VMware Photon Controller Quick Start Guide

Contents

1 Introduction

This guide explains how to install VMware Photon Controller for demonstration or trial purposes. As a quick start guide, it focuses on a minimal configuration to set up Photon Controller 1.1.1 with authentication in a controlled environment.

Photon Controller forms part of VMware Photon Platform, a highly scalable multitenant control plane for cloud-native applications. Photon Platform includes VMware ESXi, Photon Controller, VMware Lightwave security services, VMware NSX-T, and VMware vSAN.

Photon Controller furnishes an API, a CLI, and a UI to manage infrastructure as a service. You can create virtual machines and Kubernetes clusters to securely run cloud-native applications and containerized workloads at scale.

1.1 Version

This guide covers Photon Controller version 1.1.1. For earlier versions, see Photon Platform Guides. To read the release notes, see Release Notes.

1.2 Overview

Photon Controller runs on ESXi and virtual machines in ESXi. You install Photon Controller by first downloading the Photon Controller installer—an OVA that creates a VM to which you connect with SSH to deploy the system's infrastructure from a YAML configuration file.

The infrastructure of Photon Controller contains two main components:

- A management ESXi host composed of one or more virtual machines running on ESXi. The management plane coordinates workloads and allocates resources.
- A cloud host that resides on an ESXi host to run your users' VMs.

This guide installs Photon Controller on a single ESXi machine that holds the management plane, the cloud host, the load balancer, and the Lightwave security service. For a production system, you would deploy the management plane as a cluster of 3 VMs across multiple ESXi hosts. After you install the system, you can use the management plane to create tenants, resource tickets, and projects.

1.3 Lightwave Authentication

Photon Controller integrates with Lightwave to help secure Photon Platform. An open source project published by VMware on GitHub, Lightwave furnishes a directory service, a certificate authority, a certificate store, and an authentication service. Lightwave authenticates users and groups with its directory service.

The Photon Controller installation OVA installs Lightwave when it installs Photon Controller. Lightwave includes a DNS server that the Photon Controller management plane, cloud host, and other components use.

1.4 Assumptions

This guide assumes that an ESXi host is in place with the following attributes. If you do not have a computer running the ESXi operating system, you can obtain ESXi at the VMware vSphere Hypervisor 6.0 Download Center. For help installing it, see the instructions at the download center and in the VMware vSphere 6 Documentation. The ESXi host can be either the licensed or the free version.

- It is running VMware ESXi 6.0.0 Patch 201611001 (ESXi600-201611001), which you can find by searching for patches for ESXi 6.0.0 on the My VMware Product Patches web site at https://my.vmware.com/group/vmware/patch. The patch's build number is 4600944.
- It contains no existing VMs or workloads and has at least 4 CPU cores and 8 GB of RAM.
- It is assigned a static IP address.
- It contains a datastore with read-write access.
- It is not managed by vCenter.

This guide also assumes that you have root access to the ESXi host, know how to manage it with the vSphere Web Client, and understand basic networking in a virtualized environment. The vSphere Web Client is also known as the VMware ESXi Host Client. Only minimal instructions are provided for using ESXi and its web client; if you need help, see the VMware documentation for ESXi.

If you plan to install Photon Controller with NSX-T, you must install NSX-T before installing Photon Controller; see Setting UP NSX.

1.5 Requirements

- Photon Controller version 1.1.1.
- At least three static IP addresses. One static IP address is required for the VM running the Photon Controller management node; a second static IP address is required for the VM running the Lightwave security service; and a third static IP address is required for the Photon load balancer.

After you install Photon Platform, you will need a workstation that can connect to a virtual machine on your ESXi host to run commands with the Photon Controller command-line interface (CLI). This guide uses a Linux workstation running Ubuntu 14.04 as an example. You can also install the Photon Controller CLI on a Microsoft Windows or Mac workstation.

2 Installing the Photon Controller Installation OVA

Download the installer for Photon Controller 1.1.1—`installer-ova-nv-1.1.1-dfea3bb.ova`—from the following URL and then deploy it by using the vSphere Web Client:

`https://github.com/vmware/photon-controller/releases`

After you download it, quickly check its checksum to make sure the entire file downloaded correctly; the checksum resides at https://github.com/vmware/photon-controller/wiki/Download.

To deploy the OVA by using the vSphere Web Client, under `Navigator`, right-click `Host`, and then click `Create\Register VM`. Select `Deploy a virtual machine from an OVF or OVA file`, click `Next`, enter a name for the VM, such as `pc-installer`, and then click in the blue box to select the OVA from the directory that you downloaded it to.

