Informationen Zu Load Balancer Options

NetApp Solutions

NetApp
April 26, 2024

Inhalt

Die Load Balancer-Optionen werden untersucht

Eine in Anthos implementierte Applikation ist der Welt durch einen Service ausgesetzt, der von einem Load Balancer in der On-Premises-Umgebung von Anthos bereitgestellt wird.

Die folgenden Seiten verfügen über zusätzliche Informationen zu den in Anthos mit NetApp validierten Load Balancer-Optionen:

- "Installation von F5 BIG-IP Load Balancer"
- "Installation von MetalLB Load Balancer"
- "Installieren von Seesaw-Load-Balancer"

Installation von F5 BIG-IP Load Balancer

F5 BIG-IP ist ein Application Delivery Controller (ADC), der eine breite Palette an fortschrittlichen, produktionsbereiten Traffic Management- und Sicherheitsservices wie L4-L7 Load Balancing, SSL/TLS-Entlastung, DNS, Firewall und mehr bietet. Diese Services sorgen für eine deutlich höhere Verfügbarkeit, Sicherheit und Performance Ihrer Applikationen.

F5 BIG-IP kann auf verschiedene Arten implementiert und genutzt werden, beispielsweise auf dedizierter Hardware, in der Cloud oder als virtuelle Appliance vor Ort. Lesen Sie die Dokumentation hier, um F5 BIG-IP zu erkunden und zu implementieren.

F5 BIG-IP war das erste Load Balancer-System, das bei Anthos On-Premises verfügbar war. Bei den ersten Anthos Ready Partner-Validierungen für Anthos mit NetApp Lösung wurde es eingesetzt.

> F5 BIG-IP kann im Standalone- oder Cluster-Modus implementiert werden. Zum Zweck dieser Validierung wurde F5 BIG-IP im Standalone-Modus implementiert. Aus Produktionsgründen empfiehlt NetApp jedoch die Erstellung eines Clusters MIT BIG-IP-Instanzen, um Single Point of Failure zu vermeiden.

> Ein F5 BIG-IP System kann auf dedizierter Hardware, in der Cloud oder als virtuelle Appliance on-Premises mit Versionen über 12.x bereitgestellt werden, damit es mit F5 CIS integriert werden kann. Für dieses Dokument wurde das F5 BIG-IP System als virtuelle Appliance validiert, beispielsweise mit DER BIG-IP VE Edition.

Validierte Versionen

Diese Lösung nutzt die in VMware vSphere implementierte virtuelle Appliance. Die Netzwerkkonfigurationen für die virtuelle F5 Big-IP Appliance können je nach Netzwerkumgebung in Konfigurationen mit zwei oder drei bewaffneten Konfigurationen konfiguriert werden. Die Bereitstellung in diesem Dokument basiert auf der Konfiguration mit zwei Scharfstellen. Weitere Informationen zur Konfiguration der virtuellen Appliance für die Verwendung mit Anthos finden Sie hier "Hier".

Das Solutions Engineering Team von NetApp hat die Versionen in der folgenden Tabelle für die On-Premises-Implementierung von Anthos validiert:

Make	Typ	Version
F5	BIG-IP VE	15.0.1-0.0.11
F5	BIG-IP VE	16.1.0-0.0.19

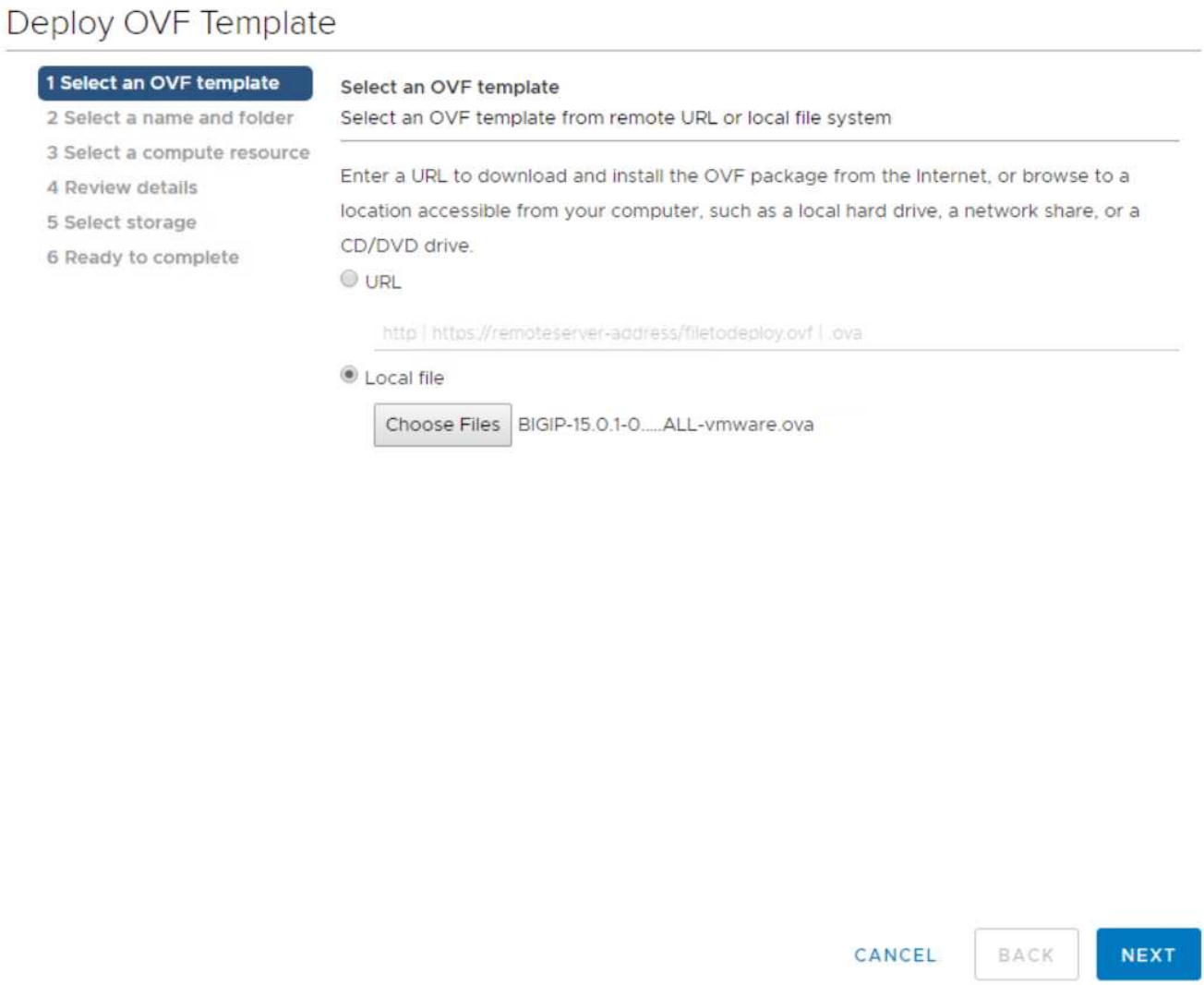
Installation

Gehen Sie wie folgt vor, um F5 BIG-IP zu installieren:

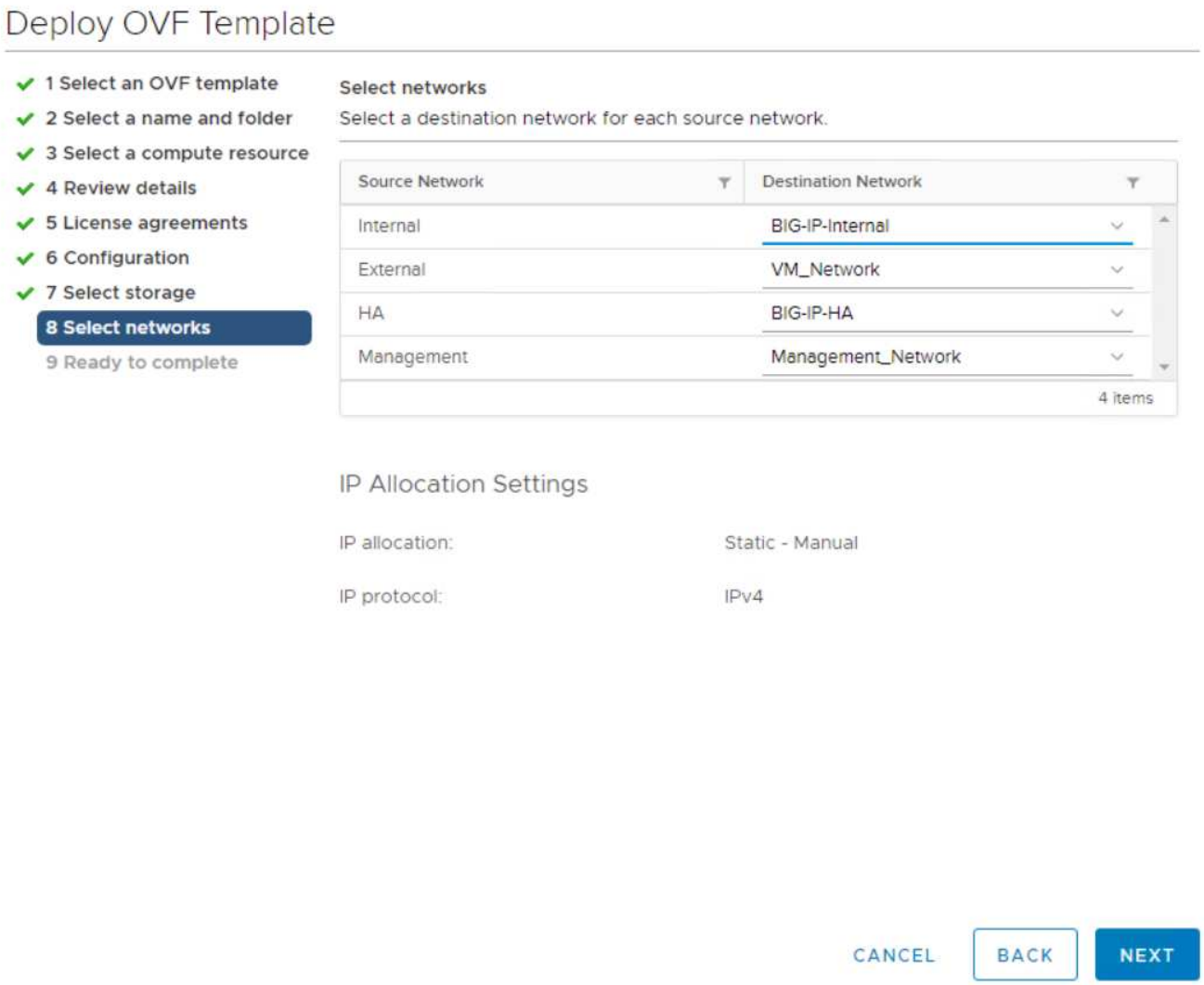
1. Laden Sie die OVA-Datei (Open Virtual Appliance) der virtuellen Anwendung von F5 herunter "Hier".

> Um die Appliance herunterzuladen, muss sich ein Benutzer bei F5 registrieren. Sie stellen eine 30-Tage-Demo-Lizenz für den Big-IP Virtual Edition Load Balancer bereit. NetApp empfiehlt eine permanente 10-Gbit/s-Lizenz für die Implementierung einer Appliance in Produktionsumgebungen.

2. Klicken Sie mit der rechten Maustaste auf den Infrastruktur-Ressourcen-Pool, und wählen Sie OVF-Vorlage bereitstellen aus. Ein Assistent startet, mit dem Sie die OVA-Datei auswählen können, die Sie gerade in Schritt 1 heruntergeladen haben. Klicken Sie Auf Weiter.



3. Klicken Sie auf Weiter, um die einzelnen Schritte fortzusetzen und die Standardwerte für jeden angezeigten Bildschirm zu akzeptieren, bis Sie den Bildschirm zur Speicherauswahl erreichen. Wählen Sie den VM_Datastore aus, für den Sie die virtuelle Maschine bereitstellen möchten, und klicken Sie dann auf Weiter.
4. Auf dem nächsten Bildschirm des Assistenten können Sie die virtuellen Netzwerke für die Verwendung in der Umgebung anpassen. Wählen Sie VM_Network für das Feld External aus, und wählen Sie Management_Network für das Feld Management aus. Interne Konfigurationen und HA werden für erweiterte Konfigurationen der F5 Big-IP Appliance verwendet und sind nicht konfiguriert. Diese Parameter können allein gelassen oder für die Verbindung mit verteilten Portgruppen ohne Infrastruktur konfiguriert werden. Klicken Sie Auf Weiter.

