueerde routering

Gedistribueerde routering wordt geboden door een logisch element dat Distributed Logical Router (DLR) wordt genoemd. De DLR is een router met rechtstreeks verbonden interfaces met alle hosts waar VM-connectiviteit is vereist. Logische switches worden verbonden met logische routers om L3-connectiviteit te bieden. De toezichthoudende functie, de control plane om fowarding te regelen, wordt geïmporteerd van een regelende VM.

Logisch firewallgebruik

Het NSX-platform ondersteunt de volgende kritieke functies om meerlagige workloads te beveiligen.

- Native ondersteuning voor logische firewallmogelijkheden biedt stateful bescherming van meerlagige workloads.
- Ondersteuning voor beveiligingsservices van meerdere leveranciers en service-invoeging, bijvoorbeeld scannen op virussen, voor de bescherming van workloads van toepassingen.

Het NSX-platform heeft een centrale firewallservice die wordt geleverd door de NSX Edge-servicesgateway (ESG) en een gedistribueerde firewall (DFW) die in de kernel wordt ingeschakeld als VIB-pakket op alle ESXi-hosts die deel uitmaken van een bepaald NSX-domein. De DFW biedt firewallgebruik met near-line rate prestaties, virtualisatie, identiteitsbewustzijn, activiteitscontrole, logboekregistratie en overige netwerkbeveiligingsfuncties die eigen zijn aan netwerkvirtualisatie. U configureert deze firewalls om verkeer op het vNIC-niveau van elke VM te filteren. Deze flexibiliteit is essentieel om geïsoleerde virtuele netwerken te maken, zelfs voor individuele VM's als dat detailniveau is vereist.

Gebruik vCenter Server om firewallregels te beheren. De regeltabel is ingedeeld in secties waarbij elke sectie bestaat uit een specifiek beveiligingsbeleid dat kan worden toegepast op specifieke workloads.

Beveiligingsgroepen

NSX biedt criteria voor groeperingsmechanismen die elk van de volgende items kunnen bevatten.

- vCenter Server-objecten zoals virtual machines, gedistribueerde switches en clusters
- Eigenschappen van virtual machines zoals vNIC's, namen van virtual machines en besturingssystemen van virtual machines
- NSX-objecten zoals logische switches, beveiligingstags en logische routers

Groeperingsmechanismen kunnen statisch of dynamisch zijn, en een beveiligingsgroep kan elke combinatie van objecten zijn, waaronder ook elke combinatie van vCenter-objecten, NSX-objecten, VM-eigenschappen of Identity Manager-objecten zoals AD-groepen. Een beveiligingsgroep in NSX is gebaseerd op alle statische en dynamische criteria in combinatie met statische uitsluitingscriteria zoals gedefinieerd door een gebruiker. Dynamische groepen groeien en krimpen als leden toetreden of de groep verlaten. Zo kan een dynamische groep bijvoorbeeld alle VM's bevatten die beginnen met de naam web_. Beveiligingsgroepen hebben diverse nuttige karakteristieken.

- U kunt meerdere beveiligingsbeleidsregels toewijzen aan een beveiligingsgroep.
- Een object kan tegelijk bij meerdere beveiligingsgroepen horen.
- Beveiligingsgroepen kunnen andere beveiligingsgroepen bevatten.

Gebruik NSX Service Composer om beveiligingsgroepen te maken en beleidsregels toe te passen. NSX Service Composer richt firewallbeleidsregels en beveiligingsservices in en wijst ze in real time toe aan toepassingen. Beleidsregels worden toegepast op nieuwe virtual machines wanneer ze worden toegevoegd aan de groep.

Beveiligingstags

U kunt beveiligingstags toepassen op elke virtual machine, waarbij waar nodig context over de workload wordt toegevoegd. U kunt beveiligingsgroepen baseren op beveiligingstags. Beveiligingstags geven diverse algemene classificaties aan.