Click `Next` and in the `Select storage` dialog, select a datastore; the examples in this guide assume that the datastore is named `datastore1`.

Click `Next` and in the `Deployment options` dialog, for `Network mappings`, use the default setting of `NAT VM Network`.

Move through the remaining dialog boxes by clicking `Next` to accept the default settings, and then click `Finish`. On the `Additional Settings` page, under `Options`, you can leave the fields empty.

When it finishes deploying, make sure it the power is on and the VM is running. Note its IP address. In a later step, you will connect to the VM by SSH to install the Photon Controller management VM, the Lightwave security service, and other components.

3 Preparing ESXi for Photon Controller

You must prepare ESXi for Photon Controller before you can proceed with the installation.

- Make sure that the default VLAN in ESXi named `VM Network` has available to it at least 3 unused IP addresses that you can assign as static IP addresses. The static IP addresses are are for the VM that will act as the Photon Controller management node, the VM that will run the Lightwave security service, and the VM that will act as the load balancer.
- Make sure that the pool of IP addresses available to `VM Network` is large enough to support provisioning several VMs later for working with Photon Platform.
- Set up an NTP source. For instructions, see the VMware vSphere documentation.
- Make sure that there are no more than two DNS entries; if there are three DNS entries, delete one of them by running the following commands with the ESXi command-line interface: First, list the DNS entries: `esxcli network ip dns server list`. Second, remove one of them: `esxcli network ip dns server remove --server <IP-address>`.
- Turn on SSH: Connect to the ESXi host by using the vSphere Web Client. Under `Navigator`, right-click `Host`, click `Services`, and then click `Enable Secure Shell (SSH)`.

4 Preparing a YAML Configuration File

The crux of the installation revolves around understanding the YAML installation template and configuring it with the right values for your deployment.

The YAML file is, in effect, a manifest for the installation: The installer uses the values in the YAML file to identify the correct networking settings, locate the datastore, and set up the management node and cloud host as well as the Lightwave security service.

Understanding each field in the YAML template will help expedite the installation. This section describes the YAML template and provides an example of a completed YAML configuration file.

4.1 YAML Rules

Indentation–defined as zero or more space characters at the start of a line–determines the structure of a block of YAML code. You must indent each line further than its parent, and all sibling nodes must adhere to the exact same level of indentation.

Do not use tabs or tab characters to indent lines in your YAML file. Tabs and improper indentation are the most likely causes of superficial YAML errors when the installer processes a YAML configuration file.

For example, if you copy one of the example YAML code blocks in this document and paste it into a new file, it might throw errors when the installer processes it. Make sure that the indentation is correct and that the file contains no tabs. See the YAML specification.

You can validate your YAML configuration file at YAML Lint: http://www.yamllint.com/.

4.2 The Anatomy of a Configuration File

The template contains four main sections:

1. The `compute` section lists networking information for all ESXi hosts that are to be included in the deployment of Photon Platform.
2. The `lightwave` section specifies the target ESXi host and the configuration for the Lightwave security service. It also includes the credentials for initially logging on to Photon Platform as an administrator.

3. The `photon` section specifies the ESXi machines that will host the image stores, cloud hosts, and management VMs for Photon Controller.
4. The `loadBalancer` section sets the configuration for the loadbalancer that Photon Controller uses for incoming traffic.

