Lumeta QuickStart for Hybrid Visibility

Enterprise VM Command Center + AWS Cloud Scout

Dawn F. Ross
Documentation & Training Development
Lumeta, a FireMon company
FINAL v2 4/8/20 7:36 PM

Copyright Notice

Terms & Conditions

Browse to this location for the FireMon software license and services agreement.

https://www.firemon.com/software-license-and-services-agreement_lumeta_april-2019/

Thank you for choosing Lumeta CloudVisibility Community Edition! FireMon designed this community edition to create an easy path for you to preview the software. We invite you to exercise the solution in your lab, experience hybrid visibility, and then join the growing body of companies that use Lumeta to gain authoritative visibility within and across their complex hybrid computing environments.

This document explains how to deploy a Lumeta Command Center to a private virtual machine belonging to your company. We call this the Enterprise VM Command Center.

It also explains how to deploy a Lumeta Cloud Scout to your region of the public cloud hosted by Amazon Web Services (AWS).

Once the Lumeta Enterprise VM Command Center and Lumeta Cloud Scout systems are deployed, you will learn how to configure them to achieve visibility within and across your organization's hybrid cloud network.

Deploying the Lumeta Command Center

Step 1: Download the Command Center OVA

To download the Lumeta Command Center image file (i.e., the OVA):

1. Browse to http://content.firemon.com/lumeta/community.
2. Request Lumeta CloudVisibility Community Edition by completing the form.
3. Go to your email inbox and follow the directions in the confirmation message from FireMon.
4. Save the Lumeta CloudVisibility Command Center OVA file to your local system.

Step 2: Instantiate the VM

Open the OVA image file to create a Lumeta Enterprise VM Command Center as follows:

1. Log in to VMware vCenter.
2. With a VMware ESXi host name selected, click **Actions** > **Deploy OVA Template**.
3. Browse to **Lumeta-3.3.3.2-Community-Edition.ova** on your local system and open it.
4. Click **Next** to proceed through two pages of options, accepting the defaults.
    a. You may rename the system, if you like, or accept its default name.
    b. On the Disk Format page, select **Thin Provision.**
5. Click **Finish** to deploy the image.
   Processors, memory, network connections, storage, and a guest operating system for your new Lumeta Command Center are instantiated. The name of your new system displays among the inventory of VMs listed on the left-hand side of the page.

Step 3: Initialize the System

To initialize the Lumeta Enterprise VM Command Center:

1. With manual configuration information (i.e., IP address, gateway, netmask, DNS) provided by your organization's network administrator in hand, power on the remote console of your Lumeta Command Center VM as follows:
    a. Select the **Lumeta CloudVisibility Command Center** VM.
    b. With the Summary tab displayed, click **Actions** > **Power** > **Power On**.
    c. Expand the remote console to full-screen, by clicking the black thumbnail image.

2. At the login prompt, enter the default UID **admin**.
3. At the password prompt, enter the default password **(732)357-3500**.
4. Enter a new host name for your system such as **Lumeta-Enterprise-CC**.
5. At the DHCP|manual prompt, choose *manual*.
6. Enter an IPv4 address such as **172.16.42.201**.
7. Enter a netmask such as **255.255.255.0**.
8. Enter the gateway router's IPv4 address such as **172.16.42.1**.
9. Enter the IP addresses of up to three DNS servers such as **8.8.8.8, 8.8.4.4, 5.5.5.5**.
10. Allow DHCP to supply default NTP servers from NTP.org by entering **yes**.
11. Change the default login password for the user "admin" to a new one you choose.

Your Lumeta Command Center VM is initialized and comes with a Community Edition license you may use for as long as you like, but on no more than 10 accounts and 100 compute instances. You may now exit the console.

Step 4: Log In

To log in to your new Lumeta system:

1. Copy the IP address of your CloudVisibility Command Center from VMware.
2. Paste it to the address bar of a supported web browser such as Chrome, Firefox, or IE.
3. Bookmark the location for subsequent logins.
4. Login with the username **admin** and the password you set during system initialization.

Congratulations! Your Lumeta Enterprise VM Command Center is deployed.

Deploying the Lumeta Cloud Scout

Step 1: Launch the Lumeta Cloud Scout AMI

Sign in to the Amazon Web Services (AWS) Marketplace, and then select the Lumeta Cloud Scout AMI.