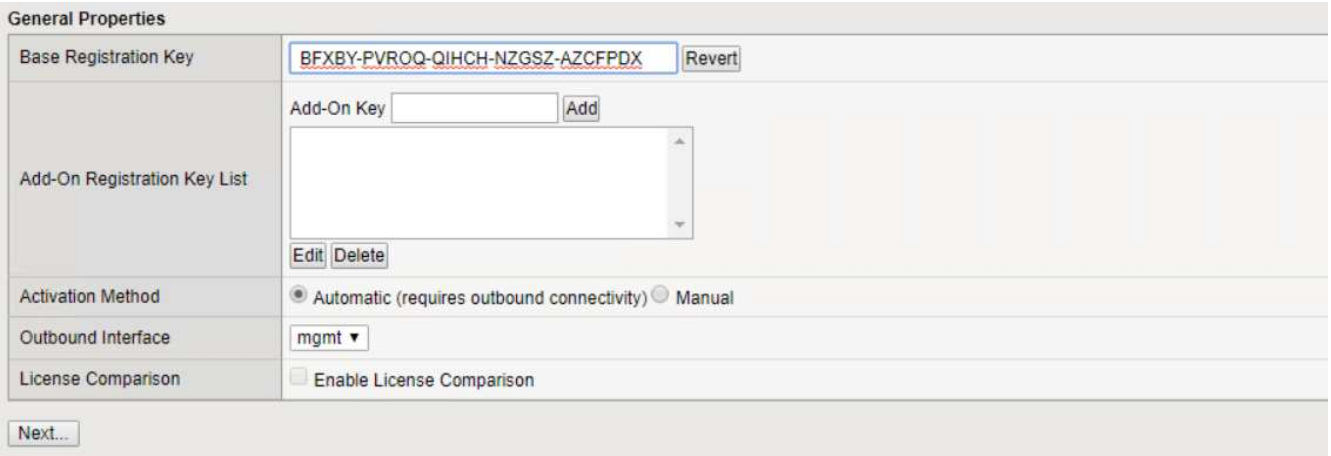


5. Prüfen Sie den Übersichtsbildschirm für das Gerät und klicken Sie, wenn alle Informationen richtig sind, auf Fertig stellen, um die Bereitstellung zu starten.
6. Klicken Sie nach der Implementierung der virtuellen Appliance mit der rechten Maustaste, und schalten Sie sie ein. Er sollte eine DHCP-Adresse im Managementnetzwerk erhalten. Die Appliance ist auf Linux basiert und verfügt über VMware Tools, sodass Sie die im vSphere Client empfangenen DHCP-Adressen anzeigen können.

7. Öffnen Sie einen Webbrowser, und stellen Sie im vorherigen Schritt eine Verbindung mit dem Gerät unter der IP-Adresse her. Die Standardanmeldedaten sind admin/admin. Nach der ersten Anmeldung werden Sie umgehend aufgefordert, das Admin-Passwort zu ändern. Sie gelangen dann zu einem Bildschirm, auf dem Sie sich mit den neuen Anmeldedaten anmelden müssen.

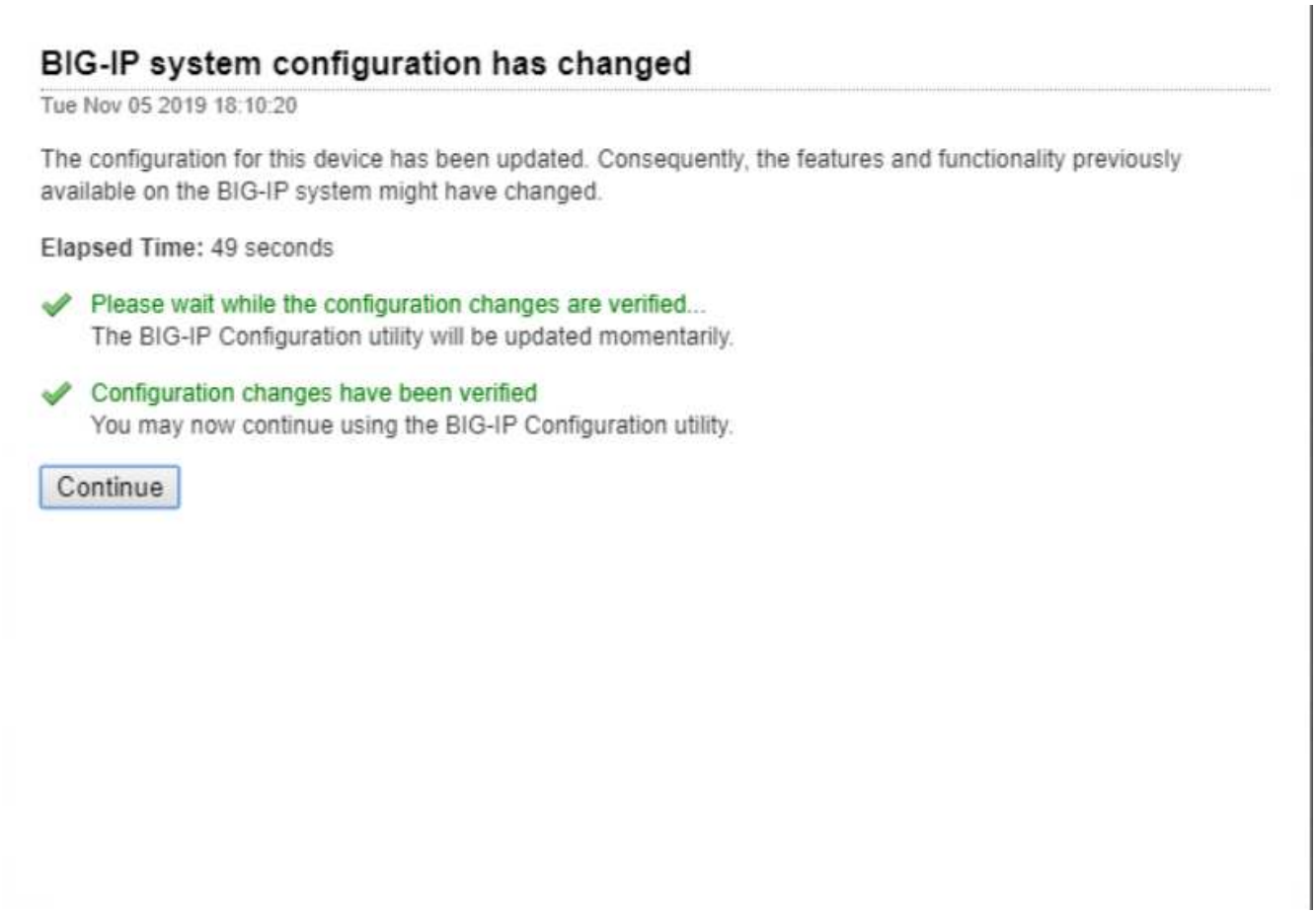
8. Der erste Bildschirm fordert den Benutzer auf, das Setup-Dienstprogramm abzuschließen. Starten Sie das Dienstprogramm, indem Sie auf Weiter klicken.

9. Im nächsten Bildschirm wird die Aktivierung der Lizenz für das Gerät angezeigt. Klicken Sie zum Starten auf Aktivieren. Wenn Sie auf der nächsten Seite dazu aufgefordert werden, fügen Sie entweder den 30-Tage-Evaluierungslizenzschlüssel ein, den Sie bei der Anmeldung zum Download erhalten haben, oder die dauerhafte Lizenz, die Sie beim Kauf des Geräts erworben haben. Klicken Sie Auf Weiter.