Here is a minimal template with descriptions of each key-value pair. The values of key-value pairs are set in double quotation marks.

```
compute:
  hypervisors:
    esxi-1:
      hostname: The host name of the target ESXi hypervisor that you want to include
                in the Photon Controller cluster.
      ipaddress: The IP address of the target ESXi hypervisor.
      dns: The static IP address that you are assigning to the Lightwave VM in the
           lightwave section of the YAML configuration.
      credential:
        username: The name of the root account on the target ESXi hypervisor;
                  for example, "root"
        password: The password for the root account of the target ESXi hypervisor.
lightwave:
  domain: The domain name that you want to set for the Lightwave domain;
          example, "example.com"
  credential:
    username: The default user name that you want set as the administrator of the
              Lightwave service. It must be all lowercase letters;
              example, "administrator"
    password: The default password that you want to set for the user name.
  controllers:
    lightwave-1:
      site: Insignificant designation of your site's location;
            this value is not acted on by the installer; example: "nydc"
      appliance:
        hostref: The name of the ESXi hypervisor on which you want Lightwave
                 to be installed.
        datastore: "datastore1"
        credential:
          username: The name of the root account on the target ESXi hypervisor.
          password: The password for the root account.
        network-config:
          network: "NAT=VM Network"
          type: "static"
          hostname: The fully qualified domain name that you want to set as
                    the hostname of the VM on which Lightwave resides.
          ipaddress: The static IP address that you want to assign
                     to the VM running Lightwave.
          dns: The IP address of your internal corporate DNS server.
          ntp: The IP address of the NTP server that the Lightwave VM will use.
          netmask: The netmask that the Lightwave VM will use.
          gateway: The gateway IP address that you want the Lightwave VM to use.
photon:
  imagestore:
    img-store-1:
      hostref: The target ESXi hypervisor on which you want Photon Controller image
               datastore to reside.
```

```
              The hypervisor must be included in the compute section's
              list of hypervisors.
      datastore: The datastore on an ESXi hypervisor for images for VMs and
                 Kubernetes clusters, etc. The datastore must be unique; that is,
                 the name of each datastore must be unique among the ESXi hosts
                 in the deployment. If there are, for instance, two ESXi hosts
                 in the deployment, and the first ESXi host's datastore is named
                 datastore1, then the second ESXi host's datastore must have a
                 different name, such as datastore2.
      enableimagestoreforvms: Allows the datastore that is set as the image
                              datastore to be used by VMs. This value must be
                              set to true if there is only one ESXi host in the
                              deployment.
  cloud:
    hostref1: "esxi-17"
  syslog:
    ipaddress: The IP address of the syslog server to which you want to send Photon
               Controller log files. The syslog entry and its ipaddress key-value pair
               are optional. You can remove both lines.
  controllers:
    pc-1:
      appliance:
        hostref: The target ESXi hypervisor on which you want the Photon Controller
                 management VM to reside. The hypervisor must be included in the
                 compute section's list of hypervisors.
        datastore: The datastore that this VM will use; it must be the name of the
                   datastore on the ESXi host referenced by the value of the
                   hostref in the previous line.
        credential:
          username: The name of the root account of the target hypervisor.
          password: The password for the root account.
        network-config:
          network: "NAT=VM Network"
          type: "static"
          hostname: The fully qualified domain name that you want to set as
                    the hostname of the Photon Controller management VM.
          ipaddress: The static IP address you want to assign to the management VM.
          netmask: The netmask that the  management VM will use.
          dns: The IP address of the DNS server that the management VM will use.
          ntp: The IP address of the NTP server that the management VM will use.
          gateway: The gateway IP address that you want the management VM to use.
loadBalancer:
  load-balancer-1:
    appliance:
      hostref: The name of the ESXi hypervisor on which you want the load
               balancer to reside. The hypervisor must be included in the
               compute section's list of hypervisors.
      datastore: "datastore1"
      credential:
        username: "root"
        password: "secret$11"
      network-config:
        network: "NAT=VM Network"
        type: "static"
```

```
        hostname: The fully qualified domain name that you want to assign as the
                  host name of the load balancer; example: "lb-1.eg.example.com"
        ipaddress: The static IP address that you want to assign to the load balancer.
        netmask: The netmask that the load balancer will use.
        dns: The IP address of the DNS server that the load balancer will use.
        ntp: The IP address of the NTP server that the load balancer will use.
        gateway: The gateway IP address that you want the load balancer to use.
```

4.3 DNS

The value that you must set for the `dns` entry for each section except `lightwave` is counterintuitive: Because Photon Controller uses the DNS server that is included with Lightwave, the DNS entry for each section except `lightwave` must be the static IP address that you are assigning to the Lightwave VM in the `lightwave` section of the YAML configuration.

Here is an example that shows the value of the Lightwave VM's `dns` key and the VM's `ipaddress` key. For the `lightwave` section only, the `dns` key is to be set to the IP address of your internal corporate network's DNS server. The value of the `dns` key for all other sections is to be set to the same value as IP address of the Lightwave VM:

```
lightwave-1:
...
    network-config:
      network: "NAT=VM Network"
      type: "static"
      hostname: "lightwave-1.example.com"
      ipaddress: "198.51.100.212"
      dns: "192.0.2.1"
```

In the example configuration file that follows, note that the `dns` key *for each section except Lightwave* is set to the same static IP address—the value of the `ipaddress` key in the `lightwave` section.

4.4 Example Basic Configuration File

Here is an example configuration file with the minimum information necessary for a basic deployment on a single ESXi hypervisor.