1. In a web browser, navigate to the AWS Login page for your preferred region and sign in.
   a. US East (Northern Virginia)
   https://console.aws.amazon.com/ec2/v2/home?region=us-east-1 -Images:visibility=public-images;search=Lumeta,Cloud;sort=name
   b. US West (Northern California)
   https://console.aws.amazon.com/ec2/v2/home?region=us-west-1#Images:visibility=public-images;search=Lumeta,Cloud;sort=name
   c. EU (London)
   https://console.aws.amazon.com/ec2/v2/home?region=eu-west-2#Images:visibility=public-images;search=Lumeta,Cloud;sort=name
   d. Canada (Central)
   https://console.aws.amazon.com/ec2/v2/home?region=ca-central-1#Images:visibility=public-images;search=Lumeta,Cloud;sort=name
   e. Asia Pacific (Tokyo)
   https://console.aws.amazon.com/ec2/v2/home?region=ap-northeast-1#Images:visibility=public-images;search=Lumeta,Cloud;sort=name

2. Select the Lumeta Cloud Scout AMI, and then click **Launch**.

Step 2: Select Instance Type & Details

1. Select the instance type **t2.2xlarge**.
2. Click **Next: Configure Instance Details** and set the details per your organization's preferences, which may be to accept all of the defaults. Suggestions follow in **bold**.
    a. Number of Instances: **1**
    b. Purchasing Option: **Do not request**
    c. Network: **Accept default (e.g., LumetaVPC)**
    d. Subnet: **No preference**
    e. Auto-assign Public IP: **Use subnet setting**
    f. Placement Group: **Do not request**
    g. Capacity Reservation: **Open**
    h. IAM Role: **None**
    i. Shutdown Behavior: **Stop**
    j. Enable Termination Protection: **Do not request**
    k. Monitoring: **Do not request**
    l. Tenancy: **Shared – Run a shared hardware instance**
    m. Elastic Inference: **Do not request**
    n. T2/T3 Unlimited: **Do not request**
    o. Advanced Details: **Do not request**
3. Click **Next: Add Storage.**

Step 3: Add Storage

1. Accept the default values.
2. Click **Next: Add Tag**.
   Tags are optional. Use them to label, identify, or keep an inventory of instances.
3. Click **Next: Configure Security Group**

Step 4: Configure Security Groups

1. Create a new security group and configure these inbound security rules:

Type	Protocol	Port Range
SSH	TCP	22
HTTPS	TCP	443

2. Click **Review and Launch**.
3. Click **Launch**.

Step 5: Create a Private Key

1. Select or create a private key pair.

2. Download the private key pair and store it in a safe and accessible location.
   The private key pair is required on your first login to the Lumeta Cloud Scout. Thereafter, you'll log in as the user **admin** with the password you set during the software's initial configuration.

Step 6: Launch Instance

1. Click **Launch Instances.**
   The system begins its Initializing Instance Launch process.
2. Navigate to your EC2 dashboard.
3. Click **Running Instances** to watch your Lumeta Cloud Scout initialize.
4. To name the instance, click the **Pencil** icon.
5. Note the IPv4 Public IP address. You will need this to configure your virtual machine.

Step 7: Initialize the System

1. From a terminal window such as PuTTY or Terminal, log in to your Cloud Scout system as the user **admin**, authenticating with your private key file.
   a. Input the IPv4 Public IP address as the Host Name.
   b. Import your private key file. If you are using PuTTY, use PuTTYgen to convert the *pem* format to *ppk* format. Use the ppk-formatted key when you connect using PuTTY.
   The FireMon Cloud SDK Initial Configuration screen displays.
   c. Press **Enter** to continue.
2. Accept the default values by pressing **Enter** in response to these prompts:
   a. New host name or <Enter> to keep the old one?
   b. How would you like to configure the network? (dhcp|manual) [dhcp]
   c. How would you like to configure DNS? (dhcp|manual) [dhcp]
   d. How would you like to configure NTP? (dhcp|manual) [dhcp]
3. Enter a new admin password containing 8 characters. Use at least one uppercase letter, one lowercase letter, one number, and one special character.
4. Confirm the password and press **Enter**. Your initial system configuration is complete.