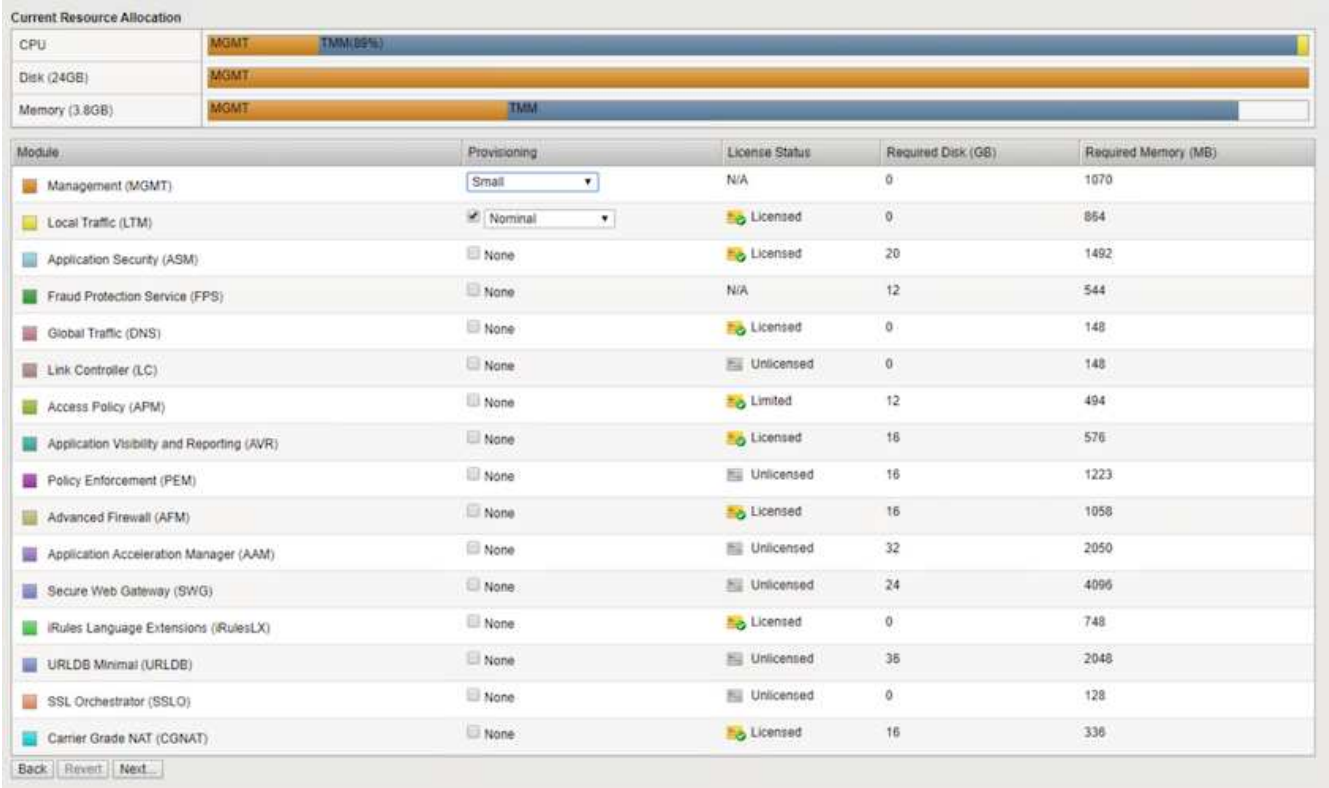


> Damit das Gerät die Aktivierung durchführen kann, muss das auf der Verwaltungsschnittstelle definierte Netzwerk in der Lage sein, das Internet zu erreichen.

10. Auf dem nächsten Bildschirm wird die Endbenutzer-Lizenzvereinbarung (End User License Agreement, EULA) angezeigt. Wenn die Bedingungen in der Lizenz akzeptabel sind, klicken Sie auf Akzeptieren.
11. Auf dem nächsten Bildschirm wird die verstrichene Zeit gezählt, während die bisherigen Konfigurationsänderungen überprüft werden. Klicken Sie auf Weiter, um mit der Erstkonfiguration fortzufahren.

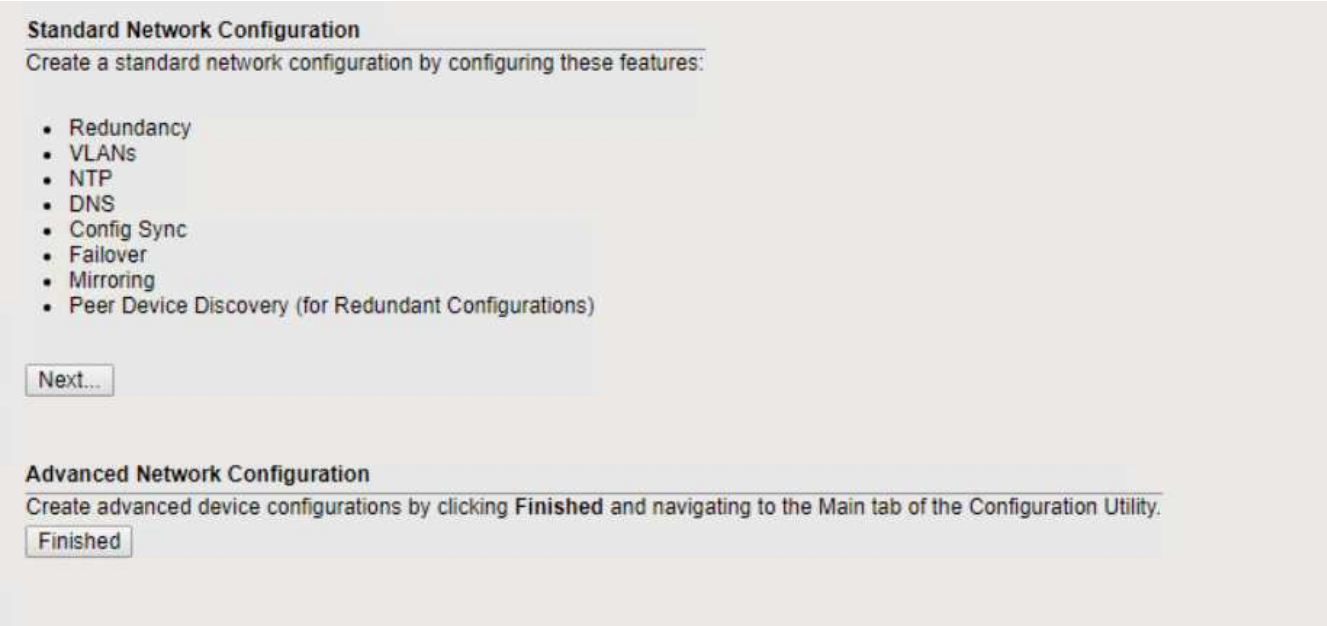


12. Das Fenster Konfigurationsänderung wird geschlossen, und im Setup-Dienstprogramm wird das Menü Ressourcenbereitstellung angezeigt. In diesem Fenster werden die derzeit lizenzierten Funktionen sowie die aktuellen Ressourcenzuordnungen für die virtuelle Appliance und jeden laufenden Service aufgeführt.