There is also a full example YAML configuration file on the installer VM. The password for the installer VM is `changeme`:

```
ssh root@198.51.100.212
cd /opt/vmware/photon/controller/share/config/
ls
log4j.properties  pc-config.yaml
```

```
compute:
  hypervisors:
    esxi-1:
      hostname: "esxi-1"
      ipaddress: "198.51.100.44"
      dns: "198.51.100.212"
      credential:
        username: "root"
        password: "secret$1"
lightwave:
```

```
  domain: "example.com"
  credential:
    username: "administrator"
    password: "Secret1!"
  controllers:
    lightwave-1:
      site: "wdc"
      appliance:
        hostref: "esxi-1"
        datastore: "datastore1"
        credential:
          username: "root"
          password: "secret$11"
        network-config:
          network: "NAT=VM Network"
          type: "static"
          hostname: "lightwave-1.example.com"
          ipaddress: "198.51.100.212"
          dns: "192.0.2.1"
          ntp: "198.51.100.1"
          netmask: "255.255.0.0"
          gateway: "198.51.100.253"
photon:
  imagestore:
    img-store-1:
      datastore: "datastore1"
      enableimagestoreforvms: "true"
  cloud:
    hostref1: "esxi-1"
  controllers:
    pc-1:
      appliance:
        hostref: "esxi-1"
        datastore: "datastore1"
        credential:
          username: "root"
          password: "secret$11"
        network-config:
          network: "NAT=VM Network"
          type: "static"
          hostname: "pc-1.example.com"
          ipaddress: "198.51.100.208"
          netmask: "255.255.0.0"
          dns: "198.51.100.212"
          ntp: "198.51.100.1"
          gateway: "198.51.100.253"
loadBalancer:
  load-balancer-1:
    appliance:
      hostref: "esxi-1"
      datastore: "datastore1"
      credential:
        username: "root"
        password: "secret$11"
```

```
network-config:
  network: "NAT=VM Network"
  type: "static"
  hostname: "lb-1.example.com"
  ipaddress: "198.51.100.207"
  netmask: "255.255.0.0"
  dns: "198.51.100.212"
  ntp: "198.51.100.1"
  gateway: "198.51.100.253"
```

Note: If NSX-T is installed and you want to include the NSX-T network information in the YAML configuration file, see Integrating with NSX.

For your first test deployment, you can either use the example YAML configuration file on the installer VM or copy the template above, paste it into a file, remove the tabs, and save the file as `config1.yaml`.

The full example YAML configuration file resides on the installer VM as `pc-config.yaml`. The password for the installer VM is `changeme`:

```
ssh root@198.51.100.212
cd /opt/vmware/photon/controller/share/config/
ls
log4j.properties  pc-config.yaml
```

You can obtain most of the information to fill out the template by connecting to your ESXi host with the vSphere Web Client. Replace the IP addresses and the user names and password with those from your ESXi host and its network. The IP addresses for the Photon management VM and the Lightwave VM should be static IP addresses that are available for use by the ESXi host. You might have to obtain static IP addresses from your network administrator.

5 Deploying Photon Platform

After you modify the YAML configuration template to match your environment, transfer the file to the Photon installer VM by using scp or sftp. The password for the installer VM is `changeme`. Example:

```
scp config1.yaml root@198.51.100.212:/tmp/config1.yaml
Password: changeme
config1.yaml                                  100% 1839     1.8KB/s   00:00
```

Next, connect to the installer VM by using SSH; example:

```
ssh root@198.51.100.212
```

The installer VM includes a command-line utility that sets up Photon Platform. Take a moment to view its help by running the following command:

```
/opt/vmware/photon/controller/bin/photon-setup
```

Here's what the output looks like:

```
Usage: photon-setup <component> <command> {arguments}
Component:
    platform:      Photon Platform including multiple components
    controller:    Photon Controller
    lightwave:     Lightwave
    controller:    Photon Controller Cluster
    agent:         Photon Controller Agent
    vsan:          Photon VSAN Manager
```

```
    dhcp:          DHCP Instance
    load-balancer: Load balancer
    help:          Help
Command:
    install:   Install components
    help:      Help about component
Run 'photon-setup <component> help' to find commands per component
```

To install the platform from your YAML configuration file, you will use the `photon-setup platform` command. Here's what its help output looks like:

```
/opt/vmware/photon/controller/bin/photon-setup platform help
Usage: photon-setup platform <command> <arguments>
Command:
    install
    help
platform install:
    -config <path to config file>
```

Now run the following command to install the Photon Platform components specified in the YAML file:

```
/opt/vmware/photon/controller/bin/photon-setup platform install -config /tmp/config1.yaml
```

The installation takes a few minutes. If the deployment is unsuccessful, see the section on troubleshooting.

