Photon Controller Quick Start Guide

Contents

1 Introduction **2**
- 1.1 Overview . . . 2
- 1.2 Lightwave Authentication . . . 2
- 1.3 Assumptions . . . 2
- 1.4 Requirements . . . 3

2 Installing the Photon Controller Installation OVA **3**

3 Installing the Photon Controller CLI on a Linux Workstation **3**

4 Preparing ESXi for Photon Controller **4**

5 Preparing a YAML Configuration File **4**
- 5.1 The Anatomy of a Configuration File . . . 4
- 5.2 Avoiding Errors in the Configuration File . . . 5
- 5.3 Example Basic Configuration File . . . 7

6 Deploying the Basic System **7**

7 Checking the System's Status **7**

8 Redeploying with Lightwave Authentication **8**
- 8.1 Destroying the Previous Deployment . . . 8
- 8.2 Preparing ESXi for Authentication . . . 8
- 8.3 Adding Lightwave Authentication to the Template . . . 9
- 8.4 Example Configuration File with Authentication . . . 10
- 8.5 Building Your Configuration File and Deploying Photon Controller . . . 11

9 Creating Accounts in Lightwave **12**

10 Connecting to the Load Balancer **12**

11 Creating a Kubernetes Cluster **13**

12 Troubleshooting **13**
- 12.1 Log Files for the Installer . . . 13
- 12.2 Deploying the OVA Installer . . . 13
- 12.3 Lightwave Authentication and NTP . . . 14

1 Introduction

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

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

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 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 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 allocates resources to tenants for projects.
- A cloud host that resides on an ESXi host to run your users' VMs.

For expedience, this guide installs Photon Controller on an ESXi machine that holds the management plane and the cloud host.[1] After you install the system, you can use the management plane to create tenants, resource tickets, and projects.

To help you learn how to install Photon Controller, this quick start guide proceeds in two stages: The first stage installs a basic deployment of the system, and the second stage installs a more advanced deployment that uses Lightwave authentication.[2]

1.2 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 to ensure that only authorized users run authorized containers.

1.3 Assumptions

This guide assumes that an ESXi host is in place with the following attributes.[3] The ESXi host can be either the licensed or the free version.

- It is running VMware ESXi 6.0 Update 2, Patch 4 (U2, P4).
- It contains no VMs and has at least 4 CPU cores and 8 GB of RAM.

[1] For a production system, you would deploy the management plane as a cluster of 3 VMs.

[2] For security, you should deploy Photon Controller with authentication turned on.

[3] 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. You can also install Photon Controller on VMware Workstation or Fusion; for instructions, see the Photon Controller GitHub Wiki.

- It is assigned a static IP address.
- It contains a datastore with read-write access.
- It is not managed with vCenter.

This guide also assumes that you have root access to the ESXi host, know how to manage it with the vSphere Web Client[4], and understand basic networking in a virtualized environment. Only minimal instructions are provided for using ESXi and its web client; for more information, see the VMware documentation for ESXi.

1.4 Requirements

- Photon Controller version 1.0.
- A static IP address that you can use to provision the Photon Controller management node.
- A Linux workstation that can connect to virtual machines on your ESXi host to run commands with the Photon Controller command-line interface (CLI). This guide uses Ubuntu 14.04 as an example.[5]
- A second ESXi hypervisor with a static IP address that the installation will dedicate to the Lightwave authentication service. This second ESXi hypervisor can be embedded as a virtual machine in your primary ESXi host. You can download it for free from VMware.

2 Installing the Photon Controller Installation OVA

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

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

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 select a datastore; the examples in this guide assume that the datastore is named `datastore1`.

Move through the remaining dialog boxes by clicking `Next` to accept the default settings, and then click `Finish`.

When it finishes deploying, power on the virtual machine. In a later step, you will connect to it to create the management virtual machine and the cloud host in ESXi.

3 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 your ESXi host.