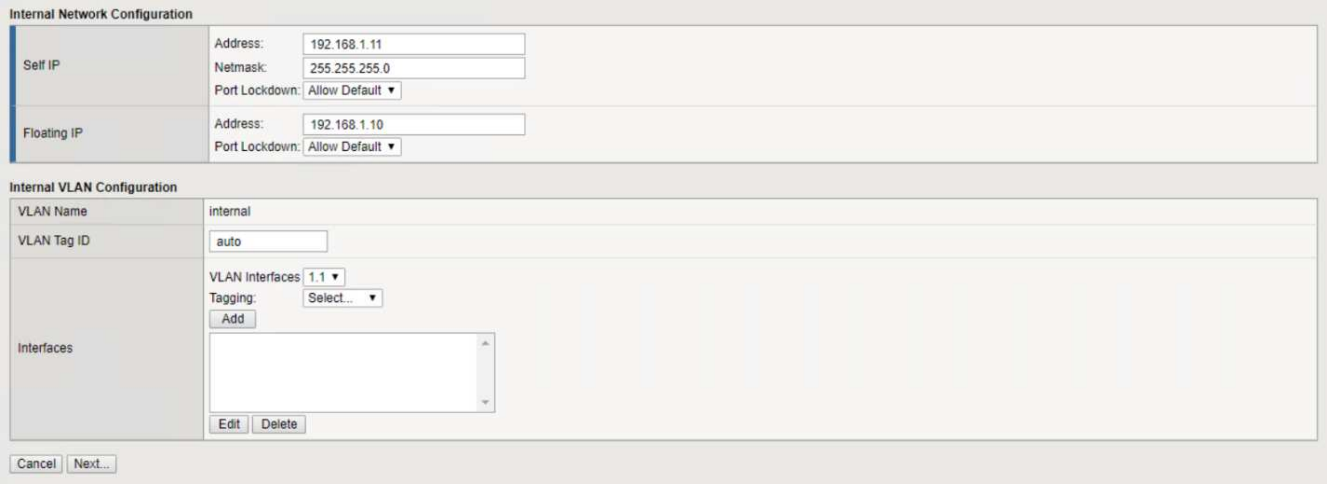


13. Durch Klicken auf die Menüoption Plattform auf der linken Seite kann die Plattform zusätzlich geändert werden. Änderungen umfassen die Einstellung der Management-IP-Adresse, die mit DHCP konfiguriert ist, die Einstellung des Host-Namens und der Zeitzone, in der die Appliance installiert ist, sowie das Sichern der Appliance über den Zugriff über SSH.

14. Klicken Sie dann auf das Menü Netzwerk, mit dem Sie Standard-Netzwerkfunktionen konfigurieren können. Klicken Sie auf Weiter, um den Assistenten für die Standard-Netzwerkkonfiguration zu starten.

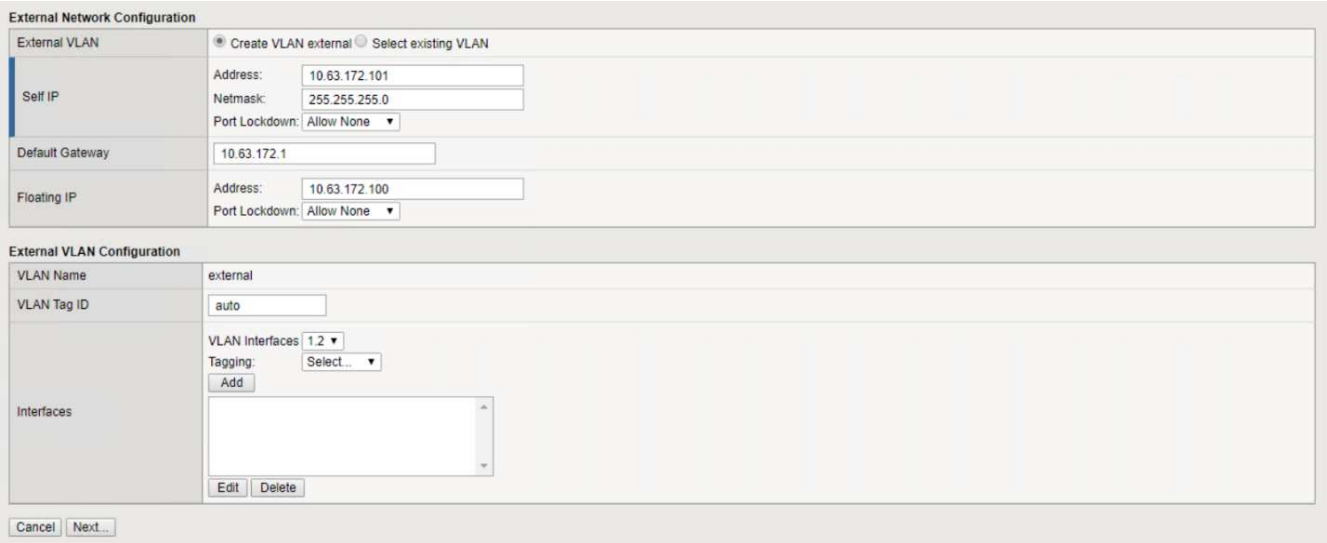


15. Auf der ersten Seite des Assistenten werden die Redundanz konfiguriert; lassen Sie die Standardeinstellungen, und klicken Sie auf Weiter. Auf der nächsten Seite können Sie eine interne Schnittstelle am Load Balancer konfigurieren. Schnittstelle 1.1 wird dem VMNIC namens Internal im OVF-Bereitstellungsassistenten zugeordnet.

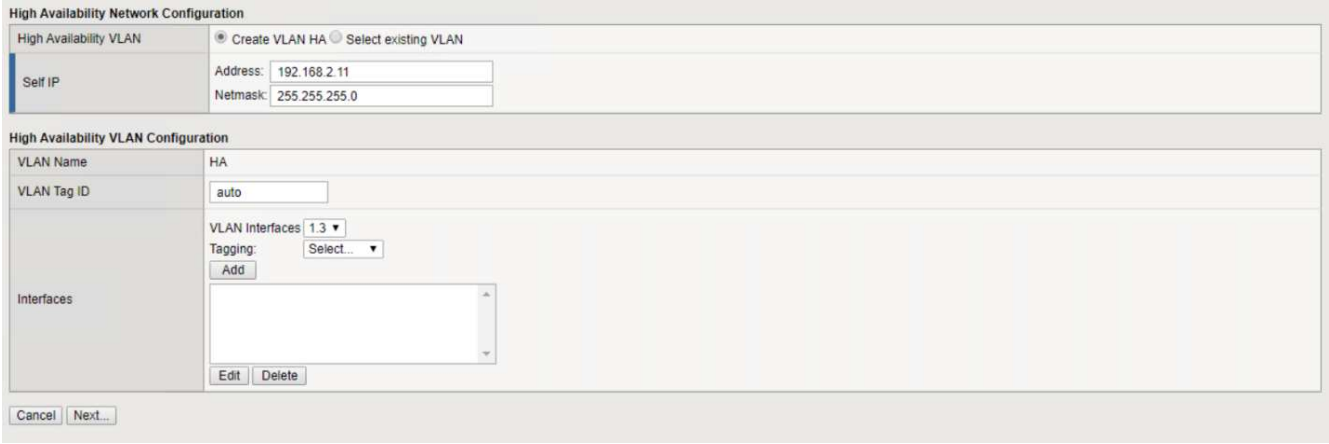


Die Leerzeichen auf dieser Seite für Self IP Address, Netzmaske und Floating IP-Adresse können mit einer nicht routingfähigen IP-Adresse ausgefüllt werden, die als Platzhalter verwendet werden kann. Sie können auch mit einem internen Netzwerk gefüllt werden, das als verteilte Portgruppe für virtuelle Gäste konfiguriert wurde, wenn Sie die drei-bewaffnete Konfiguration bereitstellen. Sie müssen abgeschlossen sein, um mit dem Assistenten fortzufahren.