If the deployment is successful, leave the Photon Platform installer VM in place; do not delete it. You are might need it later to add additional ESXi hosts to the cluster.

6 Installing the Photon Controller CLI on a Linux Workstation

Download the file named `photon-linux64` from the following URL and install it on a Linux workstation with which you can connect to the Photon Controller management VM that you installed on an ESXi host. Make sure to download the version of the CLI tool that coincides with the version of Photon Controller you are installing.

```
https://github.com/vmware/photon-controller/releases
```

To install it on Ubuntu, for example, change its mode bits so that it is executable and then move it to `/usr/local/bin/photon`. Here's an example:

```
cd ~/Downloads/
chmod +x photon-linux64
sudo mv photon-linux64 /usr/local/bin/photon
```

You can also install the Photon Controller CLI on a Microsoft Windows or Mac workstation.

7 Connecting to the Load Balancer

To manage Photon Controller, you connect to the load balancer from your workstation by using either the web interface or the command-line interface.

7.1 Using the CLI

After the installer deploys Photon Controller, you can connect to the load balancer to create tenants, resource tickets, and projects. But first, you will need the load balancer's IP address from your YAML file.

You connect to Port 443 of the IP address of the load balancer by running the following `photon target set` command with the `-c` option:

```
photon target set -c https://<ip-of-load-balancer>:443
```

After you set the target, you can log in by using the credentials that you set in the `lightwave` section of the YAML configuration file; in the example, it looked like this:

```
lightwave:
  domain: "example.com"
  credential:
    username: "administrator"
    password: "Secret1!"
```

Here's the syntax of the command to log in:

```
photon target login --username <username>@<lightwave-domain> --password 'Your$ecret1!'
```

Here is an example. In the sample YAML file, the `username` of the Lightwave `credential` is set to `administrator` and the domain is set to `example.com`. The `photon target login` uses the Lightwave domain and credentials to authenticate the user with the Lightwave security service.

```
photon target login --username administrator@example.com --password 'Secret1!'
```

Now that you are logged in, you can check the status of Photon Controller:

```
photon system status
Overall status: READY
Component          Status
PHOTON_CONTROLLER  READY
```

As the status says, you're now ready to work with the system. You can get more information about the deployment by running the following command:

```
photon deployment show
Deployment ID: default
  State:                        READY
  Image Datastores:             [datastore1]
  Use image datastore for vms: true
  Syslog Endpoint:              -
  Ntp Endpoint:                 -
  LoadBalancer:
    Enabled:                    false
  Auth:
    Endpoint:                   198.51.100.212
    Tenant:                     example.com
    Port:                       443
    Securitygroups:             [example.com\Administrators]
  Stats:
    Enabled:               false
  Migration status:
    Completed data migration cycles:          0
    Current data migration cycles progress:   0 / 0
    VIB upload progress:                      0 / 0
  Cluster Configurations:
    No cluster is supported
  Job  VM IP(s)  Ports
  VM IP  Host IP  VM ID  VM Name
```

To start working with Photon Platform, see the Command-Line Cheat Sheet and the other documentation on the Photon Controller GitHub Wiki. To create a tenant, for instance, see Working with Tenants.

7.2 Using the Web Interface

You can log in to the web interface to view a range of information and to create tenants, allocate resources, establish projects, and spin up clusters. To log in the web interface, connect to the load balancer over HTTPS by using its IP address plus Port 4343:

```
https://<ip-address-of-load-balancer>:4343
```

The load balancer redirects your browser to the IP address of the Lightwave security service. Log in by using the credentials that you set in the `lightwave` section of the YAML configuration file; for example:

```
adminsitrator@example.com
Secret1!
```

8 Creating a Kubernetes Cluster

To see the power of Photon Platform, you can create a Kubernetes cluster. For instructions, see Creating a Kubernetes Cluster on the Photon Controller GitHub wiki.

9 Troubleshooting

You can troubleshoot by looking at the installer's logs. The most likely cause of a failure is that static IP address that you tried to assign to a VM in the Photon Controller management plane is in use, unavailable, or unreachable. Another possible cause is that the DNS entries are incorrect in the YAML configuration file.

9.1 Log Files for the Installer

The log files for the deployment reside in the following location on the installer VM. The password for the root account is `changeme`.