`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
```

[4]The vSphere Web Client is also known as the VMware ESXi Host Client.

[5]You can also install the Photon Controller CLI on a Microsoft Windows or Mac workstation; for instructions, see the Photon Controller GitHub Wiki.

In a later step, you connect from the Linux workstation to the installer VM through the Photon CLI tool to run installation commands.

4 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 1 unused IP address that you can assign as a static IP address. The IP address is for the VM that will act as the Photon Controller management VM.
- Make sure that the pool of IP addresses available to `VM Network` is large enough to support provisioning several VMs later.
- 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. 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)`.

5 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 VM uses the values in the YAML file to connect to the ESXi host, identify the correct networking settings, locate the datastore, and set up the management node and cloud host.

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.

5.1 The Anatomy of a Configuration File

Here is a minimal template with descriptions of each key-value pair. The template contains two main sections: `hosts` and `deployment`. The `hosts` section specifies networking information for all the computers, or "hosts," in the cluster, including the ESXi hypervisor host and the virtual machines forming the management plane. The `deployment` section specifies parameters for the setup.

```
hosts:
  - metadata:
      MANAGEMENT_DATASTORE: <the name of a datastore on an
       ESXi hypervisor that the management plane will use>
      MANAGEMENT_PORTGROUP: <the name of a network (VLAN or
       port group) on ESXi where the management VMs will reside)
      MANAGEMENT_NETWORK_NETMASK: <the netmask of the
       network on ESXi where the management VMs reside>
      MANAGEMENT_NETWORK_DNS_SERVER: <the IP address of the
       DNS server of the network on ESXi to be used by the management VMs>
      MANAGEMENT_NETWORK_GATEWAY: <the IP address of the
       gateway of the network on ESXi to be used by the management VMs>
      MANAGEMENT_VM_IPS: <the static IP address for the
```