Your Licensed System

Congratulations! Your Lumeta Cloud Scout is deployed. Now that both the Enterprise Command Center VM and the AWS Cloud Scout are up and running, configure them to generate an authoritative index of your assets, inclusive of devices on private, on-premises, virtual, and cloud networks.

Configuring the Lumeta Command Center for Hybrid Visibility

Part 1: Configure Your Enterprise Command Center VM

1. **From a web browser, log in** to your Lumeta CloudVisibility Community Edition Command Center with the Username **admin** and the password you set during system initialization.

2. **Rename the default organization**, which serves as a container in Lumeta.
   a. Browse to **Settings** > **Organizations.**

b. Select the default, **Organization1,** and click **Edit**.
c. Set properties for your organization and click **Save**. Its new name displays.

3. **Edit the default zone**, which defines discovery space and which nodes will be map together.
   a. Browse to **Settings** > **Zones.**
   b. Select the default, **Zone1**, and click **Edit Zone**.
   b. Set properties for your zone, using an informative name and description.
   c. Set the organization name to the one you set in Step 2.
   d. Click **Update**. Your edited zone displays on the left in the Available Zones column.

4. **Add a collector**, which is a logical entity that transmits discovery rules and targets CIDRs. The collector carries a discovery definition, performs passive, active, and indirect discovery, references interfaces, watches message queues, and transmits collected data back to the Command Center. A collector must be configured and enabled in order to discover a network.

The collector will scan your network, collecting network data from it. It will then transmit this data back to your Enterprise Command Center for reporting and analysis.

To add a collector:
   a. Browse to **Settings** > **Zones**.
   b. In the Available Zones list, select the zone to which you want to add the collector.
   c. Click **Zone Collectors** > **Add**.
   d. Make sure the Enable Collector checkbox is unchecked so that discovery does not begin.
   e. Name the collector.
   f. Set the rescan interval to **30** minutes. This tells the collector to initiate a new cycle of collection every 30 minutes, unless the current cycle is still in progress.
   g. Select the Command Center interface to which you want to associate the collector.
   h. Click **Create**. Your new collector is added.

5. **Configure discovery** by defining which discovery methods and protocols the collector should use. Your Community Edition collector will abide by these settings and communicate the rules to any Scout participating in the discovery of the network.

   a. Broadcast
      i. Click **Broadcast** > **Edit** > ☑ **Enable Broadcast Discovery.** ☑
      ii. Accept all of the default options and click **Update**.

   b. OSPF, BGP, DNS, Discovery Spaces, Leak Path, Cloud
      i. Skip these discovery types for this configuration.
      ii. In this deployment model, CloudVisibility will come from the Cloud Scout.
      iii. Discovery Spaces is covered in the next section of this document.

   c. SNMP

   Tests all discovered hosts for system SNMP responsiveness. The system uses a master SNMP credentials list that indicates whether SNMPv2c Common Credentials or SNMPv3 credentials should be used during discovery, what authentication (SHA, MD5, none) and

privacy type (AES, AES256,DES, none) to use for each. The order that you input the SNMP aliases becomes their priority order.

i. Click **SNMP** > **Edit >** ☑ **Enable SNMP Discovery.**
   1. ☑ Common SNMPv2 credentials
   2. ☑ Collect interface data
   3. ☑Collect layer 2 data
   4. ☑Collect routes
   5. In Maximum route table size, input **5,000**.
   6. ☑ Skip BGP routes

ii. Select the options above and click **Update**.

iii. Select the **Credentials tab** on the right-hand side of the page and add credentials as necessary.
   1. For an SNMP v2c-type credential, supply . . .
      a. A community string such as "public"
      b. ☑ Use community string for alias
      c. An alias such as "aliasforpublic"
   2. For an SNMP v3-type credential, supply an. . .
      a. Alias such as "encrypteduser"
      b. Username such as "person123"
      c. Context, which is the name a management application should use to access network devices. Completing this field is optional.
      d. Authentication type, such as SHA, MD5, or none
         i. If you selected an authentication type of SHA or MD5, also select AES, AES256, or DES as the privacy type.

d. Path

i. Click **Path** > **Edit >** ☑ **Enable Path Discovery.**
   1. ☑ICMP
   2. ☑ SNMP
   3. ☑ DNS
   4. ☑ UDP High Port
   5. ☑ Trace to hosts
   6. ☑ Trace to discovered routes

ii. Select the options above; leave the rest as they are.

iii. Click **Update**.