- /var/log/photon-installer.log

The log files for the Photon Controller agent, which is installed on each ESXi host, reside in the following directory on each target ESXi host:

- /scratch/log/photon-controller-agent.log

The log files on the Photon Controller management VMs might contain useful troubleshooting information about API calls that fail, such as the call to add an ESXi host to the cluster. The management VM's log resides at this location:

- /var/log/esxcloud/photon-controller.log

You can access the log file through the VM's console in the vSphere Web Client. To connect to the management VM with SSH to view the log, you must first connect to the console and change the SSH configuration to permit root login; see Permitting Root Login with SSH.

9.2 Installing in Memory-Constrained Environments

If you are trying to install Photon Platform on ESXi hosts with memory constraints, you can specify the amount of RAM and CPUs that the VM will use on the target ESXi host by using the `memoryMB` key and the `cpus` key. Setting the values for these keys can help overcome out-of-memory or not-enough-memory errors.

However, the values must be, at a minimum, 2048 megabytes of memory and 2 CPU cores. Here is an example that uses the minimum settings for memory and CPUs for a Lightwave VM:

```
controllers:
  lightwave-1:
    site: "New York"
    appliance:
      hostref: "esxi-1"
      datastore: "datastore1"
      memoryMb: 2048
      cpus: 2
      credential:
        username: "root"
        password: "Your$ecret1"
      network-config:
        type: "static"
        hostname: "lightwave-1.example.com"
        ipaddress: "198.51.100.12"
        network: "NAT=VM Network"
        dns: "198.51.100.12,198.51.100.13"
        ntp: "192.0.2.1"
        netmask: "255.255.252.0"
        gateway: "198.51.100.253"
```

9.3 Retrying the Installation

If Photon Controller fails to install successfully, modify the YAML configuration file and try again by rerunning the installation command with the corrected YAML file.

9.4 Lightwave Authentication and NTP

Because Lightwave authenticates users and groups by using the Kerberos security protocol, the time on the VM running Lightwave must be synchronized with the time on VMs that are authenticating with Lightwave.

More specifically, the clock of the client must be within the Lightwave key distribution center's maximum clock skew, which is 300 seconds, or 5 minutes, by default. Lightwave discards authentication requests outside the maximum clock skew to help prevent replay attacks. See MIT Kerberos Clock Skew.

Implementing an NTP server for the ESXi host synchronizes clocks across virtual machines to avoid Kerberos clock-skew errors.

10 Deploying a Production-Level Platform

Setting up Photon Controller by following this quick start guide prepares you to deploy a production-ready system that works within the context of your unique virtualized environment. The key is to take the knowledge that you gained from a minimal installation and to apply it to modifying the YAML configuration file for a production-level deployment.

A production-level deployment should contain at least three VMs dedicated to the Photon Controller management plane—and all the management VMs should be assigned static IP addresses. The management VMs should also reside on different ESXi hypervisors to distribute the load and to ensure high availability.

In addition, a production-level deployment can contain more ESXi hypervisors to add compute and storage resources to the cluster.

A production-level deployment of Photon Platform should include VMware NSX-T and VMware vSAN. NSX-T provides software-defined virtualized networking, and vSAN furnishes a virtual storage area network. Both are addressed in later sections.