```
      management VM that the installer will create>
    address_ranges: <the IP address of the ESXi host on
     which the management plane will be installed>
    username: <the name of a user with root access to the ESXi host>
    password: <the password for the user on the ESXi host>
    usage_tags:
      - MGMT
      - CLOUD
deployment:
  resume_system: true
  image_datastores:
    - datastore1
  use_image_datastore_for_vms: true
  loadbalancer_enabled: false
  auth_enabled: false
```

In this minimal deployment template, the `CLOUD` usage tag indicates that the ESXi host will also serve as the cloud host. As a result, there is no need to add an additional `metadata` sequence for the cloud host.

5.2 Avoiding Errors in the Configuration File

A few of the fields in the template are error prone.

The value of the `MANAGEMENT_VM_IPS` key refers to the static IP address of the VM that the Photon Controller installer will deploy for the management node. The value that you add for this key should be an unused static IP address that's available to your ESXi host and reachable from the installer VM. You might need to obtain a static IP address from your network administrator.

The value of the `address_ranges` key refers to the IP address of your ESXi host on which you are installing Photon Controller. If you install Photon Controller across a cloud of ESXi hosts, the value of `address_ranges` can be the range of static IP addresses assigned to the ESXi hosts.

The value of `MANAGEMENT_PORTGROUP` is error prone because there are several terms that, in the context of ESXi networking as viewed through the vSphere Web Client, can seemingly refer to the same thing: *network*, *port group*, and *VLAN*. The default port group on an ESXi hypervisor is named `VM Network`, which often has a VLAN ID of `0`, and `VM Network` is a suitable value for `MANAGEMENT_PORTGROUP` for a trial installation.

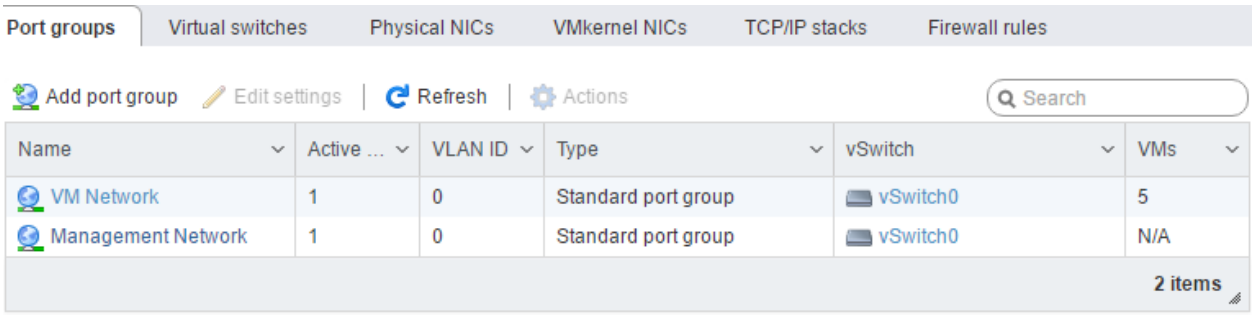

Figure 1: Port Groups in the vSphere Web Client

In this context, the term *Management Network* can refer to two entirely different networks:

1. The default ESXi management network containing the Ethernet network adapter that transmits traffic between the ESXi host and any external management software. This management network is the one shown in the image above. In the YAML template, "MANAGEMENT_NETWORK" does not refer to the ESXi Management Network.

2. The Photon Controller management plane, or "network," that you are setting up.

In the YAML template, therefore, the values for the `MANAGEMENT_NETWORK_NETMASK`, the `MANAGEMENT_NETWORK_DNS_SERVER`, and the `MANAGEMENT_NETWORK_GATEWAY` all refer to the network infrastructure that you want Photon Controller to use. To find the networking information for this infrastructure, click `Host` in the navigation pane of the vSphere Web Client. It displays a summary of its settings and IP addresses, as the following image illustrates.

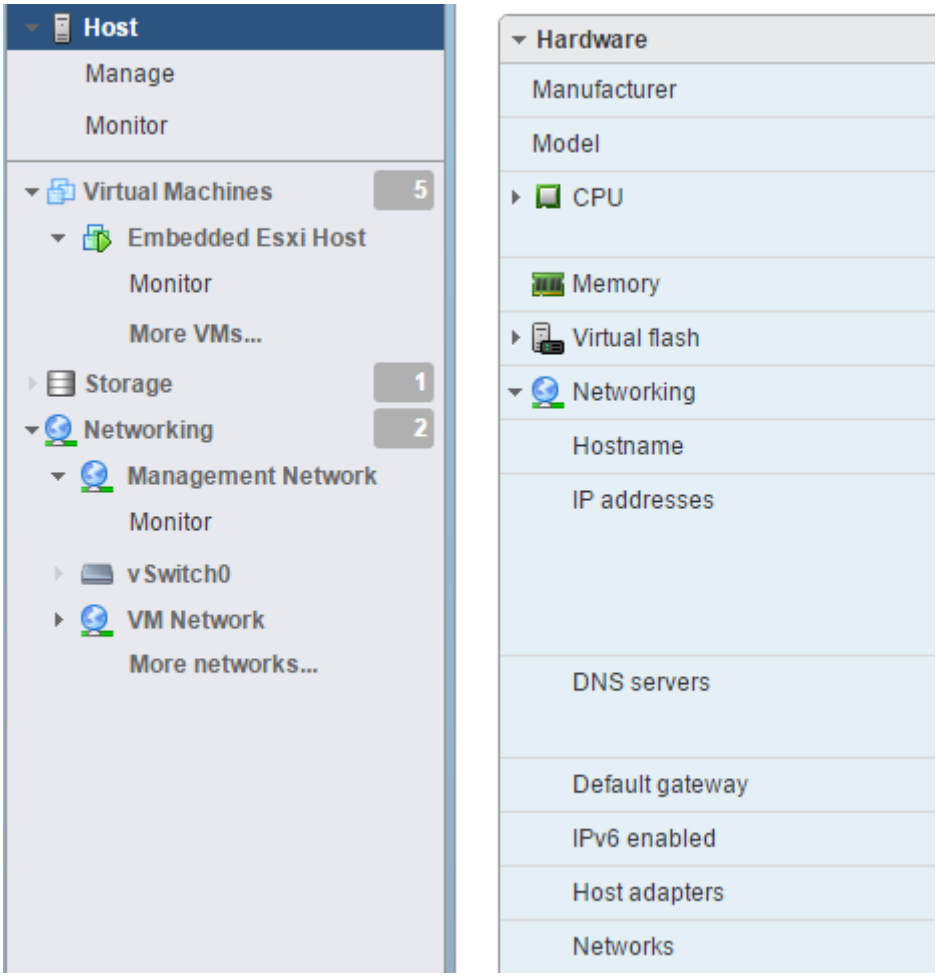

Figure 2: The ESXi Host information page in the vSphere Web Client

5.3 Example Basic Configuration File

Here is an example configuration file with the minimum information necessary for a basic deployment:

```
hosts:
  - metadata:
      MANAGEMENT_DATASTORE: datastore1
      MANAGEMENT_PORTGROUP: VM Network
      MANAGEMENT_NETWORK_NETMASK: 255.255.0.0
      MANAGEMENT_NETWORK_DNS_SERVER: 198.51.100.1
      MANAGEMENT_NETWORK_GATEWAY: 198.51.100.253
      MANAGEMENT_VM_IPS: 198.51.100.191
    address_ranges: 198.51.100.44
    username: root
    password: secret$1
    usage_tags:
      - CLOUD
      - MGMT
deployment:
  resume_system: true
  image_datastores:
    - datastore1
  use_image_datastore_for_vms: true
  loadbalancer_enabled: false
  auth_enabled: false
```

For your first test deployment, copy the template above and replace the IP addresses and the username and password with those from your ESXi host and its network. The IP address for the value of `MANAGEMENT_VM_IPS` should be a static IP address that is available for use by the ESXi host. Save the file as `config1.yml`.

You can obtain the information to fill out the template by connecting to your ESXi host with the vSphere Web Client.

6 Deploying the Basic System

You can now use the configuration file that you created to deploy a basic system from the Photon Controller CLI on your Linux workstation.

First, set the target for the Photon CLI tool by running the following command, replacing `<installer_VM_ip>` with the IP address of the Photon installation VM that you deployed earlier from the OVA. Add Port `9000` after the IP address.

```
photon target set http://<installer_VM_ip>:9000
```

You are now ready to deploy the Photon Controller system from your Linux workstation by running the following command:

```
photon system deploy config1.yml
```

If the deployment was unsuccessful, see the section on troubleshooting.

7 Checking the System's Status

First, change the target of the CLI tool to the static IP address of the management VM:

```
photon target set http://<management_VM_static_IP_address>:9000
```

Example:

```
photon target set http://198.51.100.44:9000
```

Second, check the system's status; example:

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

Finally, connect to the Photon Controller user interface by starting a web browser on your Linux workstation and going to the IP address of the management VM:

```
http://<mgt_ip>
```

Or, you can browse the API:

```
http://<mgmt_ip>:9000/api
```

When you're done checking the system out, you should delete it because authentication is disabled. To remove the system, run the following command in the Photon CLI on your Linux workstation:

```
photon system destroy
```

The next section demonstrates how to redeploy Photon Controller as a secured system.

8 Redeploying with Lightwave Authentication

This section shows you how to tear down the previous deployment of Photon Controller and redeploy it with Lightwave authentication. The redeployment builds on the knowledge you acquired during the first deployment.

Setting up Photon Controller with authentication requires you to add items to the YAML configuration file and to add a nested ESXi virtual machine to the ESXi host. You will also need a static IP address that you can dedicate to the VM running Lightwave.

8.1 Destroying the Previous Deployment

Before adding authentication, make sure you permanently erase the Photon Controller system that you deployed in the previous sections by running the following command in the Photon CLI on your Linux workstation:

```
photon system destroy
```

8.2 Preparing ESXi for Authentication

Deploying Photon Controller with authentication requires a second ESXi hypervisor dedicated to providing security services. For the purposes of installing Photon Controller with authentication quickly, this guide embeds a second ESXi host as a virtual machine in the primary ESXi host.

To support running the Lightwave authentication service on the nested ESXi host, you must enable `promiscuous mode` on the primary, physical ESXi host: In the `Navigator` pane of the vSphere Web Client, click `Networking`, click the vSwitch for `VM Network` (typically, `vSwitch0`), click `Actions`, click `Edit Settings`, expand `Security`, and then, for `Promiscuous mode`, select `Accept`.

The nested ESXi host has several requirements:

- 5 GB of RAM
- 150 GB of disk space
- A datastore with a different name than that of the primary ESXi host; in this example installation, the name will be `datastore2`. The datastore names must be unique so that each name maps to one actual datastore.
- A change to the VM's CPU settings to enable ESXi virtualization.
- SSH is enabled.

This section demonstrates how to fulfill these requirements as you install an ESXi host as a VM embedded in the primary ESXi host.

First, go to the VMware vSphere Hypervisor 6.0 Download Center and download the free version of ESXi 6.0 Update 2. Upload the ISO for ESXi to the datastore of your primary ESXi host.[6]

Now deploy a VM for the nested ESXi host by connecting to the primary ESXi host with the vSphere Web Client:

First, under `Navigator`, right-click `Host`, and then click `Create\Register VM`. On the `Select a creation type` page, select `Create a new virtual machine` and click `Next`.

Second, on the `Select a name and guest OS` page, enter a name for the VM, such as `Embedded ESXi Host for Auth`. For the `Guest OS family`, select Linux. For the `Guest OS version`, select `Other Linux (64-bit)`. Click `Next`.

Third, on the `Select storage` page, leave the datastore set to its default setting; click `Next`.

Fourth, on the `Customize settings` page, expand the `CPU` section and select `Expose hardware assisted virtualization to the guest OS`. Expand the `Memory` section and change the RAM to 5 GB. Next, change the setting for `Hard disk 1` to 150 GB. For the `CD/DVD Drive 1` setting, select `Datastore ISO file`, browse to the ESXi ISO file that you uploaded earlier, and then click `Select`. The ESXi ISO file name looks similar to this:

`VMware-VMvisor-Installer-6.0.0.update02-3620759.x86_64.iso`

Click `Next`, and then click `Finish`.

When it finishes deploying, power on the virtual machine, enable SSH on this new nested ESXi host, and then change the name of its datastore to `datastore2`.

8.3 Adding Lightwave Authentication to the Template

In the example above, the value for authentication is set to `false`. Turning on authentication requires the following additions to the YAML configuration file:

- A second `metadata` subsection that describes the networking information and credentials for the Lightwave authentication service.
- A static IP address for the nested ESXi host on which the authentication service will run.
- The name of the datastore on Lightwave's ESXi host; the name of its datastore must be different from the name of the datastore used by the management VM.
- Additional entries in the `deployment` section for authentication.

The new `metadata` section adds a key for `ALLOWED_SERVICES` set to `Lightwave`. The management VMs in this `metadata` sequence are dedicated to the Lightwave authentication service, and their networking information must be different from those in the metadata sequence for the management plane. Here is an example of a `metadata` sequence for authentication:

[6] For instructions, see Upload Files to Datastores.