- Beveiligingsstatus. Bijvoorbeeld, geïdentificeerde kwetsbaarheid.
- Classificatie per afdeling.
- Gegevenstype classificatie. Bijvoorbeeld PCI-gegevens.
- Type omgeving. Bijvoorbeeld productie of ontwikkeling.
- Geografie of locatie van VM.

Beveiligingsbeleid

Groepsregels voor beveiligingsbeleid zijn beveiligingsfuncties die worden toegepast op een beveiligingsgroep die is gemaakt in het datacenter. Met NSX kunt u secties maken in een tabel met firewallregels. Met deze secties kunt u uw firewallregels beter beheren en groeperen. Eén beveiligingsbeleid komt overeen met één sectie in een tabel met firewallregels. Dit beleid onderhoudt synchronisatie tussen regels in een tabel met firewallregels en regels die worden geschreven door het beveiligingsbeleid, zodat deze consistent worden toegepast. Aangezien beveiligingsbeleidsregels worden geschreven voor specifieke toepassingen of workloads, worden deze regels georganiseerd in specifieke secties in een tabel met firewallregels. U kunt meerdere beveiligingsbeleidsregels toewijzen aan één toepassing. De volgorde van de secties wanneer u meerdere beveiligingsbeleidsregels toepast, bepaalt de voorrang bij de toepassing van de regels.

Services voor virtuele particuliere netwerken

NSX biedt VPN-services, L2 VPN en L3 VPN genoemd. Maak een L2 VPN-tunnel tussen een paar van NSX Edge-apparaten die zijn geïmplementeerd op verschillende datacenterlocaties. Maak een L3 VPN om veilige L3-connectiviteit te bieden voor het datacenternetwerk vanaf andere externe locaties.

Op rollen gebaseerde toegangscontrole

NSX heeft ingebouwde gebruikersrollen die toegang tot computer- of netwerkbronnen in een bedrijf regelen. Gebruikers kunnen slechts één rol hebben.

Tabel 2-7. NSX -gebruikersrollen beheren

Rol	Rechten
Enterprisebeheerder	NSX-bewerkingen en -beveiliging.
NSX-beheerder	Alleen NSX-bewerkingen. Bijvoorbeeld: virtuele applicaties installeren, poortgroepen configureren.
Beveiligingsbeheerder	Alleen NSX-beveiliging. Bijvoorbeeld: gegevensbeveiligingsbeleid definiëren, poortgroepen maken, rapporten maken voor NSX-modules.
Auditor	Alleen-lezen.

Partnerintegratie

Services van VMware-technologiepartners worden geïntegreerd met het NSX-platform in de beheer-, bedienings- en gegevensfuncties om een consistente gebruikerservaring en naadloze integratie met elk cloudbeheerplatform te bieden. Zie https://www.vmware.com/products/nsx/technology-partners#security voor meer informatie.

NSX -concepten

SDDC-beheerders configureren functies van NSX zodanig dat netwerkisolatie en segmentatie in het datacenter worden gegarandeerd.

Netwerkisolatie

Isolatie is de basis voor de meeste vormen van netwerkbeveiliging, of het nu gaat om naleving, containment of isolatie van ontwikkeling, test- en productieomgevingen. Traditioneel worden ACL's, firewallregels en routeringsbeleidsregels gebruikt voor het instellen en handhaven van isolatie en meerdere tenants. Met netwerkvirtualisatie worden deze eigenschappen inherent ondersteund. Door middel van VXLAN-technologie worden virtuele netwerken standaard geïsoleerd van andere virtuele netwerken en van de onderliggende fysieke infrastructuur, waardoor een beveiligingsprincipe wordt toegepast op basis van minimale bevoegdheden. Virtuele netwerken worden geïsoleerd gecreëerd en blijven geïsoleerd tenzij er een expliciete verbinding is gemaakt. Er zijn geen fysieke subnetten, VLAN's, ACL's of firewallregels nodig om isolatie mogelijk te maken.