Here is a YAML configuration file that includes a number of ESXi hosts and three Photon Controller management plane VMs. Notice how the three management VMs—`pc1`, `pc2`, and `pc3`—are each installed on a different ESXi hypervisor.

```
compute:
  hypervisors:
    esxi-24:
      hostname: "esxi-24"
      ipaddress: "198.51.100.48"
      dns: "198.51.33.10"
      credential:
        username: "root"
        password: "secret$1"
    esxi-17:
      hostname: "esxi-17"
      ipaddress: "198.51.100.41"
      dns: "198.51.33.10"
      credential:
        username: "root"
        password: "secret$1"
    esxi-18:
      hostname: "esxi-18"
      ipaddress: "198.51.100.42"
      dns: "198.51.33.10"
      credential:
        username: "root"
        password: "secret$1"
    esxi-19:
      hostname: "esxi-19"
      ipaddress: "198.51.100.43"
      dns: "198.51.33.10"
      credential:
        username: "root"
        password: "secret$1"
    esxi-20:
      hostname: "esxi-20"
      ipaddress: "198.51.100.44"
      dns: "198.51.33.10"
      credential:
        username: "root"
        password: "secret$1"
    esxi-21:
      hostname: "esxi-21"
      ipaddress: "198.51.100.45"
      dns: "198.51.33.10"
```

```
      credential:
        username: "root"
        password: "secret$1"
    esxi-22:
      hostname: "esxi-22"
      ipaddress: "198.51.100.46"
      dns: "198.51.33.10"
      credential:
        username: "root"
        password: "secret$1"
lightwave:
  domain: "example.com"
  credential:
    username: "administrator"
    password: "VMware123$"
  controllers:
    lightwave-1:
      site: "wdc"
      appliance:
        hostref: "esxi-24"
        datastore: "datastore1"
        credential:
          username: "root"
          password: "secret$11"
        network-config:
          network: "NAT=VM Network"
          type: "static"
          hostname: "lightwave-1.example.com"
          ipaddress: "198.51.33.10"
          dns: "192.0.2.1"
          ntp: "198.51.100.1"
          netmask: "255.255.240.0"
          gateway: "198.51.100.253"
photon:
  imagestore:
    img-store-1:
      hostref: "esxi-17"
      datastore: "cloud1-ds-17_20,cloud1-ds-21_24"
  cloud:
    hostref1: "esxi-17"
    hostref2: "esxi-18"
    hostref3: "esxi-19"
    hostref4: "esxi-20"
    hostref5: "esxi-21"
    hostref6: "esxi-22"
  controllers:
    pc-1:
      appliance:
        hostref: "esxi-17"
        datastore: "cloud1-ds-17_20"
        credential:
          username: "root"
          password: "secret$11"
        network-config:
```

```
          network: "NAT=VM Network"
          type: "static"
          hostname: "pc-1.example.com"
          ipaddress: "198.51.33.20"
          netmask: "255.255.240.0"
          dns: "198.51.33.10"
          ntp: "198.51.100.1"
          gateway: "198.51.100.253"
    pc-2:
      appliance:
        hostref: "esxi-18"
        datastore: "cloud1-ds-17_20"
        credential:
          username: "root"
          password: "secret$11"
        network-config:
          network: "NAT=VM Network"
          type: "static"
          hostname: "pc-2.example.com"
          ipaddress: "198.51.33.21"
          netmask: "255.255.240.0"
          dns: "198.51.33.10"
          ntp: "198.51.100.1"
          gateway: "198.51.100.253"
    pc-3:
      appliance:
        hostref: "esxi-21"
        datastore: "cloud1-ds-21_24"
        credential:
          username: "root"
          password: "secret$11"
        network-config:
          network: "NAT=VM Network"
          type: "static"
          hostname: "pc-3.example.com"
          ipaddress: "198.51.33.22"
          netmask: "255.255.240.0"
          dns: "198.51.33.10"
          ntp: "198.51.100.1"
          gateway: "198.51.100.253"
loadBalancer:
  load-balancer-1:
    appliance:
      hostref: "esxi-17"
      datastore: "datastore1"
      credential:
        username: "root"
        password: "secret$11"
      network-config:
        network: "NAT=VM Network"
        type: "static"
        hostname: "lb-1.example.com"
        ipaddress: "198.51.33.19"
        netmask: "255.255.240.0"
```

```
        dns: "198.51.33.10"
        ntp: "198.51.100.1"
        gateway: "198.51.100.253"
```

10.1 Integrating with NSX

Here's an example of the YAML code block for NSX. The value for the `ipaddress` key in the `nsxconfig` section is the IP address of your NSX Network Manager.

```
nsxconfig:
  ipaddress: "203.0.113.220"
  credential:
    username: "admin"
    password: "secret$1"
  privateDHCPIp: "192.168.2.1"
  publicDHCPIp: "203.0.113.223"
  privateIpRootCidr: "192.168.1.0/24"
  floatingIpRootRange: "203.0.113.160-203.0.113.170"
  t0RouterId: "d3b1a8gr-6c58-2062-2562-2drc8977e414"
  edgeClusterId: "55338b48-4r72-38b0-8d4r-65b29084c99a"
  overlayTransportZoneId: "dg821bea-c5r3-34b2-a32g-b02d44726d24"
  tunnelIpPoolId: "b4h8c34d-7714-507c-78g2-ef93b6b2db2a"
  hostUplinkPnic: "vmnic4"
```

10.2 Integrating with vSAN

Adding VMware vSAN to Photon Platform creates a powerful platform for cloud-native applications. vSAN establishes a software-defined storage cluster that transforms the local physical resources of ESXi hosts into a virtual pool of storage for Photon Controller.