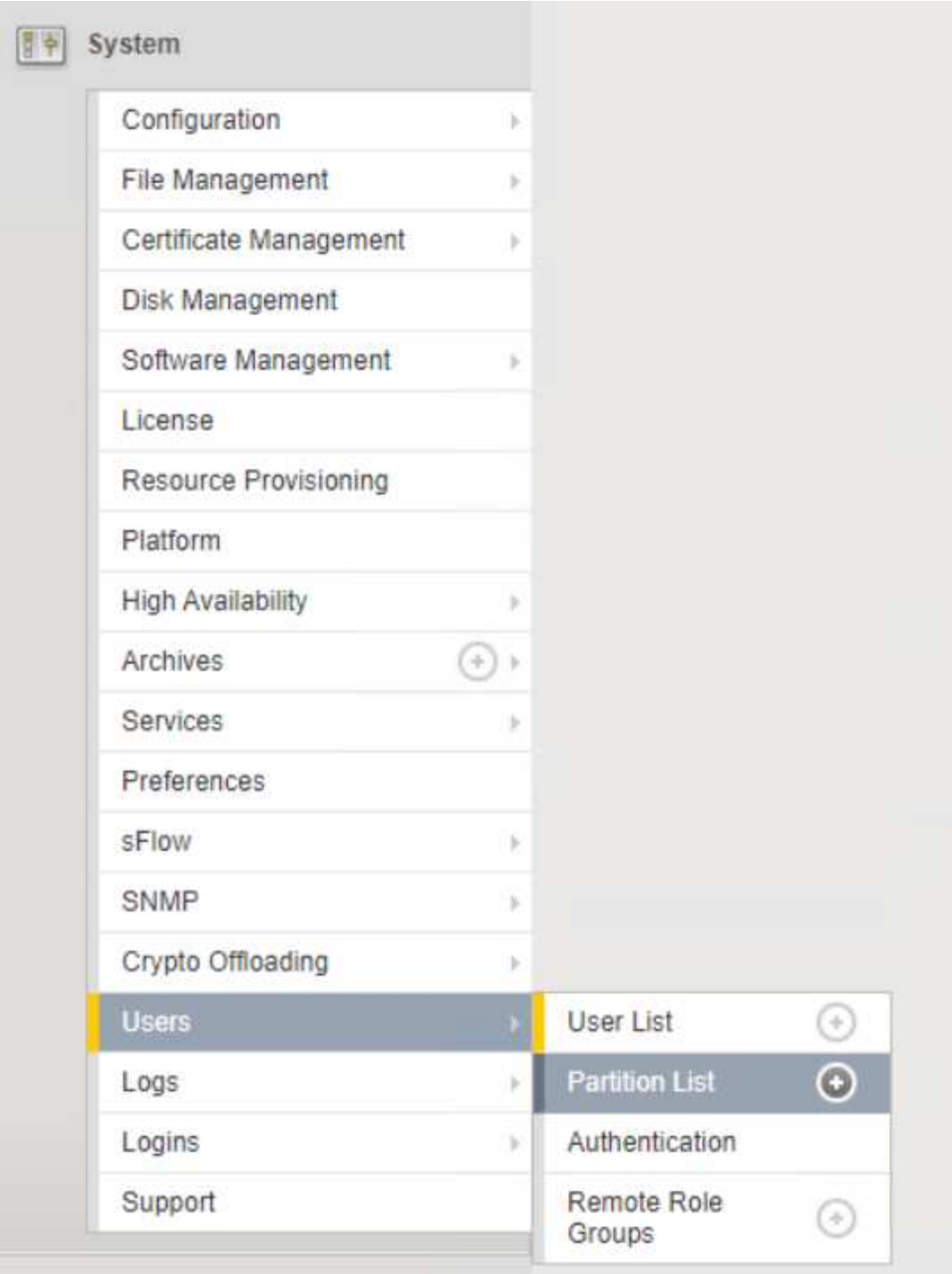
16. Auf der nächsten Seite können Sie ein externes Netzwerk konfigurieren, mit dem Services den in Kubernetes implementierten Pods zugeordnet werden können. Wählen Sie aus dem Bereich VM_Network eine statische IP, die entsprechende Subnetzmaske und eine unverankerte IP aus demselben Bereich aus. Schnittstelle 1.2 wird dem VMNIC namens External im OVF-Bereitstellungsassistenten zugeordnet.



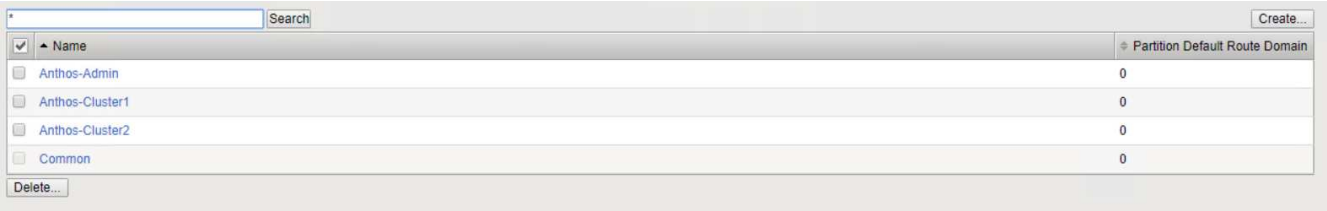
17. Auf der nächsten Seite können Sie ein internes HA-Netzwerk konfigurieren, wenn Sie mehrere virtuelle Appliances in der Umgebung bereitstellen. Um fortzufahren, müssen Sie die Felder Self-IP Address und Netmasks ausfüllen. Sie müssen Schnittstelle 1.3 als VLAN Interface auswählen, das dem vom OVF-Vorlagenassistenten definierten HA-Netzwerk zugeordnet wird.



