



Installation and Initial Configuration

SL1 version 12.1.0, rev3

Table of Contents

Introduction to Installing SL1	6
What is SL1?	7
User Interface	7
Database Server	7
Data Collection	8
Message Collection	8
What is SL1 Extended?	9
Compute	9
Load Balancer	9
Storage	9
Management	10
The SL1 Agent	10
Third-Party Software	10
Preparing Hardware Appliances for SL1	11
Hardware Specifications	12
Prerequisites for SL1 Hardware Appliances	12
Initial Configuration for SL1 Hardware Appliances	12
Changing the Password for em7admin	12
Changing Network Settings	13
Ports for SL1 Hardware Appliances	15
Preparing Virtual Machines for SL1	16
Virtual Machine Specifications	17
Build Nodes or Appliances in This Order	17
Deploying a Node or Appliance on a VMware System	17
Installing VMware Tools	18
Installing VMware Tools Using Yum	18
Installing VMware Tools Manually	19
Deploying a Node or Appliance on a Hyper-V System	19
Ports for Virtual Appliances	20
Required Ports	21
Open Ports on the ScienceLogic All-In-One Appliance	22
Open Ports on the ScienceLogic Database Server Appliance	22
Open Ports on the ScienceLogic Administration Portal Appliance	23
Open Ports on the ScienceLogic Data Collector Appliance	24
Open Ports on the ScienceLogic Message Collector Appliance	24
Installing and Configuring an SL1 Collector	26
Prerequisites	27
Workflow for Installing and Configuring an SL1 Collector	27
Configuring the PhoneHome Database Server (for Existing PhoneHome Configurations Only)	27
Downloading the ISO Image Containing the SL1 Collector	29
Installing an SL1 Collector	29
Configuring a New SL1 System for Communication	30
Configuring a New SL1 Collector	32
Connecting an SL1 Collector to the SL1 Database Server	33
Collector Initiates System Accepts	35
Collector Initiates User Accepts	38
Database Initiates System Accepts	41
Connecting an SL1 Collector to the SL1 Database Server using the Command-line Interface	46
System Accepted	46
User Accepted	47

Managing the Nodes Page	48
Viewing the List of Registered Nodes	48
Viewing the Tokens on the Nodes Page	50
Recreating a Token	51
Installing SL1 on Hardware Appliances and Virtual Appliances	52
Prerequisites	53
Upgrading	53
Installing the Database Server	53
Installing the Administration Portal, Data Collector and/or Message Collector	54
Licensing the SL1 Appliances	55
Additional Steps for SL1 10.1	55
Licensing and Configuring an Appliance	59
Navigating the Classic Web Configuration Utility	61
Logging into the Classic Web Configuration Utility	61
Changing the Password for the Classic Web Configuration Utility	62
Licensing and Configuring a Database Server or All-In-One Appliance	62
Configuring an Administration Portal	63
Configuring a Data Collector or Message Collector	65
Registering the Data Collector or Message Collector with the Database Server	66
Defining the Syslog Server	67
Defining the NTP Server	69
Creating a Bonded Interface	70
Defining a Proxy Server	72
Navigating the Node Configuration Utility	73
Logging into the Node Configuration Utility	73
Changing the Password for the Node Configuration Utility	74
Viewing the Collector Connection Status	75
Configuring the Proxy Server from the Node Configuration Utility	76
Adding a Bonded Interface from the Node Configuration Utility	76
Editing an Interface from the Node Configuration Utility	78
Navigating the Setup and Config Page	80
What is the Setup and Config Page?	81
Setup and Config Journey Workflows	82
Taking a Tour of SL1	82
Discover and Monitor Hybrid Cloud Infrastructure	83
Onboarding your Hybrid Cloud Infrastructure	83
Resetting a Completed Journey Workflow	86
Setting a Journey Workflow as "Not Applicable"	87
Configuring SL1 for PhoneHome Communication	90
What is PhoneHome Communication?	92
Prerequisites	94
Overview of the PhoneHome Configuration	94
Configuring the Database Server for PhoneHome	95
Before Configuring the Database Server	95
Configuring the Database Server in SL1 Version 11.2.0 and Later	96
Configuring a Single Database	96
Configuring a Database with a Non-default Address or Port	96
Configuring a Database with Multiple IP Addresses	97
Configuring Additional Databases in a HA or DR Environment	97
Configuring the Database Server in SL1 Version 11.1.x and Earlier	97
Configuring the Data Collectors and Message Collectors for PhoneHome	99
Registering the Data Collectors and Message Collectors	101

Managing Port Forwarding for PhoneHome Communication in SL1 Version 11.2.0 and Later	103
Viewing a List of Port Forwards	103
Adding a Port Forward	103
Removing a Port Forward	104
Defining Port Forwarding for PhoneHome Communication in SL1 Version 11.1.x and Earlier	105
Using Custom Options for AutoSSH	105
Configuring PhoneHome for High Availability and Disaster Recovery	106
Configuring the Primary Database Server for High Availability and Disaster Recovery	107
Configuring the Secondary Database Server for High Availability and Disaster Recovery	109
Configuring Data Collectors and Message Collectors for High Availability and Disaster Recovery	110
Syncing the High Availability and Disaster Recovery System	110
Adding a New Secondary Database Server	110
Managing Destinations	111
Viewing a List of Destinations	111
Adding a Destination Address	111
Removing a Destination	112
Managing Proxy Connections for PhoneHome Communication in SL1 Version 11.2.0 and Later	113
Viewing a List of Proxy Connections	113
Adding a Proxy Configuration	113
Deleting a Proxy Configuration	114
Managing Proxy Connections for PhoneHome Communication in SL1 Version 11.1.x and Earlier	115
Editing ssh_config	116
Configuring Data Collectors that Connect to the PhoneHome Database Server Through a Proxy	119
Copying the SSH key to Each Proxy	120
Synchronize the Data Collectors with the Database Server	120
Deleting a PhoneHome Collector	121
Deleting a PhoneHome Database Server	122
Using the Watchdog Service with SL1 11.1.x and Earlier	123
Logging PhoneHome Configuration Information	124
Viewing PhoneHome Logs in SL1 version 11.1.x and Earlier	124
Using the Command-Line Interface for PhoneHome Collection in SL1 Version 11.2.0 and Later	125
Additional New Command-line Features in SL1 version 11.2.0	126
Tuning PhoneHome Settings in SL1 Version 11.2.0 and Later	128
Viewing a List of Current PhoneHome Settings	128
Updating PhoneHome Settings	128
Using the Command-Line Interface for PhoneHome Collection in SL1 Version 11.1.x and Earlier	129
The phonehome Command	129
The monitor_phonehome Command	136
Troubleshooting the PhoneHome Configuration in SL1 Version 11.1.x and Earlier	136
Using the PhoneHome Troubleshooting Script	136
Available Commands	136
Basic Troubleshooting	138
Installing SL1 on AWS	140
AWS Instance Specifications	141
Deploying an SL1 System on AWS	141
What are the ScienceLogic AMIs?	141
Getting the ScienceLogic AMI	142
Launching the New Instance	144
Security Rules for Each Appliance Type	150
All-In-One Appliance	150
Database Server	152
Administration Portal	155

Data Collector	156
Message Collector	158
Additional Configuration Steps	159
Assigning an EIP to the New Instance	160
Accessing the Appliance Using SSH	162
Gathering Information Required for Accessing the Appliance Using SSH	163
Configuring SSH	163
UNIX and LINUX Users	163
Windows Users	164
Web Configuration Tool	164
Rebooting Data Collectors and Message Collectors	164
Installing SL1 in Azure	166
Prerequisites for Installing SL1 in Azure	168
System Requirements	168
Deploying an SL1 System in Azure	168
SL1 Appliance Deployment Order for Distributed Systems	168
Installing and Configuring the Azure CLI	169
Configuring an Azure Resource Group and Storage Account	169
Creating the BLOB_URI	171
Uploading a VHD Image File to an Azure Storage Account	172
Downloading the ScienceLogic VHD File	172
Converting a VHD Image File from Dynamic to Fixed	172
Uploading the VHD File to an Azure Container	173
Creating the Image	174
Creating an Azure Virtual Machine	174
Setting the Virtual Machine Allocation Method to Static	176
Configuring Ports on SL1 Appliances	178
Configuring the Virtual Machine	180
Troubleshooting	180
Updating SL1	182

Chapter

1

Introduction to Installing SL1

Overview

This manual describes how to install and configure SL1.

This chapter covers the following topics:

<i>What is SL1?</i>	7
<i>What is SL1 Extended?</i>	9
<i>The SL1 Agent</i>	10
<i>Third-Party Software</i>	10

What is SL1?

In a **Distributed** system, there are four general functions that an SL1 appliance can perform: user interface, Database Server, Data Collector, and Message Collectors. In large SL1 systems, dedicated nodes or appliances perform each function. In smaller systems, some nodes or appliances perform multiple functions. In the **All-In-One Appliance** system, a single SL1 node or appliance performs all four functions.

User Interface

Administrators and users access the user interface through a web browser. In the user interface, you can view collected data and reports, define organizations and user accounts, define policies, view events, and create and view tickets, among other tasks. The node or appliance that provides the user interface also generates all scheduled reports and provides access to the ScienceLogic API. The following nodes or appliances provide the user interface:

- **All-In-One Appliance.** An **All-In-One Appliance** performs all functions, including providing the user interface.
- **Database Server.** A **Database Server** can provide the user interface in addition to its database function.
- **Administration Portal.** A dedicated **Administration Portal** node or appliance can provide the user interface.

NOTE: The Administration Portal communicates only with the Database Server and no other SL1 appliance. All connections between the Administration Portal and the Database Server are encrypted in both directions.

Database Server

The node or appliance that provides the database function is responsible for:

- Storing all configuration data and policy data.
- Storing performance data collected from managed devices.
- In a distributed system, pushing data to and retrieving data from the nodes or appliances responsible for collecting data and collecting messages.
- Processing and normalizing collected data.
- Allocating tasks to the other nodes or appliances in the SL1 System.
- Executing some automation actions in response to events.
- Sending all email generated by the system.
- Receiving all inbound email for events, ticketing, and round-trip email monitoring.

The following appliances can perform these database functions:

- **All-In-One Appliance.** An **All-In-One Appliance** performs all functions.
- **Database Server.** A dedicated **Database Server** provides all database functions.

Data Collection

Data Collectors are the SL1 nodes or appliances that retrieve data from monitored devices. In a distributed system, nodes or appliances that perform the data collection function also perform some pre-processing of collected data and execute automation actions.

The following appliances can perform the collection function:

- **All-In-One Appliance.** An **All-In-One Appliance** performs all functions.
- **Data Collector.** One or more Data Collectors are configured in **collector groups** for resilience. A collector group can be configured such that if an individual collector fails, other members of the group will pick up and share the load (N+1). A Data Collector can also perform the message collection function.

NOTE: The SL1 Agent can also be used to collect data from devices on which it can be installed. See the [System Requirements](#) page of the Support Site for a complete list of operating systems and versions supported by the agent. You can collect data from devices using only Data Collectors, using only the SL1 Agent, or using a combination of both.

Message Collection

The SL1 appliances that receive and process inbound, asynchronous syslog and trap messages from monitored devices.