After you install Photon Platform, you can add a virtual storage area network by deploying vSAN. For installation instructions, see Deploying vSAN for Photon Platform.

11 Creating Accounts in Lightwave

After you deploy Photon Platform, you can log in to the Lightwave service with SSH and create additional users and groups.

Before you can log in with SSH, however, you must access the VM through its console in ESXi and modify the VM's SSH configuration file to permit root login.

To permit root login over SSH, open `/etc/ssh/sshd_config` with the vim text editor and set all three instances of `PermitRootLogin` to `yes`. After you modify and save the SSH daemon's configuration file, you must restart the sshd daemon for the changes to take effect:

```
systemctl restart sshd
```

Then connect to the Lightwave VM with SSH using the root account and password that you set in the YAML file for the Lightwave VM; example:

```
 ssh root@<IPaddressOfLightwaveVM>
```

After you log in to the Lightwave VM with SSH, change directories:

```
cd /opt/vmware/bin
```

Using the Lightwave adminstrator password that you defined in the YAML configuration file, run the following Lightwave directory commands to create a group, create a user, and add the user to the group.

```
./dir-cli ssogroup create --name "photonControllerAdmins"
./dir-cli user create --account pc-admin --user-password 'Your$ecret1!'
                      --first-name pc --last-name admin
./dir-cli group modify --name photonControllerAdmins --add pc-admin
```

When you are done, type `exit` again to leave the SSH session.

11.1 Connecting to the Lightwave Web Interface

To connect to the Lightwave web interface, you must first add a Lightwave entry to the `/etc/hosts` file of your Linux workstation so that your browser can use the hostname that you set for the Lightwave VM instead of its IP address.

Here's an example of how to add a Lightwave entry to `/etc/hosts`:

```
##
# Host Database
#
# localhost is used to configure the loopback interface
# when the system is booting.  Do not change this entry.
##
127.0.0.1   localhost
255.255.255.255 broadcasthost
::1             localhost
198.51.33.10    lightwave-1.example.com
```

You can now connect to the Lightwave VM by connecting to its full hostname over HTTPS; example:

```
https://lightwave-1.example.com
```

11.2 Using Lightwave Groups in Photon Controller

Photon Controller uses Lightwave groups as generic collections of user accounts. The groups are created by a Lightwave administrator, not the Photon Controller administrator. In Lightwave, the groups contain no properties that distinguish system administrators from tenant administrators or project users.

To control access by enforcing the distinctions among groups in Photon Controller, you use one of the following commands to set a group from Lightwave as the security group for a deployment, tenant, or project.

`photon deployment set-security-groups`

Members of the security group for a deployment are system administrators for Photon Controller.

`photon tenant set_security_groups`

Members of the security groups for a tenant are tenant administrators.

`photon project set_security_groups`

Members of the security groups for a project are project users. They receive project-specific rights to work with and modify projects.

Important: The command to set security groups *overrides* existing groups. The groups that you include in the `photon project set_security_groups` command, for example, replace all the existing security groups—even ones that you have already defined. The only exception is inherited groups, which are retained

by default. When you create a project, the project inherits the security groups from the tenant that governs the project, including whatever groups the tenant inherited.

The next section presents examples of how to set the security groups for a deployment, a tenant, and a project. Remember to be careful when you run the commands to set a security group so that you don't lock yourself out of the system.

11.3 Setting Security Groups for Administrators, Tenants, and Project Users

To set a group named `dev-project-users` as the security group for an existing project named `dev-project`, connect to Photon Controller by using the Photon command-line utility on your workstation and then run the following command:

```
photon project set_security_groups dev-project -t demo -g photon\\dev-project-users
```

As the example above illustrates, you specify group names in the following format: `<securitydomain>\\<NameOfGroup>`. Here's an example: `photon\\Administrators`. The security domain must be made up of all lowercase letters.

Here's an example of how to set a group as a tenant administrator. All the members of the group have tenant administrator rights. In the example, `plato` is the name of the tenant.

```
photon tenant set_security_groups plato photon\\tenant-admins
```

A system administrator can set a Lightwave group that contains a list of users who have rights to administer the entire deployment of Photon Controller. **Important:** The following command overrides the existing groups. Be careful running it because providing the wrong groups could remove your access:

```
photon deployment set-security-groups photon\\photonControllerAdmins
```

All the commands to set security groups can contain a comma-separated list of groups; example:

```
photon deployment set-security-groups photon\\photonControllerAdmins,
       photon\\Administrators, photon\\superUsers
```