```
  - metadata:
      ALLOWED_SERVICES: Lightwave
      MANAGEMENT_DATASTORE: datastore2
      MANAGEMENT_PORTGROUP: VM Network
      MANAGEMENT_NETWORK_NETMASK: 255.255.0.0
      MANAGEMENT_NETWORK_DNS_SERVER: 198.51.100.1
      MANAGEMENT_NETWORK_GATEWAY: 198.51.100.253
      MANAGEMENT_VM_IPS: 198.51.100.244
    address_ranges: 198.51.100.134
    username: root
    password: secret$1
    usage_tags:
      - MGMT
      - CLOUD
```

You also must add items to the `deployment` section for authentication:

```
deployment:
  resume_system: true
  image_datastores:
    - datastore1
    - datastore2
  auth_enabled: true
  oauth_tenant: 'esxcloud'
  oauth_username: 'Administrator'
  oauth_password: 'L1ghtWave!'
  oauth_security_groups:
  - "esxcloud\\Administrators"
  - "esxcloud\\photonControllerAdmins"
  sdn_enabled: false
  stats_enabled: false
  use_image_datastore_for_vms: true
  loadbalancer_enabled: true
  ntp_endpoint: 203.0.113.1
```

Here's what the relevant key-value pairs mean:

`resume_system`: This setting determines whether Photon Controller should continue operating after deployment; set it to `true`.

`auth_enabled`: Setting the value of this key to `true` turns on authentication.

`oauth_tenant`: The Photon Controller security domain; it must be set to `esxcloud`. All letters must be lowercase.

`oauth_username`: The user name of the Lightwave administrator.

`oauth_password`: The password for the Lightwave administrator. Change the value to a strong password that you will remember.

`oauth_security_groups`: A list of groups whose members receive system administrator rights on Photon Controller.

8.4 Example Configuration File with Authentication

Here is an example configuration file that includes key-value pairs and sequence items for authentication.