The following nodes or appliances can perform the message collection function:

- **All-In-One Appliance.** An **All-In-One Appliance** performs all functions.
- **Message Collector.** A dedicated **Message Collector** receives and processes inbound, asynchronous syslog and trap messages from monitored devices.
 - In distributed systems that use the SL1 agent, the Message Collector passes agent data to the Database server. On these distributed systems, the **Message Collector** must be a stand-alone node or appliance, not a combination **Data Collector/Message Collector**.
- **Data Collector.** A Data Collector can also perform the message collection function in addition to the data collection function.

What is SL1 Extended?

SL1 Extended Architecture includes additional types of SL1 nodes or appliances. The following SL1 features require the SL1 Extended Architecture:

- **Expanded Agent Capabilities.** You can configure the SL1 Agent to communicate with SL1 via a dedicated Message Collector. However, this configuration limits the capabilities of the SL1 Agent. If you configure the SL1 Agent to communicate with SL1 via a Compute Cluster, you expand the capabilities of the SL1 Agent to include features like extensible collection and application monitoring.
- **Data Pipelines.** Data pipelines transport and transform data. Data transformations include enrichment with metadata, data rollup, and pattern-matching for alerting and automation. The Data Pipelines provide an alternative to the existing methods of data transport (data pull, config push, streamer, and communication via encrypted SQL) in SL1. Data pipelines introduce message queues and communicate using encrypted web services.
- **Publisher.** Publisher enables the egress of data from SL1. Publisher can provide data for long-term storage or provide input to other applications that perform analysis or reporting.
- **Scale-out storage of performance data.** Extended Architecture includes a non-SQL database (Scylla) for scalable storage of performance data.
- **Anomaly Detection and future AI/ML developments.** Anomaly detection is a technique that uses machine learning to identify unusual patterns that do not conform to expected behavior. SL1 does this by collecting data for a particular metric over a period of time, learning the patterns of that particular device metric, and then choosing the best possible algorithm to analyze that data. Anomalies are detected when the actual collected data value falls outside the boundaries of the expected value range.

SL1 Extended Architecture includes the following additional SL1 nodes or appliances:

Compute

Compute nodes are the SL1 appliances that transport, process, and consume the data from Data Collectors and the SL1 Agent. SL1 uses Docker and Kubernetes to deploy and manage these services. T

Load Balancer

A load balancer is the SL1 node or appliance that brokers communication with services running on the Compute Cluster. Services running on the Compute Cluster are managed by Kubernetes. Therefore, a single service could be running on one Compute node in the Compute Cluster; to provide scale, multiple instances of a single service could be running on one, many, or all nodes in the Compute Cluster. To provide scale and resiliency, you can include multiple Load Balancers in your configuration.

Storage

SL1 Extended includes a **Storage Cluster** that includes multiple Storage Nodes and a Storage Manager. These SL1 nodes or appliances provide a NoSQL alternative to the SL1 relational database. The Storage Cluster can store performance and log data collected by the Data Collectors and the SL1 Agent.

Management

The **Management Node** allows administrators to install, configure, and update packages on the Compute Nodes cluster, Storage Nodes, and the Load Balancer. The Management Node also allows administrators to deploy and update services running on the Computer Cluster.

The SL1 Agent

The **SL1 agent** is a program that you can install on a device monitored by SL1. There is a Windows agent and a Linux agent. The agent collects data from the device and pushes that data back to SL1.

Similar to a Data Collector or Message Collector, the agent collects data about infrastructure and applications.

You can configure an agent to communicate with either the Message Collector or the Compute Cluster.

Third-Party Software



ScienceLogic does not support users installing third-party software on SL1 systems or users making unauthorized changes to the configuration of SL1. Doing so voids any warranties, express or implied.

Preparing Hardware Appliances for SL1

Overview

This chapter describes how to prepare hardware appliances before installing SL1.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (.
- To view a page containing all of the menu options, click the Advanced menu icon (.

This chapter covers the following topics:

<i>Hardware Specifications</i>	12
<i>Prerequisites for SL1 Hardware Appliances</i>	12
<i>Initial Configuration for SL1 Hardware Appliances</i>	12
<i>Ports for SL1 Hardware Appliances</i>	15

Hardware Specifications

For details about supported ScienceLogic Hardware Appliances, see the ScienceLogic Support Site.
<https://support.sciencelogic.com/s/system-requirements?tabset-e65a2=2>

Prerequisites for SL1 Hardware Appliances

Perform the following steps to prepare an SL1 appliance for configuration:

- Install the SL1 appliance in a server rack and connect the power cables according to the instructions provided with the hardware.
- Connect the SL1 appliance to your network.
- Connect a monitor and keyboard to the SL1 appliance.

Initial Configuration for SL1 Hardware Appliances

You must perform the following tasks during initial configuration of an SL1 hardware appliance shipped by ScienceLogic:

- *Change the password for the administrative user **em7admin**.*
- *Change the network settings for the appliance.* This includes changing the following:
 - The IP address for the network gateway; you must have already allocated IP addresses for the SL1 appliances
 - The primary IP address of the appliance
 - The Netmask for the primary IP address of the appliance
 - The IP address for the primary Nameserver

Changing the Password for **em7admin**

To change the password for the default administrative user **em7admin** for console logins and SSH access:

1. Either go to the console of the SL1 appliance or use SSH to access the server.
2. Log in as user **em7admin** with the current password.
3. At the shell prompt, type the following:

```
passwd
```

4. When prompted, type and re-type the new password.

Changing Network Settings

To change the IP address, Netmask, Gateway address, and DNS Server for an appliance in the **ifconfig** file:

1. Either go to the console of the SL1 appliance or use SSH to access the server.
2. Login as user **em7admin** with the appropriate password.
3. Enter the following at the command line:

```
sudo ifconfig
```

Your output will look like this:

```
ens32: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.64.68.20 netmask 255.255.255.0 broadcast 10.64.68.255
inet6 fe80::250:56ff:fe84:455f prefixlen 64 scopeid 0x20<link>
ether 00:50:56:84:45:5f txqueuelen 1000 (Ethernet)
RX packets 1774927 bytes 161985469 (154.4 MiB)
RX errors 0 dropped 861 overruns 0 frame 0
TX packets 1586042 bytes 158898786 (151.5 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 0 (Local Loopback)
RX packets 13406577 bytes 4201274223 (3.9 GiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 13406577 bytes 4201274223 (3.9 GiB)
```

```
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

4. Examine the output, find the first interface in the output, and note its name.
5. Use the vi editor to edit the settings for the interface. To do this, enter the following at the command line:

```
sudo vi /etc/sysconfig/network-scripts/ifcfg-interface name you noted in step #4
```

For example, from our output, we could enter:

```
sudo vi /etc/sysconfig/network-scripts/ifcfg-ens32
```

6. Your output will look like this:

```
TYPE=Ethernet
```

```
BOOTPROTO=none
```

```
DNS1=10.64.20.33
```

```
DEFROUTE=yes
```

```
IPV4_FAILURE_FATAL=no
```

```
IPV6INIT=yes
```

```
IPV6_AUTOCONF=yes
```

```
IPV6_DEFROUTE=yes
```

```
IPV6_FAILURE_FATAL=no
```

```
NAME=ens32
```

```
UUID=d471435d-9adf-47c9-b3f3-32f61dccbad8
```

```
DEVICE=ens32
```

```
ONBOOT=yes
```

```
IPADDR=10.64.68.20
```

```
PREFIX=24
```

```
GATEWAY=10.64.68.1
```

```
IPV6_PEERDNS=yes
```

```
IPV6_PEERROUTES=yes
```

7. You can edit one or more of the following settings:
 - **DNS1**=IP address of the DNS server that will be used by the SL1 appliance.
 - **IPADDR**=IP address of the SL1 appliance.
 - **PREFIX**=netmask for the SL1 appliance.
 - **GATEWAY**=IP address of the network gateway that will be used by the SL1 appliance.
8. Save your changes and exit the file (:wq)
9. At the command line, enter the following:

```
sudo service network restart
```

Ports for SL1 Hardware Appliances



See the chapter on [ports](#) to configure firewalls to allow traffic to and from the SL1 appliances.

Preparing Virtual Machines for SL1

Overview

This chapter describes how to prepare virtual nodes or appliances before installing SL1.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (.
- To view a page containing all of the menu options, click the Advanced menu icon ().

This chapter covers the following topics:

<i>Virtual Machine Specifications</i>	17
<i>Build Nodes or Appliances in This Order</i>	17
<i>Deploying a Node or Appliance on a VMware System</i>	17
<i>Installing VMware Tools</i>	18
<i>Deploying a Node or Appliance on a Hyper-V System</i>	19
<i>Ports for Virtual Appliances</i>	20

Virtual Machine Specifications

For details about supported hypervisors and the requirements and specifications for each SL1 appliance, see the ScienceLogic Support Site: <https://support.sciencelogic.com/s/system-requirements>

NOTE: You must have already allocated an IP address for each SL1 appliance.

Build Nodes or Appliances in This Order

For ease of configuration, create nodes or appliances in this order:

1. Database Server
2. Administration Portal (if applicable)
3. Data Collectors
4. Message Collectors (if applicable)

NOTE: The following instructions describe how to configure a ScienceLogic virtual machine in VMWare. If you are looking for resources and support for VMWare, see the VMWare Marketplace: <https://marketplace.cloud.vmware.com/>.

Deploying a Node or Appliance on a VMware System

To deploy an SL1 node or appliance on a VMware system:

1. If you have not already done so, download the ISO file for SL1.
2. Using the vSphere client, connect to your VMware system as a user that has permissions to deploy a new virtual machine and use the **Create New Virtual Machine** wizard to create a new virtual machine.
3. In the **Create New Virtual Machine** wizard, select the configuration options that are appropriate for your environment and the current recommended specifications for the appliance type you are installing. For details about requirements and specifications, see the **ScienceLogic System Requirements** page at <https://support.sciencelogic.com/s/system-requirements>
4. On the **Guest Operating System** page, select *Linux* as the **Guest Operating System**, and then select *Oracle Linux 4/5/6/7 (64-bit)* in the **Version** drop-down list.
5. On the **Network** page, you must select *VMXNET 3* in the **Adapter** field.
6. After completing the **Create New Virtual Machine** wizard, edit the settings for the virtual machine:

- Set the CPU and memory allocation to the values recommended in <https://support.sciencelogic.com/s/system-requirements>.
 - Configure the CD/DVD drive to use the SL1 ISO file.
6. Turn on the virtual machine and boot from the CD/DVD drive.
 7. Repeat these steps for each node or appliance in your SL1 system.

Installing VMware Tools

You must install VMware Tools on each Database Server, each Data Collector, and each Message Collector. You can install VMware tools in two ways:

- If your appliance can connect to the Internet, use the yum utility to install the necessary packages.
- If you have an appliance that is not able to reach the Internet, you can retrieve the required packages from a similar appliance that does have Internet access.

NOTE: When you install SL1 version 11.1.0 or later, the installer checks if you are installing on a VM in a vSphere environment. If true, the installer will automatically install VMware Tools.

Installing VMware Tools Using Yum

To install VMware tools using the yum utility:

1. Log in to the appliance as the em7admin user using the console or SSH.
2. Execute the following command:
3. Type the password for the em7admin user when prompted.
4. When prompted to confirm the installation, type "y".
5. Execute the following commands:

```
sudo yum install open-vm-tools
```

```
sudo systemctl start vmtoolsd.service
```

```
sudo systemctl enable vmtoolsd.service
```

```
sudo systemctl status vmtoolsd.service
```

If the installation was successful, the "Active" line in the output indicates VMware tools is "active (running)".

Installing VMware Tools Manually

CAUTION: If the `libtool-ldd` and `libxslt` packages were already installed on the host where you run the `yum downloadonly` command in step 1, below, then those dependent packages will be listed as missing and prevent you from installing VMware Tools. To work around this, remove those two packages from the host before running the following procedure.

To install VMware tools manually:

1. Retrieve the required packages from an appliance that has Internet access with the following command:

```
sudo yum install open-vm-tools --downloadonly --  
downloadaddir="/var/tmp/vmtools"
```
2. Once the download is complete, gather the downloaded RPM files into an archive file by running the following command, where "vmtools.tgz" can be any filename you choose:

```
cd /var/tmp && tar cvfz vmtools.tgz vmtools
```
3. Transfer the archive file to the appliance that does not have Internet access, and extract the RPMs by running the following command:

```
tar zxvf [name of the archive file]
```
4. Install the files with the following command:

```
sudo rpm -ivh vmtools/*.rpm
```
5. Start the `vmtoolsd` service with the following command:

```
sudo systemctl start vmtoolsd
```
6. To ensure that `vmtoolsd` starts automatically after a reboot, run the following command:

```
sudo systemctl enable vmtoolsd
```
7. Execute the following command:

```
sudo systemctl status vmtoolsd.service
```

If the installation was successful, the "Active" line in the output indicates VMware tools is "active (running)".

Deploying a Node or Appliance on a Hyper-V System

To deploy an SL1 node or appliance on a Hyper-V system:

1. Follow the instructions from Microsoft:
<https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/create-virtual-machine#create-a-virtual-machine-with-hyper-v-manager>
2. When prompted to **select a Generation** for the VM:

- **Generation 1.** Fully supports Oracle Linux and SL1.
 - **Generation 2.** To support Oracle Linux and SL1, you must disable the "secure boot" feature.
3. When prompted to **Assign Memory** and **Connect Virtual Hard Disk**, enter the hardware requirements as specified here:
<https://support.sciencelogic.com/s/system-requirements>
 4. In the **Installation Options** wizard, select **Install an operating system later**
 5. Click **[Finish]**.
 6. If you selected a **Generation 2** virtual machine, open a PowerShell session on the Hyper-V Manager host and execute the following PowerShell cmdlet to disable secure boot on the VM:

```
Set-VMFirmware "Test VM" -EnableSecureBoot Off
```
 7. Follow the steps specified here to install the Operating System (Oracle Linux 64 bit):
<https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/create-virtual-machine#complete-the-operating-system-deployment>
 8. Repeat these steps for each node or appliance in your SL1 system.
 9. To install SL1 on the Hyper-V virtual machines, see [Installing SL1 on Hardware Appliances and Virtual Appliances](#).

Ports for Virtual Appliances

See the chapter on [ports](#) to configure firewalls to allow traffic to and from the SL1 appliances.

Chapter



4

Required Ports

Overview

This chapter describes the required open ports on each SL1 appliance. These open ports allow communication between appliances in an SL1 system.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon .
- To view a page containing all of the menu options, click the Advanced menu icon ().

This chapter covers the following topics:

Open Ports on the ScienceLogic All-In-One Appliance	22
Open Ports on the ScienceLogic Database Server Appliance	22
Open Ports on the ScienceLogic Administration Portal Appliance	23
Open Ports on the ScienceLogic Data Collector Appliance	24
Open Ports on the ScienceLogic Message Collector Appliance	24

Open Ports on the ScienceLogic All-In-One Appliance

Name	Description	Protocol	Port
HTTP Interface	HTTP from browser session on user workstation. ScienceLogic recommends disabling HTTP during deployment.	TCP	80
HTTPS Secure Interface	Used for browser sessions on a user workstation, API requests from external systems, and requests from the ScienceLogic Agent running on a monitored device.	TCP	443
Database Web Admin	Optional. Administrative Web Interface (phpMyAdmin) from browser session on user workstation to Database.	TCP	8008
SSH	Optional. For ssh sessions from user workstation.	TCP	22
Web Configurator	Configuration Utility from browser session on user workstation.	TCP	7700
SNMP	Optional. SNMP information about the All-In-One Appliance can be collected by SL1.	UDP	161
SNMP Traps	Optional. Can receive SNMP traps from managed devices.	UDP	162
Syslog messages	Optional. Can receive syslog messages from managed devices.	UDP	514
SMTP	Optional. To receive inbound Email for tickets, events, and email round-trip monitoring.	TCP	25
DRBD Replication	This port is open only if your All-In-One Appliance is configured for Disaster Recovery.	TCP	7788

Open Ports on the ScienceLogic Database Server Appliance

Name	Description	Protocol	Port
HTTP Interface	Optional. Can be used if the Database Server also serves as an Administration Portal.	TCP	80
HTTPS Secure Interface	Optional. Can be used if the Database Server also serves as an Administration Portal.	TCP	443
Database Web Admin	Optional. Administrative Web Interface (PHPMYAdmin) from browser session on user workstation.	TCP	8008

Name	Description	Protocol	Port
MariaDB	Communication from Administration Portal. Communication from HA-secondary and DR to HA primary. NOTE: If you are using HA/DR, you must keep this port open. This port is required for communication between the HA-secondary and DR to the HA-primary appliance. If this port is blocked, the em7service on these databases will fail and could lead to issues such as DR backup not working or inability to license the appliances.	TCP	7706
SSH	Optional. Can be manually closed. For ssh sessions from user workstation.	TCP	22
Web Configurator	Configuration Utility from browser session on user workstation.	TCP	7700
SNMP	Optional. SNMP information about the Database Server can be collected by SL1.	UDP	161
ScienceLogic HA	Optional. Communication between Database Server and other Database Server(s) in a high-availability cluster.	TCP	694
SMTP	Optional. Can be manually closed. To receive inbound email for tickets, events, and email round-trip monitoring.	TCP	25
High Availability	One of two ports used by the cluster management process to test cluster availability. This port is open only if your Database Server appliance is configured for High Availability.	UDP	5555
High Availability	One of two ports used by the cluster management process to test cluster availability. This port is open only if your Database Server appliance is configured for High Availability.	UDP	5556
DRBD Replication	This port is open only if your Database Server appliance is configured for High Availability, Disaster Recovery, or both.	TCP	7788
PhoneHome Configuration	This port is open only if your Database Server appliance is configured for PhoneHome communication from Data Collectors and Message Collectors. The port number is configurable.	TCP	7705

Open Ports on the ScienceLogic Administration Portal Appliance

Name	Description	Protocol	Port
HTTP Interface	HTTP from browser session on user workstation.	TCP	80
HTTPS Secure Interface	Used for browser sessions on a user workstation and API requests from external systems.	TCP	443

Name	Description	Protocol	Port
SSH	Optional. For ssh sessions from user workstation.	TCP	22
Web Configurator	Configuration Utility from browser session on user workstation.	TCP	7700
SNMP	Optional. SNMP information about the Administration Portal can be collected by SL1.	UDP	161

Open Ports on the ScienceLogic Data Collector Appliance

Name	Description	Protocol	Port
Data Pull	Requests from Database Servers to retrieve collected data. In a Phone Home configuration, this port is accessed via an SSH tunnel created by the Data Collector.	TCP	7707
SSH	Optional. For ssh sessions from user workstation.	TCP	22
Web Configurator	Configuration Utility from browser session on user workstation.	TCP	7700
SNMP	Optional. SNMP information about the Data Collector can be collected by SL1.	UDP	161
SNMP Traps	Optional. Can receive SNMP traps from managed devices.	UDP	162
Syslog messages	Optional. Can receive syslog messages from managed devices.	UDP	514
HTTPS Secure Interface	Optional. Data from the ScienceLogic Agent running on a monitored device.	TCP	443

Open Ports on the ScienceLogic Message Collector Appliance

Name	Description	Protocol	Port
Data Pull	Requests from Database Servers to retrieve collected data. In a Phone Home configuration, this port is accessed via an SSH tunnel created by the Message Collector.	TCP	7707
SSH	Optional. For ssh sessions from user workstation.	TCP	22
Web Configurator	Configuration Utility from browser session on user workstation.	TCP	7700
SNMP	Optional. SNMP information about the Message Collector can be collected by SL1.	UDP	161
SNMP Traps	Optional. Can receive SNMP traps from managed devices.	UDP	162
Syslog messages	Optional. Can receive syslog messages from managed devices.	UDP	514
HTTPS Secure Interface	Optional. Data from the ScienceLogic Agent running on a monitored device.	TCP	443



Installing and Configuring an SL1 Collector

Overview

This chapter describes how to download and install an SL1 Collector, and how to establish a connection between the new SL1 Collector and the SL1 Database Server on the SL1 **Nodes** page. An SL1 Collector can be either a Data Collector or a Message Collector.

NOTE: The **Nodes** page and the Node Configuration Utility replace functionality previously found in the Web Configuration utility in versions of SL1 prior to version 11.2.0.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (.
- To view a page containing all of the menu options, click the Advanced menu icon ().

This chapter covers the following topics:

<i>Prerequisites</i>	27
<i>Workflow for Installing and Configuring an SL1 Collector</i>	27
<i>Configuring the PhoneHome Database Server (for Existing PhoneHome Configurations Only)</i>	27
<i>Downloading the ISO Image Containing the SL1 Collector</i>	29
<i>Installing an SL1 Collector</i>	29
<i>Configuring a New SL1 System for Communication</i>	30
<i>Configuring a New SL1 Collector</i>	32
<i>Managing the Nodes Page</i>	48

Prerequisites

Before installing and configuring an SL1 Collector in your ScienceLogic environment, you must:

- Have SSH access or console access to each Database Server
- On each ScienceLogic appliance, know the username and password for access to the console.
- On each ScienceLogic appliance, know the username and password for access to the console. Please note that the mysql password gets set using the same password that was set during the ISO installation as the "system" password, so the mysql password matches the login password for SL1 (unless one or both of the passwords were manually changed after the installation).
- Ensure that the Database Server opens a port for PhoneHome communication. The default port for this is **7705**, but you can use other ports if you prefer.

Workflow for Installing and Configuring an SL1 Collector

The typical workflow for installing and configuring an SL1 Collector includes the following steps:

1. **For existing PhoneHome configurations only:** [Configure the PhoneHome Database Server](#).
Complete this step *only* if you are currently using PhoneHome communication with your SL1 Collectors, and you are upgrading to SL1 version 11.2.0 or later from an earlier version of SL1.
 - If you use a proxy in your PhoneHome configuration, [perform the steps in the proxy section](#) before configuring the other steps in the PhoneHome configuration.
 - For more information about PhoneHome communication, see [Configuring SL1 for PhoneHome Communication](#).
2. [Download the ISO image containing the SL1 Collector](#). The ISO includes the Database Server, Administration Portal, and Data Collectors.
3. [Use the ISO to install the Database Server and Administration Portal](#), if they are not already installed.
4. [Use the ISO to install an SL1 Collector](#).
5. Update the new SL1 Collector to the same version of SL1 that the Database Server is running, if applicable.
6. [Configure a new SL1 system for communication](#), if applicable.
7. [Configure the new SL1 Collector](#) to communicate with the SL1 Database Server.

Configuring the PhoneHome Database Server (for Existing PhoneHome Configurations Only)

NOTE: If you are using a new SL1 system or a system that has not previously used PhoneHome communication for collectors, you can skip this section.

When upgrading to SL1 version 11.2.0, a pre-upgrade test in the system update procedure checks for existing PhoneHome Database Servers. Specifically, this test looks for PhoneHome token IDs inside the `/home/phonehome0/config.json` file, and fails if the value of the `id` field is less than or equal to "0".

In versions of SL1 prior to version 11.2.0, the primary PhoneHome Database Server was not self-registered with a token, causing it to have an `id` value of "0".

Therefore, if you are currently using a version of SL1 prior to version 11.2.0 and you are using PhoneHome communication with your SL1 Collectors, you or your SL1 administrator **must** complete the following one-time manual configuration steps prior to upgrading to version 11.2.0 .

CAUTION: Do not attempt to upgrade to SL1 version 11.2.0 until all pre-upgrade tests are successful on all PhoneHome Database Servers.

NOTE: For more information and configuration steps, see [Configuring SL1 for PhoneHome Communication](#).

To register a token for your primary PhoneHome Database Server:

1. Log in to the console of the Database Server or use SSH to access the server.
2. To determine if your PhoneHome Database Server is registered, type the following command and locate its `id` value:

```
cat /home/phonehome0/config.json
```

3. If a PhoneHome Database Server has an `id` value of "0", type the following command and locate the `id` of the current appliance:

```
phonehome status
```

4. Type the following command and locate the PhoneHome token:

```
phonehome token <id from step 3>
```


5. Type the following command to register the PhoneHome token:

```
phonehome register <token from step 4>
```

6. Repeat steps 2-5 for all PhoneHome Database Servers that have an `id` value of "0".
7. Type the following command to ensure that all of your PhoneHome Database Servers are synced:

```
phonehome sync
```

8. Repeat step 2 and confirm that all Database Servers have `id` values greater than "0".

TIP: After you have **downloaded** but not yet **installed** the ISO, you can also go to the **System Updates** page (System > Tools > Updates) and check the **Preupgrade Status** column to determine if the upgrade has successfully passed the pre-upgrade test. If the **Preupgrade Status** is *Incomplete*, click the magnifying glass icon () to determine which appliance is failing during the pre-upgrade test. **Do not** install the upgrade until the **Preupgrade Status** status displays as *Complete*.

Downloading the ISO Image Containing the SL1 Collector

NOTE: The following ISO installation steps do not affect the performance of the SL1 system. ScienceLogic recommends that you perform these steps at least 3 days before upgrading.

To download the ISO image:

1. Log in to the ScienceLogic Support site at <https://support.sciencelogic.com/s/> using your ScienceLogic customer account and password to access the site.
2. Select the **Product Downloads** menu and choose *Platform*. The **Platform Downloads** page appears.
3. Click the name of the SL1 version you want to download. The **Release Version** page appears.
4. Click the link for the "Product Image" you want to download and scroll to the bottom of the page. The **Release File Details** page appears.
5. Click the **[Download File]** button for the ISO file to download the file to your local computer.

Installing an SL1 Collector

In SL1 version 12.1.0, a new Oracle Linux 8 (OL8)-compatible installation wizard was added to the SL1 ISO file. All new SL1 12.1.0 installations from the ISO file will include OL8 by default.

NOTE: After you deploy the ISO version of SL1 12.1.0, you might get an "Appliance is not licensed" message on the login page. This situation only occurs if you use another tab or browser to log in to the SL1 environment after deployment. If you use the same browser or tab that you used for the deployment, the user interface will be available.

Before you can install the SL1 Collector, you will need to [use the ISO to install the SL1 Database Server](#) if it is not already installed.

After installing the Database Server, you can then install:

1. The Administration Portal (if applicable)
2. The Data Collectors
3. The Message Collectors (if applicable)

NOTE: You can use the following instructions to build the Administration Portal, and one or more Data Collectors and Message Collectors.

To install an SL1 Collector:

1. Boot the collector from the SL1 ISO.
2. Select **Install EM7**. The **Model Type** window appears.
3. Select **Collector** or **Message Collector** and then select **[Continue]**.
4. After the installer for the collector is loaded, the **Network Configuration** window appears.
5. Enter the following information:
 - **IP Address**. Type the primary IP address of the collector.
 - **Netmask**. Type the netmask for the primary IP address of the collector.
 - **Gateway**. Type the IP address for the network gateway.
 - **DNS Server**. Type the IP address for the primary Nameserver.
 - **Hostname**. Type the hostname for the collector.
7. Select **[Continue]**. The **System Password** window appears.
8. Type the password for the em7admin user on the operating system and select **[Continue]**.
9. Type the password for the em7admin user again and select **[Continue]**.
10. If you are using a VMware instance, after the collector reboots, follow the instructions to [install VMware tools](#).
11. After you install the SL1 Collector, upgrade the collector if needed to make sure the collector is running the same version of SL1 that the Database Server is running. Then you can connect the new collector with the SL1 Database Server.

Configuring a New SL1 System for Communication

If you are using a new SL1 system or a system that has not previously used PhoneHome communication for collectors, you or your SL1 administrator will need to configure each Database Server in the SL1 system to accept these connections.

NOTE: For more information about PhoneHome communication in previous releases, see [Configuring SL1 for PhoneHome Communication](#).

To enable communication between each Database Server and the new collector:

1. Log in to the console of the Database Server or use SSH to access the server:

```
ssh em7admin@<IP_address_of_Database_Server>
```

2. Run the following command to ensure that the collector can reach the IP address of the Database Server, which typically involves the use of port 7705:

```
sudo phonehome setup -a "<IP_address_of_Database_Server>:<port_number>" -n "<name_of_Database_Server>"
```

If setup succeeds, a message like the following displays: `New database with id 2 successfully added.`

After configuring communication between a Database Server and a collector, you can go to the console of the SL1 Collector or Database Server and run the following commands to view more information about your servers and collectors:

- To view a list of all PhoneHome Database Servers and collectors, including the addresses for the Database Server and the remote IP address corresponding to the collectors, run the following command:

```
phonehome list
```

- To view a list of only the Database Servers:

```
phonehome destination list
```

- To view information about a specific PhoneHome Database Server:

```
phonehome destination list --id <id>
```

where `<id>` is the PhoneHome device ID for the Database Server.

- To view information about the PhoneHome configuration of a specific Database Server or SL1 Collector:

```
phonehome view <id>
```

where `<id>` is the PhoneHome device ID for the Database Server or SL1 Collector.

- To ensure that the PhoneHome service is active on the Database Server and view additional configuration information about the server:

```
systemctl status phd.service
```

- To view the status of the PhoneHome service on the Database Server or SL1 Collector:

```
phonehome status
```

- If the PhoneHome service is disconnected on a Database Server or SL1 Collector and you want to start it:

```
systemctl start phc
```

NOTE: For more information about other PhoneHome-related commands, see [Using the Command-Line Interface for PhoneHome Collection in SL1 Version 11.2.0 and Later](#).

Configuring a New SL1 Collector

After you install an SL1 Collector, use the Add Node wizard on the **Nodes** page (Manage > Nodes) to register the collector so that it can communicate with the SL1 Database Server to share its collected data. Part of the setup takes place in the Node Configuration Utility, which has its own user interface separate from the SL1 user interface.

NOTE: The **Nodes** page and the Node Configuration Utility replace some of the functionality previously found in the Web Configuration Utility in versions of SL1 prior to version 11.2.0.

Depending on the type of connection you select in the Add Node wizard, communication between the SL1 Collector and the SL1 Database Server works in one of the following ways:

- **The SL1 Collector initiates an outbound connection to the Database Server over SSH.** Requests originate from edge to core via TCP, using port 7705 by default.

CAUTION: Please note that allow-listing port 7705 in the firewall is not enough. If the firewall does a layer 7 (application layer) filtering, you must create an exception rule to allow any outgoing traffic from the collector to all the Database Servers on the control port, which is port 7705 by default. Some firewalls enable this by default and, as a result, those firewalls will drop SSH traffic on a non-standard port like 7705 in this situation.

Access must be permitted from the trusted to the untrusted network. Each Data Collector is aligned with an SSH account on the Database Server and uses SSH to communicate with the Database Server. The benefits of this method are that no ingress firewall rules need to be added as the collector initiates an outbound connection, and no new TCP ports are opened on the network that contains the Data Collectors. Please note that starting with SL1 version 12.1.0, custom firewall rules must use the rich rules syntax and added to `/etc/siteconfig/firewalld-rich-rules.siteconfig`.

NOTE: This method was called the "PhoneHome" method in versions of SL1 prior to version 11.2.0. In the Add Node wizard, the "Collector Initiates | System Accepts" and "Collector Initiates | User Accepts" options use this communication method.

- **The SL1 Database Server initiates communication with each SL1 Collector over an open TCP port.** The connection request traverses the network, including the Internet if necessary, eventually reaching the collector. For this approach to work, the collector administrator must allow ingress communication from the Database Server on port 7707 (the MariaDB port on the collector). The communication is encrypted using SSL whenever possible. The benefit of this method is that communication to the Database Server is extremely limited, so the Database Server remains as secure as possible.

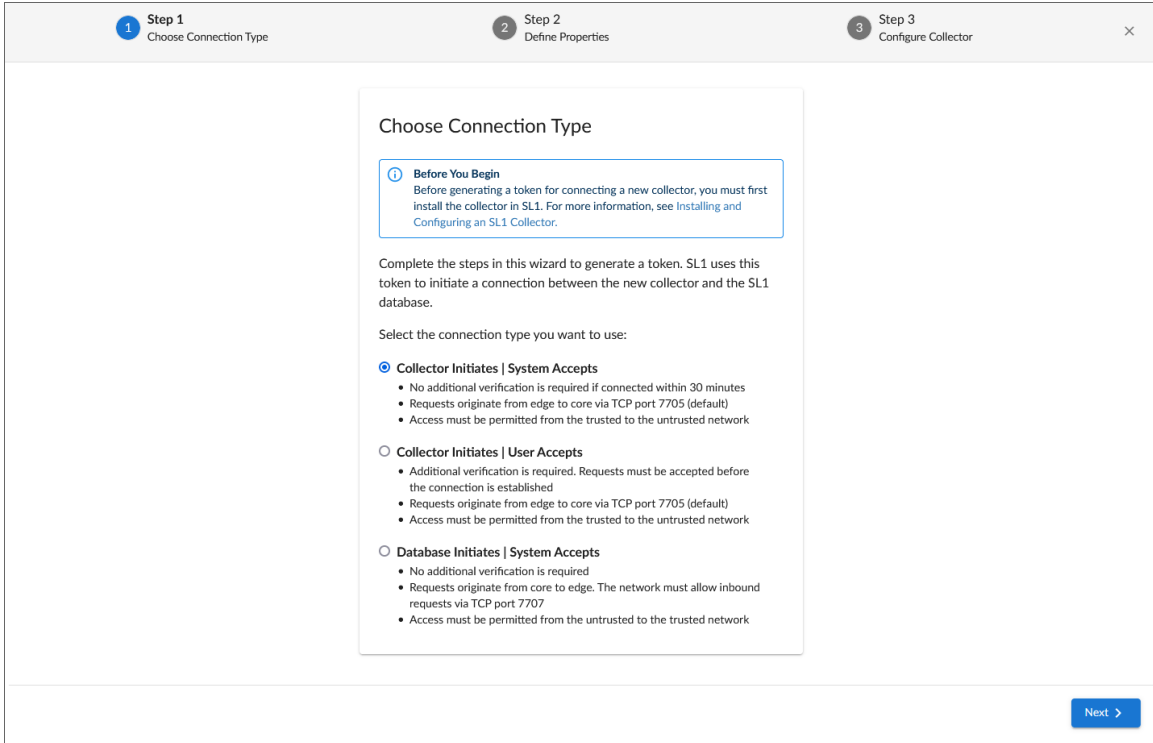
NOTE: This method was called the "Traditional" method in previous versions of SL1. In the Add Node wizard, the "Database Initiates | System Accepts" option uses this communication method.

Connecting an SL1 Collector to the SL1 Database Server

The **Add Node** wizard on the **Nodes** page in SL1 lets you configure your new SL1 Collector so that SL1 can register the SL1 Collector, connect it to the SL1 Database Server, and align it to a new or existing Collector Group.

All connection types require a token that SL1 generates as part of the wizard. A **token** is a JSON web token (JWT) that contains a set of secure data that SL1 uses to establish communication between the new SL1 Collector and the SL1 Database Server.

You access the **Add Node** wizard by clicking **[Add Nodes]** on the SL1 **Nodes** page (Manage > Nodes). The **Choose Connection Type** window of the Add Node wizard appears:



NOTE: Depending on your user permissions, you might not see all three connection type options on this window.

The following topics cover how to set up the three different connection types:

- [Collector Initiates | System Accepts \(Token-based PhoneHome\)](#)
- [Collector Initiates | User Accepts \(Token-less PhoneHome\)](#)
- [Database Initiates | System Accepts \(Traditional\)](#)

If you have used PhoneHome Communication with SL1 in previous releases, the connection types map as follows:

SL1 version 11.2.0 and later	Previous releases of SL1
Collector Initiates System Accepts	Token-based PhoneHome Communication
Collector Initiates User Accepts	Token-less PhoneHome Communication (using the Web Configuration Utility)
Database Initiates System Accepts	Traditional

Collector Initiates | System Accepts

To register and connect an SL1 Collector with the **Collector Initiates | System Accepts** option (a "token-based PhoneHome Communication" collector type):

1. On the **[Registered]** tab on the **Nodes** page (Manage > Nodes), click **[Add Nodes]**. The **Choose Connection Type** window of the Add Node wizard appears.
2. Select **Collector Initiates | System Accepts** and click **Next**. The **Define Collector Properties** window appears.
3. Complete the following fields as needed:
 - **Collector Name**. Type the name the collector used when registering the collector. SL1 will update this value with the collector hostname.
 - **Collector IP Address or Hostname**. Type the IP address or the hostname of the collector. This information is optional but recommended, as it is used in Step 3 of the wizard to create a link to the collector's Node Configuration Utility, where you will input the token you generate.
 - **Collector Description**. Type a description of the collector. This field is optional.
 - **Collector Group**. The new collector must be aligned to an SL1 Collector Group. You have the following options for this field:
 - Select an existing Collector Group from the drop-down.
 - Create a new Collector Group for the collector by clicking the plus icon (+). On the **Add Collector Group** modal, you can name the new group and choose to make that Collector Group available to all current and future organizations. You can also limit the Collector Group to specific organizations.

The **All current and future organizations** toggle is enabled by default. If you want to limit Organization access to the new Collector Group, disable this toggle and select the organization or organizations from the drop-down.
 - **Collector Type**. Your options include:
 - *Data Collector*. This is the most commonly used type. A Data Collector retrieves a specific set of information from monitored devices. A Data Collector can also work as a Message Collector.
 - *Message Collector*. A Message Collector receives and processes inbound, asynchronous syslog and trap messages from monitored devices.

4. Click [**Generate Token**]. The **Configure Collector** window appears.

NOTE: You can go back to a previous step at any point in the wizard, but when you click the [**Generate Token**] button, SL1 always generates a new token. You cannot retrieve this particular token if you close the Add Node wizard. The generated token expires after 30 minutes.

5. In the **Token** field, click the Copy icon (📄) to copy the token .
6. Open the Node Configuration Utility by clicking the Open icon (🔗) in the **Node Configuration Utility** field. The login page for the Node Configuration Utility opens in a new browser window.

TIP: If you did not specify an IP address or a hostname in step 2 of this wizard, you will need to open a new browser window and type the IP address or hostname for the collector, followed by ":7700/node-config", such as "https://10.1.1.100:7700/node-config".

NOTE: If the node type is not a collector, the Node Configuration Utility will display the following message: "This page will only be visible if you are on a collector."

7. Log in to the Node Configuration Utility using the same username and password that you used when you installed the collector. After you log in, the collector and the SL1 Database Server attempt to connect. The connection will fail, which is expected. The **Connect Collector** page appears with an empty **Paste token** text field:

Connect Collector

Enter a token to register your collector and initiate a connection to your SL1 database server. Alternatively, click the "Manual Entry" button, below, to enter SL1 database addresses to configure this collector or initiate a connection request.

Paste token

- Paste the token you copied in step 6 in the **Paste token** field.

NOTE: If you did not generate a token, you can click **[Manual Entry]**, select *User Accepted Connection Request*, and add the IP addresses for the Database Servers (CMDDBs) in the text box.

- After pasting the token, click **[Register]** or **[Register Database]**, based on your choices in the previous step. When the connection is made, a **Success** dialog states that the collector was registered and the connection to the database was initiated.
- Click **[OK]** on the **Success** dialog. The **Collector Connection Status** page displays details about the collector and the Database Server, along with the connection state, which can be "Connected", "Not Connected", or "Unknown". "Unknown" indicates that SL1 has not yet completed its first check of the connection state; click **[Refresh Status]** after a few moments and the status should update to "Connected".

Collector Connection Status

Collector Details

Collector ID: 3
Remote IP: 127.0.0.3

Database 2 ✓ Connected

Address: 10.64.226.33:7705
Connected Since: Feb 15, 2022, 10:13 AM (13 seconds)
Last Status Check: Feb 15, 2022, 10:13 AM
Network Path:
10.64.226.33:7705

[Disconnect & Clear Configuration](#) Refresh Status

- On the **Collector Connection Status** page, click the expand icon (∨) to view the connection path. The health of each hop in the connection is reported separately, but hops after an unresponsive hop will not be checked. This "Connection Path" information can be useful in diagnosing collector-database connection issues.
- To view any changes to the connection status, click **[Refresh Status]**.

NOTE: If you want to disconnect the collector and close the SSH tunnel between the collector and the Database Server, click *Disconnect & Clear Configuration*. This action will close the outgoing connection from the collector to all configured destinations, and it will also clear all local configuration. This action cannot be undone.

13. Close the Node Configuration Utility.
14. In SL1, go to the **[Registered]** tab on the **Nodes** page, where you can now see the new collector in the list, aligned with the Collector Group you specified in the Add Node wizard. The new collector also displays on the **Appliance Manager** page (System > Settings > Appliances).
15. On Step 3 of the Add Node wizard, click **[See Pending Requests]**. The **[Pending]** tab on the **Nodes** page appears with the pending request.
16. Select the Actions icon (⚙️) next to the pending request for the new collector and select **Accept**. The **Accept Request** dialog appears.
17. Paste the six-digit confirmation code from the **Connect Collector** page of the Node Configuration Utility and click **[Validate]**. The **Configure Collector** dialog displays a summary of the collector information you entered in the Add Node wizard.
18. Edit the collector information and collector group as needed, and then click **[Save]**. The **Configure Collector** dialog displays a summary of your information.
19. Click **[OK]**. The **[Registered]** tab on the **Nodes** page displays the new collector, aligned with the collector group you specified. The new collector also displays on the **Appliance Manager** page (System > Settings > Appliances).

Collector Initiates | User Accepts

To register and connect an SL1 Collector with the **Collector Initiates | User Accepts** option (a "token-less PhoneHome Communication" collector type):

1. On the **[Registered]** tab on the **Nodes** page (Manage > Nodes), click **[Add Nodes]**. The **Choose Connection Type** window of the Add Node wizard appears.
2. Select **Collector Initiates | User Accepts** and click **Next**. The **Define Collector Properties** window appears.
3. Complete the following fields as needed:
 - **Collector Name**. Type the name the collector used when registering the collector. SL1 will update this value with the collector hostname.
 - **Collector IP Address or Hostname**. Type the IP address or the hostname of the collector.
 - For "Collector Initiates | System Accepts" and "Collector Initiates | User Accepts" connection types, this information is optional but recommended, as it is used in Step 3 of the wizard to create a link to the collector's Node Configuration Utility, where you will input the token you generate.
 - For a "Database Initiates | System Accepts" connection type, you must type the IP address in this field so the Database Server can connect to the collector.
 - **Collector Description**. Type a description of the collector. This field is optional.



- **Collector Group.** The new collector must be aligned to an SL1 Collector Group. You have the following options for this field:
 - Select an existing Collector Group from the drop-down.
 - Create a new Collector Group for the collector by clicking the plus icon (+). On the **Add Collector Group** modal, you can name the new group and choose to make that Collector Group available to all current and future organizations. You can also limit the Collector Group to specific organizations.