Netwerksegmentatie

Netwerksegmentatie is verwant aan isolatie, maar wordt toegepast in een meerlagig virtueel netwerk. Netwerksegmentatie is van oorsprong een functie van een fysieke firewall of router die is ontworpen om verkeer toe te staan of weigeren tussen netwerksegmenten of -lagen. Bij het segmenteren van verkeer tussen web, toepassing en databaselagen zijn traditionele configuratieprocessen tijdrovend en zeer gevoelig voor menselijke fouten, wat resulteert in een hoog percentage beveiligingslekken. Implementatie vereist expertise op het gebied van apparaatconfiguratie-syntaxis, netwerkadressering en toepassingspoorten en -protocollen.

Netwerkvirtualisatie vereenvoudigt het bouwen en testen van configuraties van netwerkservices voor de levering van beproefde configuraties die programmatisch in het netwerk kunnen worden geïmplementeerd en gedupliceerd om segmentatie toe te passen. Netwerksegmentatie is net als isolatie een kerncapaciteit van NSX-netwerkvirtualisatie.

Microsegmentatie

Microsegmentatie isoleert verkeer op het vNIC-niveau door het gebruik van gedistribueerde routers en firewalls. Toegangsbeheer op vNIC-niveau vergroot de efficiency ten opzichte van regels die op het fysieke netwerk zijn geïmplementeerd. U kunt microsegmentatie gebruiken met een NSX gedistribueerde firewall en binnen de implementatie gedistribueerde firewall om microsegmentatie toe te passen voor een drielaagse toepassing, bijvoorbeeld webserver, toepassingsserver en database waarbij meerdere organisaties dezelfde logische netwerktopologie kunnen delen.

Zero-trust-model

Om de strengste beveiligingsinstellingen te realiseren moet een zero-trust-model worden toegepast bij de configuratie van beveiligingsbeleidsregels. Een zero-trust-model geeft geen toegang tot resources en workloads tenzij dit specifiek is toegestaan door een beleid. In dit model moet verkeer op de goedgekeurde lijst staan om te zijn toegestaan. Zorg ervoor dat essentieel infrastructuurverkeer is toegestaan. Standaard zijn NSX Manager, NSX Controllers en NSX Edge-servicegateways uitgesloten van gedistribueerde firewallfuncties. vCenter Server-systemen zijn niet uitgesloten en moeten voor het toepassen van een dergelijk beleid expliciet worden toegestaan ter voorkoming van uitsluiting.

Beheercluster en tenantworkloads beschermen

Als u een SDDC-beheerder bent, kunt u NSX-mogelijkheden gebruiken voor het isoleren en beschermen van het vRealize Suite-beheercluster en tenantworkloads in het datacenter.

Het beheercluster omvat de vCenter Server voor het domein, de NSX Manager en vRealize Suite-producten en andere beheerproducten en -onderdelen. Gebruik Transport Layer Security (TLS) en verificatie om deze systemen te beschermen tegen ongeautoriseerde toegang. Gebruik NSX-mogelijkheden om de isolatie en segmentatie te verbeteren van de virtuele netwerksystemen van het beheercluster ten opzichte van het randcluster en de workloadsystemen en -clusters. Zorg voor de juiste toegang tot vereiste beheersysteempoorten zoals beschreven in de installatie- en configuratiedocumenten voor de geïmplementeerde beheersystemen.

Tenantworkloads in het datacenter kunnen worden geïmplementeerd als drielaagse toepassingen bestaande uit web-, toepassings- en databaseservers. Gebruik Transport Layer Security (TLS) en verificatie om deze systemen te beschermen tegen ongeautoriseerde toegang. Gebruik de beschikbare beveiligingsservices zoals database-verbindingsreeksen voor veilige verbindingen en SSH voor veilige hosttoegang. Pas NSX-mogelijkheden indien mogelijk toe op het vNic-niveau voor isolatie en microsegmentatie van tenantworkloads.