```
hosts:
```

```
  - metadata:
      MANAGEMENT_DATASTORE: datastore1
      MANAGEMENT_PORTGROUP: VM Network
      MANAGEMENT_NETWORK_NETMASK: 255.255.0.0
      MANAGEMENT_NETWORK_DNS_SERVER: 198.51.100.1
      MANAGEMENT_NETWORK_GATEWAY: 198.51.100.253
      MANAGEMENT_VM_IPS: 198.51.100.46
    address_ranges: 198.51.100.44
    username: root
    password: Secret$1
    usage_tags:
      - MGMT
      - CLOUD
  - metadata:
      ALLOWED_SERVICES: Lightwave
      MANAGEMENT_DATASTORE: datastore2
      MANAGEMENT_PORTGROUP: VM Network
      MANAGEMENT_NETWORK_NETMASK: 255.255.0.0
      MANAGEMENT_NETWORK_DNS_SERVER: 198.51.100.1
      MANAGEMENT_NETWORK_GATEWAY: 198.51.100.253
      MANAGEMENT_VM_IPS: 198.51.100.244
    address_ranges: 198.51.100.134
    username: root
    password: secret1
    usage_tags:
      - MGMT
      - CLOUD
deployment:
  resume_system: true
  image_datastores:
    - datastore1
    - datastore2
  auth_enabled: true
  oauth_tenant: 'esxcloud'
  oauth_username: 'Administrator'
  oauth_password: 'L1ghtWave!'
  oauth_security_groups:
  - "esxcloud\\Administrators"
  - "esxcloud\\photonControllerAdmins"
  sdn_enabled: false
  stats_enabled: false
  use_image_datastore_for_vms: true
  loadbalancer_enabled: true
  ntp_endpoint: 203.0.113.1
```

8.5 Building Your Configuration File and Deploying Photon Controller

Armed with these examples of how to add authentication to the YAML template, you can now rename your original deployment file `config2.yml` and modify it to include authentication. Or you can use the example configuration in the previous section as a template for your deployment. Replace the IP addresses, usernames, passwords, and datastore names in the template with those from your environment.

After you complete your YAML file, deploy it from your Linux workstation:

```
photon target set http://<installer_VM_ip>:9000
photon system deploy config2.yml
```

If the deployment was unsuccessful, see the section on troubleshooting.

9 Creating Accounts in Lightwave

After you deploy Photon Controller with authentication, you must log in to the Lightwave service and create a Photon Controller system administrators group that contains a user. When you're done, the authenticated user can create tenants, projects, and users on Photon Controller.

First, find the end point IP address of the Lightwave container by running the following commands with the Photon CLI on your Linux workstation:

```
photon deployment show
```

Connect to the Lightwave VM with SSH; the default password is `vmware`:

```
ssh esxcloud@<IPaddressOfAuthEndPoint>
```

Connect to the Lightwave container:

```
docker exec -it Lightwave bash
```

Change directories:

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

Using the password defined in the `oauth_password` key of your deployment template (`L1ghtwave!` in the example), run the following Lightwave directory commands to create a group, create a user, and add the user to the group.[7]

```
./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
```

Type `exit` to leave the container, and then type `exit` again to leave the SSH session.

10 Connecting to the Load Balancer

After the installer deploys Photon Controller and you created a security group in Lightwave, you can connect to the load balancer to create tenants, resource tickets, and projects.

First, find the load balancer's IP address by running the following commands with the Photon CLI on your Linux workstation:

```
photon deployment show
```

Since you deployed Photon Controller with authentication, you must connect to the IP address of the load balancer by appending Port `443`:

```
photon target set -c https://<production_system_ip>:443
```

And then you can log in by using the `pc-admin` account at `oauth_tenant` that you created in the Lightwave directory. Lightwave authenticates the user.

```
photon target login --username pc-admin@<oauth_tenant> --password 'Your$ecret1!'
```

[7] The second command in the series should be run as one line; here it wraps onto a second line to fit the page.

Here is an example. In the sample YAML file, the `oauth_tenant` is set to `esxcloud`—so `<oauth_tenant>` is replaced with `esxcloud`:[8]

```
photon target login --username pc-admin@esxcloud --password 'Your$ecret1!'
```

Finally, check your work:

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

As the status says, you're now ready to work with the system.

11 Creating a Kubernetes Cluster

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

12 Troubleshooting

If Photon Controller fails to install successfully, clean up the unsuccessful installation by destroying it before you try again:

```
photon system destroy
```

You can then troubleshoot by looking at the installer's logs. The most likely cause of a failure is that IP addresses assigned to a VM in the Photon Controller management plane are in use, unavailable, or unreachable.

12.1 Log Files for the Installer

The log files for the deployment reside in the following directory on the Photon Controller installer VM:

- /var/log/esxcloud/photon-controller-core/

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

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

12.2 Deploying the OVA Installer

If you get a failure screen when you deploy the OVA by using the vSphere Web Client, download and install the latest VIB for the web client from this URL:

```
https://labs.vmware.com/flings/esxi-embedded-host-client
```

[8] If you set `oauth-tenant` to something other than `esxcloud`, make sure all the letters are lowercase.

12.3 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.