e. Host

i. Click **Host** > **Edit >** [☑ **Enable Host Discovery.**
   1. ☑ ICMP
   2. ☑ SNMP
   3. ☑ DNS
   4. ☑ UDP High Port
   5. ☑ Target discovered routes,
   6. ☑ Use custom TCP port: Set to **80**

ii. Select or set the options above and click **Update**.

f. Port

i. Click **Port** > **Edit >** ☑ **Enable Port Discovery.**

ii. Accept the default settings and click **Update**.

g. Profile

i. Click **Profile** > **Edit**

1. ☑ Collect Windows File Sharing Protocol (CIFS)
2. ☑ Collect HTTP
3. HTTP ports: Input **80,8080**
4. HTTPS Ports: Input **443**
5. Click **Update**.

6. **Configure the Discovery Space** by specifying which networks to investigate.
   a. Make sure your zone and zone collector are still selected.
   b. Select **Discovery Spaces** > **Target List**.
   c. Click **Add** and then manually input a few network CIDRs for the system to pursue. Choose a relatively small and familiar target network in your test lab or sandbox environment for this first exploration. You can target IPv4 or IPv6 addresses. Separate entries with either commas or line breaks, like this: 10.201.0.7/24, 172.16.53.41/32, 2600:802:460:132::1/128.
   d. Click **Create**.
   Now the system is configured and you are poised to query your AWS cloud resources *and* discover the CIDR space in your Target List.
   e. Return to your zone collector and kick-off discovery by checking the box for . . .
      i. ☑ Enable Collector. Discovery processing begins immediately.

Configuring the Lumeta Cloud Scout for Hybrid Visibility

Part 2: Configure Your Lumeta Cloud Scout in AWS

For maximum visibility into AWS-hosted clouds, configure your AWS Cloud Scout as described here.

1. On the main menu of your Lumeta Command Center, browse to **Settings** > **Cloud Visibility**.
2. Set the Polling Interval to **30**. This tells the Command Center how often to retrieve results from the Cloud Scout.
3. In the Server Name field, enter the IPv4 public IP address (noted earlier) of your Cloud Scout.
4. In the Username field, enter **admin**, which is the username to the Cloud Scout.
5. In the Password field, enter the password you set when you deployed the Cloud Scout.
6. Click **Submit**. The message, “Configuration Saved” displays.
7. On the Credentials tab, click the green **Plus** icon.
8. Select the record type your organization uses to authenticate to AWS: *Basic*, *Role*, or *Instance*. These AWS credentials tell the Cloud Scout to collect data about your company account.
   a. If you selected *Basic*, provide these AWS account credentials:
      i. Name: Name of the AWS cloud account such as **sa-account**
      ii. Regions: Areas of operation such as **us-west-1**. The Scout monitors this region.
      iii. Access Key: AWS access key for the user
      iv. Secret Key: AWS secret key for the user
   b. If you selected *Role*, provide these AWS account credentials:
      i. Name: Name of the AWS cloud account such as **teambob**
      ii. Regions: An optional input such as **us-east-1**.

iii. Role: A set of permissions for making AWS service requests
iv. Session Name: Validates temporary security credentials
v. Account ID: AWS account key for the user
vi. Master Account ID: AWS account key for the user

c. If you selected *Instance*, provide this AWS account credential:
i. Name: Name of the AWS cloud account such as **devops**

9. Click **Save Credentials.**
10. To optimize discovery, these AWS IAM User policy permissions are recommended:
    a. EC2ReadOnlyAccess
    b. VPCReadOnlyAccess
    c. AmazonS3ReadOnlyAccess
    d. AWSCloudTrailReadOnlyAccess
    e. AmazonInspectorReadOnly Access.
11. Kick-off the discovery of your AWS-hosted cloud by returning to the Configuration tab and toggling the slider at the top from red (off) to **blue (on)**.

Thank you for configuring Lumeta for Hybrid Visibility! The system is now discovering your enterprise + cloud network.

To tell others in the community about your setup experience and access a variety of resources, browse to the Resource Center located at http://content.firemon.com/lumeta/cloudvisibility/resources. From there, you can connect to the CloudVisibility Community Forum to pose questions, get answers, and share your deployment experience.

On behalf of all of us at Lumeta, a FireMon company, thank you for evaluating our product and joining the Lumeta CloudVisibility community.