Voor meer informatie over het gebruik van NSX-mogelijkheden, zie VMware NSX for vSphere (NSX) ontwerphandleiding voor netwerkvirtualisatie. Voor procedures om mogelijkheden van NSX te configureren, raadpleeg de documentatie van VMware NSX for vSphere.

Checklist voor de installatie van vRealize Suite

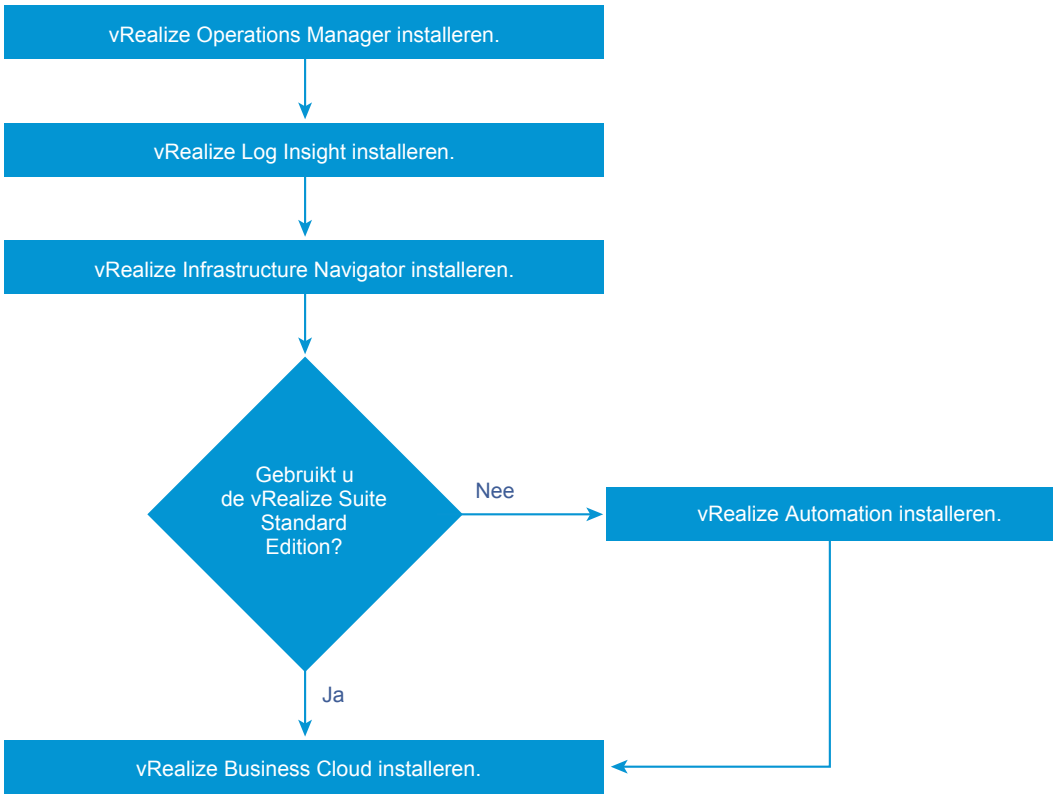
3

U downloadt, installeert en configureert vRealize Suite-producten afzonderlijk in een specifieke volgorde. Individuele producten in vRealize Suite worden geleverd als installatiepakketten voor Windows- of Linux-machines, of als virtuele applicaties die u kunt implementeren op virtual machines die worden uitgevoerd op ESXi-hosts. Welke producten u installeert, is afhankelijk van uw editie van vRealize Suite.

Controleer of uw vRealize Suite-producten de juiste versies hebben om te verzekeren dat ze met elkaar samenwerken. Zie Compatibiliteitshandleidingen voor VMware voor meer informatie over gecertificeerde compatibiliteit van VMware.

U kunt ook vRealize Suite Lifecycle Manager gebruiken om de vRealize Suite in zijn geheel te installeren in één vereenvoudigd installatieproces. Zie Installatie en beheer van vRealize Suite Lifecycle Manager.