18. Auf der nächsten Seite können Sie die NTP-Server konfigurieren. Klicken Sie dann auf Weiter, um mit dem DNS-Setup fortzufahren. Die DNS-Server und die Domänensuchliste sollten bereits vom DHCP-Server ausgefüllt werden. Klicken Sie auf Weiter, um die Standardeinstellungen zu übernehmen und fortzufahren.
19. Klicken Sie für den Rest des Assistenten auf Weiter, um das Advanced Peering Setup fortzusetzen, dessen Konfiguration über den Umfang dieses Dokuments hinausgeht. Klicken Sie anschließend auf Fertig stellen, um den Assistenten zu beenden.
20. Erstellen Sie einzelne Partitionen für den Anthos Admin-Cluster und für jeden in der Umgebung implementierten Benutzer-Cluster. Klicken Sie im Menü auf der linken Seite auf System, navigieren Sie zu Benutzern, und klicken Sie auf Partitionsliste.



21. Der angezeigte Bildschirm zeigt nur die aktuelle gemeinsame Partition an. Klicken Sie auf der rechten Seite auf Erstellen, um die erste zusätzliche Partition zu erstellen, und benennen Sie sie `GKE-Admin`. Klicken Sie dann auf Wiederholen, und benennen Sie die Partition `User-Cluster-1`. Klicken Sie erneut auf die Schaltfläche Wiederholen, um die nächste Partition zu benennen `User-Cluster-2`. Klicken Sie abschließend auf Fertig, um den Assistenten abzuschließen. Der Bildschirm Partitionsliste wird mit allen jetzt aufgeführten Partitionen angezeigt.



Integration in Anthos

In jeder Konfigurationsdatei gibt es einen Abschnitt, bzw. für das Admin-Cluster. Jedes Benutzer-Cluster, das Sie bereitstellen möchten, um den Load Balancer zu konfigurieren, sodass er von Anthos On-Premises gemanagt wird.

Das folgende Skript ist ein Beispiel aus der Konfiguration der Partition für den GKE-Admin-Cluster. Die Werte, die nicht kommentiert und geändert werden müssen, werden in Fettdruck unten gesetzt:

```
# (Required) Load balancer configuration
loadBalancer:
  # (Required) The VIPs to use for load balancing
  vips:
    # Used to connect to the Kubernetes API
    controlPlaneVIP: "10.61.181.230"
    # # (Optional) Used for admin cluster addons (needed for multi cluster
features). Must
    # # be the same across clusters
    # # addonsVIP: ""
  # (Required) Which load balancer to use "F5BigIP" "Seesaw" or
"ManualLB". Uncomment
  # the corresponding field below to provide the detailed spec
  kind: F5BigIP
  # # (Required when using "ManualLB" kind) Specify pre-defined nodeports
  # manualLB:
  #   # NodePort for ingress service's http (only needed for user cluster)
  #   ingressHTTPNodePort: 0
  #   # NodePort for ingress service's https (only needed for user
cluster)
  #   ingressHTTPSNodePort: 0
  #   # NodePort for control plane service
  #   controlPlaneNodePort: 30968
  #   # NodePort for addon service (only needed for admin cluster)
  #   addonsNodePort: 31405
  # # (Required when using "F5BigIP" kind) Specify the already-existing
partition and
  # # credentials
  f5BigIP:
    address: "172.21.224.21"
    credentials:
```

```
      username: "admin"
      password: "admin-password"
    partition: "GKE-Admin"
  #   # # (Optional) Specify a pool name if using SNAT
  #   # snatPoolName: ""
  # (Required when using "Seesaw" kind) Specify the Seesaw configs
  # seesaw:
    # (Required) The absolute or relative path to the yaml file to use for
IP allocation
    # for LB VMs. Must contain one or two IPs.
    #  ipBlockFilePath: ""
    # (Required) The Virtual Router IDentifier of VRRP for the Seesaw
group. Must
    # be between 1-255 and unique in a VLAN.
    #  vrid: 0
    # (Required) The IP announced by the master of Seesaw group
    #  masterIP: ""
    # (Required) The number CPUs per machine
    #  cpus: 4
    # (Required) Memory size in MB per machine
    #   memoryMB: 8192
    # (Optional) Network that the LB interface of Seesaw runs in (default:
cluster
    # network)
    #   vCenter:
      # vSphere network name
      #     networkName: VM_Network
    # (Optional) Run two LB VMs to achieve high availability (default:
false)
    #   enableHA: false
```

Installation von MetalLB Load Balancer

Auf dieser Seite werden die Installations- und Konfigurationsanweisungen für den von der MetalLB verwalteten Load Balancer aufgeführt.

Installieren des MetalLB Load Balancer

Der MetalLB Load Balancer ist vollständig mit Anthos Clusters auf VMware integriert und hat eine automatisierte Bereitstellung als Teil der Admin- und User-Cluster-Setups ab der Version 1.11 durchgeführt. Es gibt Textblöcke in der jeweiligen `cluster.yaml` Konfigurationsdateien, die Sie ändern müssen, um Informationen zum Load Balancer bereitzustellen. Die Lösung wird automatisch auf Ihrem Anthos Cluster gehostet, anstatt externe Ressourcen wie die anderen unterstützten Load Balancer-Lösungen bereitzustellen. Sie können auch einen ip-Pool erstellen, der automatisch Adressen bei der Erstellung von Kubernetes-Services des Typs Load Balancer in Clustern zuweist, die nicht auf einem Cloud-Provider ausgeführt werden.

Integration in Anthos

Wenn Sie den MetalLB Load Balancer für Anthos Admin aktivieren, müssen Sie einige Zeilen im ändern `loadBalancer:` Abschnitt, der in vorhanden ist `admin-cluster.yaml` Datei: Die einzigen Werte, die Sie ändern müssen, sind die Einstellung des `controlPlaneVIP:` Adresse und dann die einstellen `kind:` Als MetalLB. Ein Beispiel hierfür finden Sie im folgenden Code-Snippet:

```
# (Required) Load balancer configuration
loadBalancer:
  # (Required) The VIPs to use for load balancing
  vips:
    # Used to connect to the Kubernetes API
    controlPlaneVIP: "10.61.181.230"
    # # (Optional) Used for admin cluster addons (needed for multi cluster
features). Must
    # # be the same across clusters
    # addonsVIP: ""
  # (Required) Which load balancer to use "F5BigIP" "Seesaw" "ManualLB" or
"MetalLB".
  # Uncomment the corresponding field below to provide the detailed spec
  kind: MetalLB
```

Bei Aktivierung des MetalLB Load Balancer für Anthos-Benutzer-Cluster gibt es jeweils zwei Bereiche `user-cluster.yaml` Datei, die aktualisiert werden muss. Erstens, in einer Weise ähnlich wie die `admin-cluster.yaml` Datei, müssen Sie die ändern `controlPlaneVIP:`, `ingressVIP:`, und `kind:` Werte in der `loadBalancer:` Abschnitt. Ein Beispiel hierfür finden Sie im folgenden Code-Snippet:

```
loadBalancer:
  # (Required) The VIPs to use for load balancing
  vips:
    # Used to connect to the Kubernetes API
    controlPlaneVIP: "10.61.181.240"
    # Shared by all services for ingress traffic
    ingressVIP: "10.61.181.244"
  # (Required) Which load balancer to use "F5BigIP" "Seesaw" "ManualLB" or
"MetalLB".
  # Uncomment the corresponding field below to provide the detailed spec
  kind: MetalLB
```

> Die ingressVIP IP-Adresse muss im Pool der IP-Adressen vorhanden sein, die dem MetalLB Load Balancer später in der Konfiguration zugewiesen wurden.

Dann müssen Sie zum navigieren `metalLB:` Unterabschnitt und ändern Sie den `addressPools:` Wenn Sie den Pool im benennen `- name:` Variabel. Sie müssen außerdem einen Pool mit ip-Adressen erstellen, den MetalLB Services vom Typ Load Balancer zuweisen kann, indem Sie dem einen Bereich zur Verfügung stellen `addresses:` Variabel.

```
# # (Required when using "MetalLB" kind in user clusters) Specify the
MetalLB config
 metalLB:
 #   # (Required) A list of non-overlapping IP pools used by load balancer
typed services.
 #   # Must include ingressVIP of the cluster.
    addressPools:
 #   # (Required) Name of the address pool
    - name: "default"
 #     # (Required) The addresses that are part of this pool. Each address
must be either
 #     # in the CIDR form (1.2.3.0/24) or range form (1.2.3.1-1.2.3.5).
      addresses:
      - "10.61.181.244-10.61.181.249"
```

> Der Adressenpool kann wie im Beispiel als Bereich bereitgestellt werden, indem er sich auf eine Anzahl von Adressen in einem bestimmten Subnetz beschränkt, oder er kann als CIDR-Notation bereitgestellt werden, wenn das gesamte Subnetz zur Verfügung gestellt wird.

1. Wenn Kubernetes-Services vom Typ loadbalancer erstellt werden, weist MetalLB den Diensten automatisch eine externe IP zu und gibt die IP-Adresse durch Antwort auf ARP-Anfragen an.

Installieren von Seesaw-Load-Balancer

Auf dieser Seite werden die Installations- und Konfigurationsanweisungen für den vom Seesaw verwalteten Load Balancer aufgeführt.

Seesaw ist der Standard-verwaltete Netzwerk-Load-Balancer, der in einer Anthos-Cluster-Umgebung von Version 1.6 bis 1.10 installiert ist.

Installieren des Load Balancer für die Seifentäfer

Der Seesaw Load Balancer ist vollständig mit Anthos Clusters auf VMware integriert und hat eine automatisierte Implementierung als Teil der Admin- und User-Cluster-Setups durchgeführt. Im befinden sich Textblöcke `cluster.yaml` Konfigurationsdateien, die geändert werden müssen, um Informationen zum Load Balancer bereitzustellen. Vor der Cluster-Bereitstellung ist dann ein zusätzlicher Schritt erforderlich, um den Load Balancer mit dem integrierten bereitzustellen `gkectl` Werkzeug.

> Seesaw Load Balancer können im HA- oder Non-HA-Modus eingesetzt werden. Im Rahmen dieser Validierung wurde der Seesaw-Load-Balancer im Non-HA-Modus eingesetzt, der Standardeinstellung. Für die Produktion empfiehlt NetApp die Implementierung von Seesaw in einer HA-Konfiguration, um Fehlertoleranz und Zuverlässigkeit zu gewährleisten.

Integration in Anthos

In jeder Konfigurationsdatei gibt es einen Abschnitt, bzw. für das Admin-Cluster. In jedem Benutzer-Cluster können Sie den Load Balancer so konfigurieren, dass er von Anthos On-Premises gemanagt wird.

Der folgende Text ist ein Beispiel aus der Konfiguration der Partition für das GKE-Admin-Cluster. Die Werte, die nicht kommentiert und geändert werden müssen, werden in Fettdruck unten gesetzt:

```
loadBalancer:
  # (Required) The VIPs to use for load balancing
  vips:
    # Used to connect to the Kubernetes API
    controlPlaneVIP: "10.61.181.230"
    # # (Optional) Used for admin cluster addons (needed for multi cluster
features). Must
    # # be the same across clusters
    # # addonsVIP: ""
  # (Required) Which load balancer to use "F5BigIP" "Seesaw" or
"ManualLB". Uncomment
  # the corresponding field below to provide the detailed spec
  kind: Seesaw
  # # (Required when using "ManualLB" kind) Specify pre-defined nodeports
  # manualLB:
  #   # NodePort for ingress service's http (only needed for user cluster)
  #   ingressHTTPNodePort: 0
  #   # NodePort for ingress service's https (only needed for user
cluster)
  #   ingressHTTPSNodePort: 0
  #   # NodePort for control plane service
  #   controlPlaneNodePort: 30968
  #   # NodePort for addon service (only needed for admin cluster)
  #   addonsNodePort: 31405
  # # (Required when using "F5BigIP" kind) Specify the already-existing
partition and
  # # credentials
  # f5BigIP:
  #   address:
  #   credentials:
  #     username:
  #     password:
  #   partition:
  #   # # (Optional) Specify a pool name if using SNAT
  #   # snatPoolName: ""
  # (Required when using "Seesaw" kind) Specify the Seesaw configs
  seesaw:
  # (Required) The absolute or relative path to the yaml file to use for
IP allocation
  #  for LB VMs. Must contain one or two IPs.
  ipBlockFilePath: "admin-seesaw-block.yaml"
  #   (Required) The Virtual Router IDentifier of VRRP for the Seesaw
group. Must
```

```
  #   be between 1-255 and unique in a VLAN.
    vrid: 100
  #   (Required) The IP announced by the master of Seesaw group
    masterIP: "10.61.181.236"
  #   (Required) The number CPUs per machine
    cpus: 1
  #   (Required) Memory size in MB per machine
    memoryMB: 2048
  #   (Optional) Network that the LB interface of Seesaw runs in (default:
cluster
  #   network)
    vCenter:
  #   vSphere network name
      networkName: VM_Network
  #   (Optional) Run two LB VMs to achieve high availability (default:
false)
    enableHA: false
```

Der Seesaw-Load-Balancer hat ebenfalls eine separate statische `seesaw-block.yaml` Datei, die Sie für jede Cluster-Implementierung bereitstellen müssen. Diese Datei muss sich im selben Verzeichnis im Verhältnis zum befinden `cluster.yaml` Die Bereitstellungsdatei oder der vollständige Pfad müssen im Abschnitt oben angegeben werden.

Eine Auswahl der `admin-seesaw-block.yaml` Die Datei sieht wie das folgende Skript aus:

```
blocks:
  - netmask: "255.255.255.0"
    gateway: "10.63.172.1"
    ips:
    - ip: "10.63.172.152"
      hostname: "admin-seesaw-vm"
```

> Diese Datei stellt das Gateway und die Netmask für das Netzwerk bereit, das der Load Balancer für das zugrunde liegende Cluster bereitstellt, sowie die Management-IP und den Hostnamen für die virtuelle Maschine, die zur Ausführung des Load Balancer bereitgestellt wird.