Figuur 3-1. Implementatieproces voor vRealize Suite



Tabel 3-1. Checklist voor de installatie van vRealize Suite

vRealize Suite-producten	Meer informatie
 Installeer vRealize Operations Manager als virtuele applicatie of op een Windows- of Linux-server.	Raadpleeg de installatiedocumentatie voor uw versie van vRealize Operations Manager. ■ vRealize Operations Manager 6.6 installeren ■ vRealize Operations Manager 6.5 installeren ■ vRealize Operations Manager 6.4 installeren ■ vRealize Operations Manager 6.3 installeren ■ vRealize Operations Manager 6.2 installeren
 Installeer vRealize Log Insight als een virtuele applicatie.	Raadpleeg de installatiedocumentatie voor uw versie van vRealize Log Insight. ■ vRealize Log Insight 4.5 installeren ■ vRealize Log Insight 4.3 installeren ■ Aan de slag met VMware vRealize Log Insight 4.0 ■ Handleiding Aan de slag voor VMware vRealize Log Insight 3.6 ■ Handleiding Aan de slag voor VMware vRealize Log Insight 3.3.1
 Installeer vRealize Infrastructure Navigator als een virtuele applicatie.	Raadpleeg de Installatie- en configuratiehandleiding voor vRealize Infrastructure Navigator.
 Als u de Advanced of Enterprise Edition van vRealize Suite hebt aangeschaft, installeer dan vRealize Automation. U installeert een vRealize Automation-applicatie met beheer- en selfservicefunctionaliteit, en een Infrastructure as a Service (IaaS) Windows-server die infrastructuurvoorzieningen ondersteunt voor vectorproducten.	1 Plan uw installatie. Raadpleeg de documentatie voor referentie-architectuur voor uw versie van vRealize Automation. ■ vRealize Automation 7.3 referentie-architectuur ■ vRealize Automation 7.2 referentie-architectuur ■ vRealize Automation 7.1 referentie-architectuur ■ vRealize Automation 7.0.1 referentie-architectuur 2 Installeer vRealize Automation. Raadpleeg de installatiedocumentatie voor uw versie van vRealize Automation. ■ vRealize Automation 7.3 installeren ■ vRealize Automation 7.2 installeren of upgraden ■ vRealize Automation 7.1 installeren of upgraden ■ vRealize Automation 7.0.1 installeren of upgraden
 Installeer vRealize Business for Cloud als een virtuele applicatie.	Raadpleeg de installatiedocumentatie voor uw versie van vRealize Business for Cloud. ■ Installatie en beheer vRealize Business for Cloud 7.3 ■ Installatie en beheer van vRealize Business for Cloud 7.2 ■ Installatiehandleiding voor vRealize Business for Cloud 7.1 ■ Installatiehandleiding voor vRealize Business for Cloud 7.0.1.

Upgraden vanaf oudere versies van vRealize Suite of vCloud Suite

4

U kunt vRealize Suite upgraden vanaf vCloud Suite of een oudere versie van vRealize Suite door de afzonderlijke producten te upgraden naar actuele versies. Houd de aanbevolen updatevolgorde aan om te verzekeren dat vRealize Suite zonder problemen wordt geüpgraded.

Controleer voor het upgraden voor elk product de VMware-interoperabiliteitsmatrix om te verzekeren dat u beschikt over ondersteunde, compatibele productversies. Zie de website met VMware-interoperabiliteitsmatrices.

Tabel 4-1. vRealize Suite -producten upgraden

Product	Meer informatie
VMware vRealize Operations Manager	U kunt van vCenter Operations Manager overstappen naar een nieuwe installatie van VMware vRealize Operations Manager. Zie vCenter Operations Manager-implementatie migreren naar deze versie .
vRealize Infrastructure Navigator	vCenter Infrastructure Navigator upgraden
vRealize Log Insight	vRealize Log Insight upgraden
vRealize Automation	vRealize Automation upgraden
vRealize Business for Cloud	Upgraden naar vRealize Business for Cloud

Index

V

W