NOTE: The **All current and future organizations** toggle is enabled by default. If you want to limit Organization access to the new Collector Group, disable this toggle and select the organization or organizations from the drop-down.

- **Collector Type.** Your options include:
 - *Data Collector.* This is the most commonly used type. A Data Collector retrieves a specific set of information from monitored devices. A Data Collector can also work as a Message Collector.
 - *Message Collector.* A Message Collector receives and processes inbound, asynchronous syslog and trap messages from monitored devices.

4. Click [**Generate Token**]. The **Configure Collector** window appears.

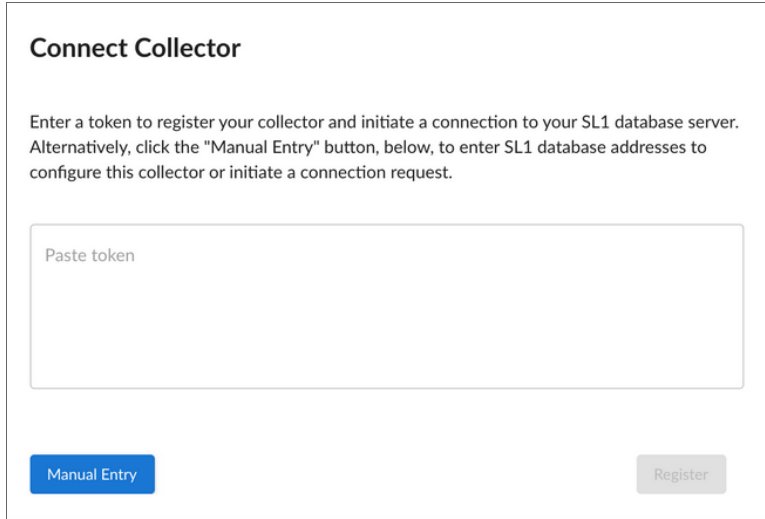
NOTE: You can go back to a previous step at any point in the wizard, but when you click the [**Generate Token**] button, SL1 always generates a new token. You cannot retrieve this particular token if you close the Add Node wizard. The generated token expires after 30 minutes.

5. Click the Copy icon () to copy the token in the **Token** field.
6. Open the Node Configuration Utility by clicking the Open icon () in the **Node Configuration Utility** field. The login page for the Node Configuration Utility opens in a new browser window.

TIP: If you did not specify an IP address or a hostname in step 2 of this wizard, you will need to open a new browser window and type the IP address or hostname for the collector, followed by ":7700/node-config", such as "https://10.1.1.100:7700/node-config".

NOTE: If the node type is not a collector, the Node Configuration Utility will display the following message: "This page will only be visible if you are on a collector."

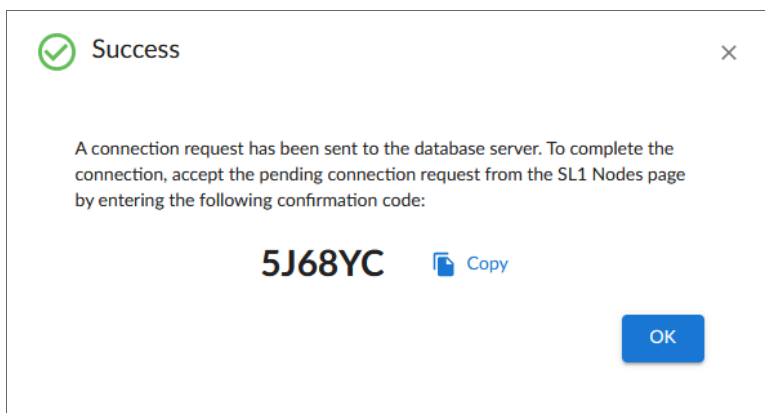
7. Log in to the Node Configuration Utility using the same username and password that you used when you installed the collector. After you log in, the collector and the SL1 Database Server attempt to connect. The connection will fail, which is expected. The **Connect Collector** page appears with an empty **Paste token** text field:



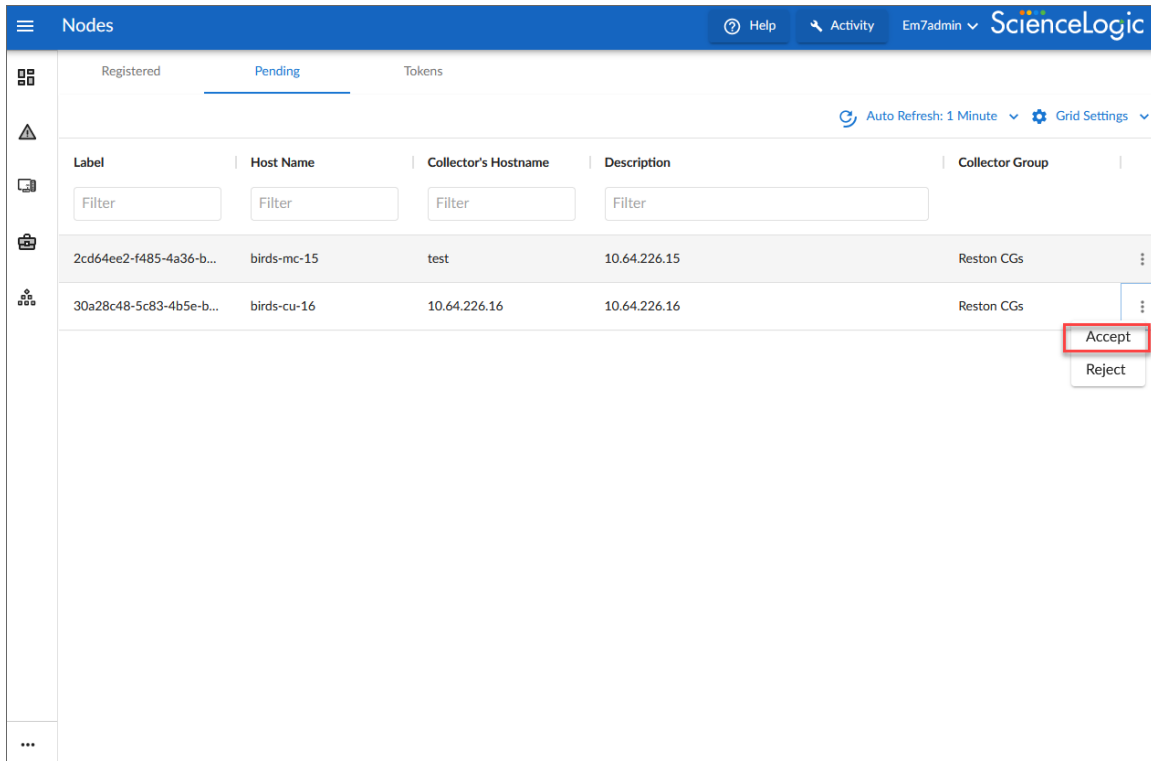
8. Paste the token you copied in step 6 in the **Paste token** field.

NOTE: If you did not generate a token, you can click **[Manual Entry]**, select *User Accepted Connection Request*, and add the IP addresses for the Database Servers (CMDBs) in the text box.

9. After pasting the token, click **[Register]** or **[Register Database]**, based on your choices in the previous step. When the connection is made, the **Success** dialog contains a six-digit confirmation code. Click the Copy icon (📄) to copy the confirmation code.



10. Click **[OK]** on the **Success** dialog. The **Collector Connection Status** page displays details about the connection request and the same six-digit confirmation code.
11. In SL1, click **[See Pending Requests]** on Step 3 of the Add Node wizard. The **[Pending]** tab on the **Nodes** page appears with the pending request.



12. Select the Actions icon (⋮) next to the pending request for the new collector and select **Accept**. The **Accept Request** dialog appears.
13. Paste the six-digit confirmation code from the **Connect Collector** page of the Node Configuration Utility and click **[Validate]**. The **Configure Collector** dialog displays a summary of the collector information you entered in the Add Node wizard.
14. Edit the collector information and collector group as needed, and then click **[Save]**. The **Configure Collector** dialog displays a summary of your information.
15. Click **[OK]**. The **[Registered]** tab on the **Nodes** page displays the new collector, aligned with the collector group you specified. The new collector also displays on the **Appliance Manager** page (System > Settings > Appliances).

Database Initiates | System Accepts

To register and connect an SL1 Collector with the **Database Initiates | System Accepts** option (a "traditional" or non-PhoneHome collector type):

1. On the **[Registered]** tab on the **Nodes** page (Manage > Nodes), click **[Add Nodes]**. The **Choose Connection Type** window of the Add Node wizard appears.
2. Select **Database Initiates | System Accepts** and click **Next**. The **Define Collector Properties** window appears.
3. Complete the following fields as needed:
 - **Collector Name**. Type the name the collector used when registering the collector. SL1 will update this value with the collector hostname.
 - **Collector IP Address or Hostname**. Type the IP address in this field so the Database Server can connect to the collector. Required.
 - **Collector Description**. Type a description of the collector. This field is optional.
 - **Collector Group**. The new collector must be aligned to an SL1 Collector Group. You have the following options for this field:

NOTE: The **All current and future organizations** toggle is enabled by default. If you want to limit Organization access to the new Collector Group, disable this toggle and select the organization or organizations from the drop-down.

- **Collector Type**. Your options include:
 - *Data Collector*. This is the most commonly used type. A Data Collector retrieves a specific set of information from monitored devices. A Data Collector can also work as a Message Collector.
 - *Message Collector*. A Message Collector receives and processes inbound, asynchronous syslog and trap messages from monitored devices.
4. Click **[Generate Token]**. The **Configure Collector** window appears.

NOTE: You can go back to a previous step at any point in the wizard, but when you click the **[Generate Token]** button, SL1 always generates a new token. You cannot retrieve this particular token if you close the Add Node wizard. The generated token expires after 30 minutes.

5. Click the Copy icon (📄) to copy the token in the **Token** field.
6. Open the Node Configuration Utility by clicking the Open icon (🔗) in the **Node Configuration Utility** field. The login page for the Node Configuration Utility opens in a new browser window.

TIP: If you did not specify an IP address or a hostname in step 2 of this wizard, you will need to open a new browser window and type the IP address or hostname for the collector, followed by ":7700/node-config", such as "https://10.1.1.100:7700/node-config".

NOTE: If the node type is not a collector, the Node Configuration Utility will display the following message: "This page will only be visible if you are on a collector."

7. Log in to the Node Configuration Utility using the same username and password that you used when you installed the collector. After you log in, the collector and the SL1 Database Server attempt to connect. The connection will fail, which is expected. The **Connect Collector** page appears with an empty **Paste token** text field:

Connect Collector

Enter a token to register your collector and initiate a connection to your SL1 database server. Alternatively, click the "Manual Entry" button, below, to enter SL1 database addresses to configure this collector or initiate a connection request.

Paste token

8. Paste the token you copied in step 6 in the **Paste token** field.

NOTE: If the collector and Database Server are not able to connect, make sure that port 7707 is open between the Database Server and the collector.

9. Alternately, instead of pasting the token here, you can save time with additional configuration that you will need to do later by clicking **[Manual Entry]**, selecting **Database Initiated Connection**, and adding the IP addresses for the Database Servers (CMDBs) in the text box.

Collector Connection Status

User Accepted Connection Request

- Sends a pending connection request to the SL1 database server. Pending requests must be accepted before this collector connects to the SL1 database.

Database Initiated Connection

- Configures this collector to accept a connection request from the SL1 database server. This collector must be registered with SL1 before the database server will attempt to connect.

Please enter one or more database server IP addresses, one per line.

192.1.1.1
192.1.1.2
2001:0db8:85a3:0000:0000:8a2e:0370:7334

TIP: Using this option lets you add all IP addresses for your Database Servers (CMDBs), including primary, High Availability (HA) and Disaster Recovery (DR) servers.

10. After pasting the token or manually adding the IP addresses, click **[Register]** or **[Register Database]**, based on your choices in the two previous steps. When the connection is made, a **Success** dialog states that the collector was configured to accept a connection from the Database Server, and that you need to register the collector in SL1 if you have not already done so. Click the link in the **Status** dialog to get more information about registering a collector.

11. Click **[OK]** on the **Success** dialog. The **Connect Collector** page appears, with a message stating that the collector can receive inbound connection requests.

Connect Collector

i This collector accepts inbound connections from a SL1 database at the following address(es):
10.64.226.33

Enter a token (or manually enter a database address) only if you wish to initiate an outbound connection or update the list of accepted inbound database addresses.
[Clear List Of Accepted Inbound Addresses](#)

Enter a token to register your collector and initiate a connection to your SL1 database server. Alternatively, click the "Manual Entry" button, below, to enter SL1 database addresses to configure this collector or initiate a connection request.

Paste token

Manual Entry **Register**

12. After you connect the new collector, you will need to manually register the collector in SL1 by navigating to the **Appliance Manager** page (System > Settings > Appliances).

13. At the top of the **Appliance Manager** page, complete the following fields:

- **Host Name.** Type the host name of the collector.
- **IP Address.** Type the **loopback IP address** of the collector. The loopback IP address is a special, virtual network interface that your computer uses to communicate with itself. This address also allows you to view content on a server in the same way a client would. In most cases, the loopback address is 127.0.0.1, although the loopback address can be any IP address in the 127.0.0.0/8 block.
- **Model Type.** Select the type of appliance (Data Collector or Message Collector) you are registering.


NOTE: When you select either type of collector, the **DB User** and **DB Password** fields appear. If the Database Server has different credentials from the collector, type the credentials for MariaDB on the Collector. This credential was entered when the ISO was deployed.

- **Description.** Type a description for the Data Collector or Message Collector. This field is optional.
- **DB User.** Type a user name that can access the MariaDB database on the Data Collector or Message Collector.

NOTE: For SL1 version 11.3.0 and later, this user is the default database user for MariaDB. This user has the same password as the admin and root user, and the password is set during the initial installation. If you upgraded to SL1 version 11.3.0 or later from an earlier version, the DB user name is "root". If you installed SL1 version 11.3.0 from the ISO, the DB user name will be "clientdbuser".

- **DB Password.** Type a password that allows access to the MariaDB database on the Data Collector or Message Collector.

NOTE: In SL1 version 11.2.0, SL1 automatically set the default database credentials when adding an SL1 collector to the stack. Starting with SL1 version 11.3.0, SL1 no longer specifies the credentials. As a result, you will need to specify the credentials for the collector on the **Appliances** page (System > Settings > Appliances), in the **DB User** and **DB Password** fields.

14. Click **[Save]**. If the save is successful, the message "Appliance Registered" displays.
15. If all information is valid and the Database Server can communicate with the Data Collector or Message Collector, the **Appliance Manager** page displays the SL1 version installed on the collector in the **Build** column. If the **Build** column remains blank for longer than five minutes, double-check your settings and network connection.
16. Perform steps 13-15 for each Data Collector and Message Collector in your configuration.
17. Finally, align the new collector with the relevant Collector Group by going to the **Collector Groups** page (Manage > Collector Groups or System > Settings > Collector Groups in the classic user interface).
18. Select the Collector Group you want to use, select the new collector from the **Message Collector Selection** field or the **Message Collector Selection** field, and click **[Save]**. In the classic user interface, click the edit icon () next to the Collector Group you want to use, select the new collector from the **Collector Selection** field, and click **[Save]**.
19. Go to the **[Registered]** tab on the **Nodes** page (Manage > Nodes), where you can now see the new collector in the list, aligned with the Collector Group you specified.

Connecting an SL1 Collector to the SL1 Database Server using the Command-line Interface

System Accepted

In this connection method, the database administrator creates a new token on the database appliance.

To connect a collector using the System Accepted method with the command-line interface:

1. Go to the console of the Database Server or use SSH to access the server and log in as user **em7admin** with the password you configured during setup.

2. Run the following command:

```
phonehome token new <model_type> <name> <CUG_ID ><description>
```

where:

- `<model_type>` is either a `cu` for a Data Collector or `mc` for a Message Collector.
- `<name>` is the name of the PhoneHome collector. You can use any name you want.
- `<CUG_ID>` is the numeric ID of a collector group from SL1.
- `<description>` is the descriptive text about the collector.

3. Make a note of the resulting token and share it with the collector administrator.
4. The collector administrator registers the collector using the token value by running the following command on the SL1 collector:

```
sudo phonehome register <token>
```

User Accepted

In this connection method, the collector administrator sends a registration request from the collector.

To connect a collector using the User Accepted method with the command-line interface:

1. Go to the console of the SL1 collector or use SSH to access the collector and log in as user **em7admin** with the password you configured during setup.

2. Run the following command on the collector:

```
sudo phonehome request send <address_1> [<address_2> <address_3> ...  
<address_n>] [-l <label>]
```

where:

- `<address>` is the destination address of the database server, in "host:port" format. You can include multiple addresses to one or multiple databases. Separate multiple addresses with a space.
- `<label>` is an optional field you can use to associate a human-friendly identifier with the request. Every request is identified by a random string on the server side, and it might be confusing for the database administrator to find a specific request if numerous requests are coming from other collectors.

3. Make a note of the one-time secret and share it with the database administrator.

4. The Database administrator accepts the incoming request using the one-time secret by running the following command on the Database Server:

```
phonehome request accept <uuid> <model_type> <name> <CUG_ID>
<description> <one_time_secret>
```

where:

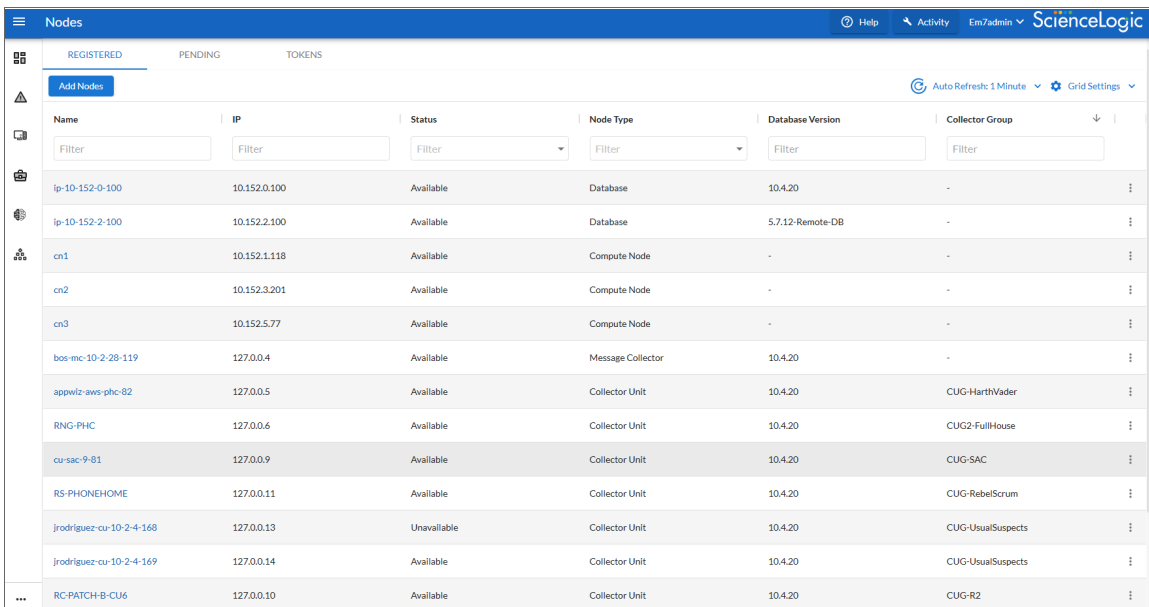
- `<uuid>` is the unique ID of the request.
- `<model_type>` is either a `cu` for a Data Collector or `mc` for a Message Collector.
- `<name>` is the name of the PhoneHome collector. You can use any name you want.
- `<CUG_ID>` is the numeric ID of a collector group from SL1 to which you want to assign this collector.
- `<description>` is the descriptive text about the collector.
- `<one_time_secret>` is the secret generated when sending a request from the collector.

Managing the Nodes Page

The following topics describe how to use and add information on the **Nodes** page.

Viewing the List of Registered Nodes

The **[Registered]** tab of the **Nodes** page lets you manage the nodes used for installing SL1 collectors, SL1 instances, and other related appliances. You can also click the **[Add Node]** button to connect an SL1 collector to an SL1 Database Server.



The screenshot shows the 'Nodes' page in the ScienceLogic interface. The 'REGISTERED' tab is active, displaying a table of nodes. The table has columns for Name, IP, Status, Node Type, Database Version, and Collector Group. The nodes listed include Database nodes, Compute Nodes, and Collector Units, each with their respective IP addresses and statuses.

Name	IP	Status	Node Type	Database Version	Collector Group
ip-10-152-0-100	10.152.0.100	Available	Database	10.4.20	-
ip-10-152-2-100	10.152.2.100	Available	Database	5.7.12-Remote-DB	-
cn1	10.152.1.118	Available	Compute Node	-	-
cn2	10.152.3.201	Available	Compute Node	-	-
cn3	10.152.5.77	Available	Compute Node	-	-
bos-mc-10-2-28-119	127.0.0.4	Available	Message Collector	10.4.20	-
appwiz-aws-phc-82	127.0.0.5	Available	Collector Unit	10.4.20	CUG-HarthVader
RNG-PHC	127.0.0.6	Available	Collector Unit	10.4.20	CUG2-FullHouse
cu-sac-9-81	127.0.0.9	Available	Collector Unit	10.4.20	CUG-SAC
RS-PHONEHOME	127.0.0.11	Available	Collector Unit	10.4.20	CUG-RebelScrum
Jrodriguez-cu-10-2-4-168	127.0.0.13	Unavailable	Collector Unit	10.4.20	CUG-UsualSuspects
Jrodriguez-cu-10-2-4-169	127.0.0.14	Available	Collector Unit	10.4.20	CUG-UsualSuspects
RC-PATCH-B-CU6	127.0.0.10	Available	Collector Unit	10.4.20	CUG-R2

The **[Pending]** tab displays a list of pending requests for establishing a connection between a collector and an SL1 Database Server. The **[Tokens]** tab displays a list of existing and expired tokens used for connecting collectors.

The **[Pending]** tab and the **[Tokens]** tab do not display on an All-In-One SL1 system.

NOTE: The **Nodes** page replaces some of the functionality previously found in the Web Configuration utility and the **Appliance Manager** page.

TIP: You can filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see "Filtering Inventory Pages" in the *Introduction to SL1* manual.

By default, the **Nodes** page displays the following about each node:

- **Name.** Name of the node.
- **IP .** Primary IP address for the node.
- **Status.** The node status types include:
 - Available
 - Unavailable
 - Failed Over
 - Available Failed Over
 - Unconfigured
 - Unlicensed
- **Node Type.** The node types include:
 - All-In-One Appliance
 - Application Server (Administration Portal)
 - Compute Node
 - Collector Unit (Data Collector)
 - Database Server
 - Message Collector
 - Storage Node

- **Database Version.** Version number of the Database Server for an All-In-One Appliance or a Database Server node.
- **Collector Group .** For Data Collectors and All-In-One Appliances, specifies the Collector Group name associated with the node.

In addition, you can click the **[Grid Settings]** button and select *Column Preferences* to add the following columns to the **Nodes** page:

- **Node ID.** Unique numeric ID, automatically assigned by SL1 to each node on the **Nodes** page.
- **Capacity.** For Database Servers, specifies the licensed capacity of the node.
- **Description.** Description of the node.
- **Patch Level.** Most recent patch version number for the node, where applicable.
- **Release Version.** SL1 version running on the node.
- **Version ID.** Unique numeric ID, automatically assigned by the platform to each SL1 version.
- **Created.** Date and time the node was registered and licensed.
- **Edit User.** User who last edited the node's information.
- **Last Edited.** Date the node's information was discovered or last edited.
- **Task Manager Paused.** Specifies whether the task manager service is paused. This value is updated every two minutes.
- **Needs Reboot.** Specifies whether the node requires reboot to add latest kernel or security updates.
- **Allocation.** For Data Collectors, specifies the number of devices aligned with the node.
- **Endpoint.** SL1 Agent endpoint for the Gen 1 Agent.
- **Collector Group ID.** For Data Collectors and All-In-One Appliances, specifies the Collector Group ID associated with the node.

Viewing the Tokens on the Nodes Page

The **[Tokens]** tab on the **Nodes** page lists the existing and expired tokens that get used when connecting a collector. A **token** is a JSON web token (JWT) that contains a set of secure data that SL1 uses to establish communication between the new SL1 Collector and the SL1 Database Server.

By default, tokens for a "Collector Initiates | System Accepts" connection type have a 30-minute expiration period.

The **[Tokens]** tab lists the following:

- Collector registration details entered by the user at the time of token creation (collector hostname, description)
- Collector type (Data Collector or Message Collector) and aligned Collector Group
- Details about the token (including its type, date of creation, and expiration date)

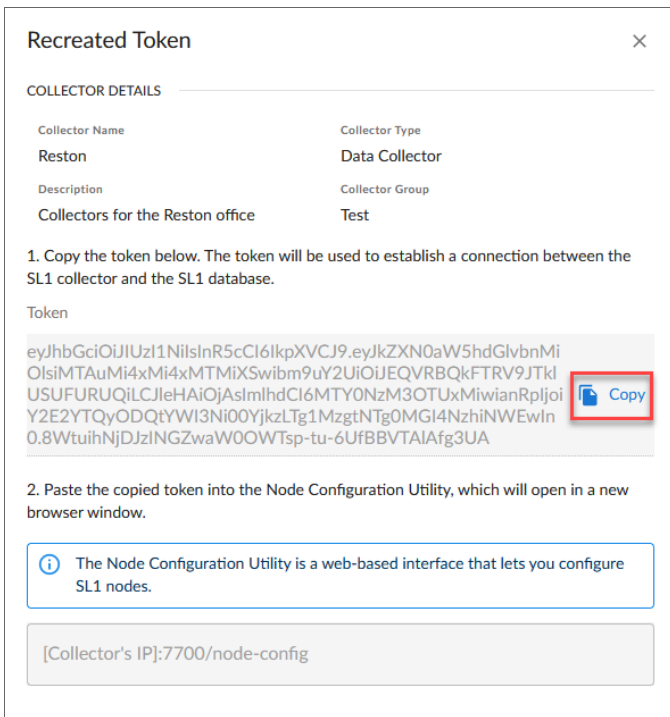
A token inherits organization membership from the Collector Group to which it is aligned to allow multi-tenancy.

Recreating a Token

Expired tokens cannot be recovered on the **[Tokens]** tab, but you can recreate an expired token, which lets you generate a new token with the same collector details. Recreating the token actually deletes the existing token, but retains the user-supplied collector registration details to use in the new token.

To recreate an expired token:

1. Go to the **[Tokens]** tab on the **Nodes** page (Manage > Nodes).
2. Click the **Actions** menu (⚙) and select *Recreate* for the expired token. The **Recreated Token** window appears:





3. Click the **[Copy]** button to copy the token, and then paste the copied token into the Node Configuration Utility.

Installing SL1 on Hardware Appliances and Virtual Appliances

Overview

This chapter describes how to install SL1 on hardware Appliances or on virtual machines.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (.
- To view a page containing all of the menu options, click the Advanced menu icon ().

This chapter covers the following topics:

<i>Prerequisites</i>	53
<i>Upgrading</i>	53
<i>Installing the Database Server</i>	53
<i>Installing the Administration Portal, Data Collector and/or Message Collector</i>	54
<i>Licensing the SL1 Appliances</i>	55
<i>Additional Steps for SL1 10.1</i>	55

Prerequisites

To perform the steps in this section:

- You must have already performed the prerequisites for all the [ScienceLogic Hardware Appliances](#) in your SL1 stack or for all the [Virtual Appliances](#) in your SL1 stack.
- You must have a valid customer account that allows you to download the SL1 ISO. For details, contact your Customer Success Manager.
- You must download the SL1 ISO.
- Mount the SL1 ISO on each virtual appliance.
- You must have access to the files for your SSL certificate.
- You must have a valid customer account that allows you to access the Artifactory page on the ScienceLogic Support Site. For details, contact your Customer Success Manager.

CAUTION: ScienceLogic does not support vmotion or VMware Snapshots for backups of data. For backup purposes, ScienceLogic supports only SL1 backups to remote storage. vmotion and VMware Snapshots can cause SL1 outages. For details on SL1 backups, see the chapter on *Backup Management* in the *System Administration* manual.

Upgrading

For detailed upgrade instructions, see the chapter on *Upgrading SL1*, in the *System Administration* manual.

Installing the Database Server

In SL1 version 12.1.0, a new Oracle Linux 8 (OL8)-compatible installation wizard was added to the SL1 ISO file. All new SL1 12.1.0 installations from the ISO file will include OL8 by default.

NOTE: After you deploy the ISO version of SL1 12.1.0, you might get an "Appliance is not licensed" message on the login page. This situation only occurs if you use another tab or browser to log in to the SL1 environment after deployment. If you use the same browser or tab that you used for the deployment, the user interface will be available.

The Database Server should be the first node or appliance you install. To do so:

1. Boot the appliance from the SL1 ISO. The Installation window appears.

NOTE: If you are using Hyper-V, check that the ScienceLogic installation ISO mounted correctly and that the Virtual Machine displays the install screen. To do this, right-click the Virtual Machine in inventory and select *Connect or View* and then *Connect via Console*.

2. Select **Install EM7**. The **Model Type** window appears.
3. Select **Database**. Select **[Continue]**.
4. In the **Database** window, select **Local Database** and select **[Continue]**.
5. After the installer for the selected appliance type is loaded, the **Network Configuration** window appears.
6. Enter the following information:
 - **IP Address**. Type the primary IP address of the node or appliance.
 - **Netmask**. Type the netmask for the primary IP address of the node or appliance.
 - **Gateway**. Type the IP address for the network gateway.
 - **DNS Server**. Type the IP address for the primary Nameserver.
 - **Hostname**. Type the hostname for the node or appliance.
7. Select **[Continue]**.
8. The **System Password** window appears.
11. Type the password for the em7admin user on the operating system and select **[Continue]**.
12. Type the password for the em7admin user again and select **[Continue]**.
13. The appliance installer runs, and the virtual machine reboots automatically, and you are returned to a login prompt.
14. If you are using a VMware instance, after the appliance reboots, follow the instructions to [install VMware tools](#).
15. If the Database Server is running a version of SL1 before 11.2.0, [follow the instructions to license the appliance](#).
16. Repeat these steps for the remaining nodes or appliances: the Administration Portal, the Data Collectors, and the Message Collectors (if applicable).

Installing the Administration Portal, Data Collector and/or Message Collector

WARNING: Starting with SL1 version 11.2.0, the installation process for SL1 Collectors was updated. For detailed procedures for installing a collector, see [Installing and Configuring an SL1 Collector](#).

After installing the Database Server, you can next install:

1. The Administration Portal (if applicable)
2. The Data Collectors
3. The Message Collectors (if applicable)

You can use the following instructions to build the Administration Portal, and one or more Data Collectors and Message Collectors.

1. Boot the appliance from the SL1 ISO.
2. Select **Install EM7**. The **Model Type** window appears.
3. Select the appropriate appliance type. Select **[Continue]**.
4. After the installer for the selected appliance type is loaded, the **Network Configuration** window appears.
5. Enter the following information:
 - **IP Address**. Type the primary IP address of the appliance.
 - **Netmask**. Type the netmask for the primary IP address of the appliance.
 - **Gateway**. Type the IP address for the network gateway.
 - **DNS Server**. Type the IP address for the primary Nameserver.
 - **Hostname**. Type the hostname for the appliance.
6. Select **[Continue]**.
7. The **System Password** window appears.
8. Type the password for the em7admin user on the operating system and select **[Continue]**.
9. Type the password for the em7admin user again and select **[Continue]**.
10. If you are using a VMware instance, after the appliance reboots, follow the instructions to [install VMware tools](#).
11. [Follow the instructions to configure the appliance in the Web Configuration Tool](#).

Licensing the SL1 Appliances

For details on licensing the SL1 Appliances, see the chapter [Licensing and Configuring an Appliance](#).

Additional Steps for SL1 10.1

SL1 10.1.x included an upgrade to MariaDB. The upgrade did not include a tool, jemalloc, that helps manage memory usage.

NOTE: This section applies only to the following releases:

- 10.1.0
- 10.1.1
- 10.1.2
- 10.1.3
- 10.1.4
- 10.1.4.1
- 10.1.4.2
- 10.1.5
- 10.1.5.1

For SL1 versions later than 10.1.5.1, jemalloc is included with the platform. For SL1 versions prior to 10.1.0, jemalloc is included with the platform.

To avoid problems with memory usage on Database Servers, perform the following steps after upgrading MariaDB for 10.1.x.

NOTE: Perform these steps first on the active Database Server and then on each additional Database Server in your SL1 System.

1. Open an SSH session to the Database Server.
2. To verify that the Database Server is not currently running jemalloc, enter the following command at the shell prompt:

```
silosql -e 'show global variables like "version_malloc_library"'
```

If the Database Server is not currently running jemalloc, the shell will display the following:

Variable Name	Value
version_malloc_library	system

3. Search for the file `/usr/lib64/libjemalloc.so.1`.

If the file does not exist, contact ScienceLogic Customer Support to request the file `jemalloc-3.6.0-1.el7.x86_64.rpm`.

To install the RPM, use a file-transfer utility, copy the file to a directory on the SL1 appliance. Then enter the following commands at the shell prompt:

```
cd /usr/lib64
sudo yum install jemalloc-3.6.0-1.el7.x86_64.rpm
```


4. Create the file `/etc/systemd/system/mariadb.service.d/jemalloc.conf`, as follows:

```
vi /etc/systemd/system/mariadb.service.d/jemalloc.conf
```

5. Add the following lines to the file:

```
[Service]
Environment="LD_PRELOAD=/usr/lib64/libjemalloc.so.1"
```

6. Save and close the file.
7. Reload the systemd config files with the following command:

```
sudo systemctl daemon-reload
```

8. Restart the Database Server:

To restart the **standalone Database Server** or the **primary Database Server in a cluster**, enter the following:

```
sudo systemctl restart mariadb
```

To restart each **secondary Database Server in a cluster**:

- a. Open an SSH session to the secondary Database Server. At the shell prompt, enter:

```
coro_config
```

- b. Select **1**.
- c. When prompted to put the Database Server into maintenance, select **y**.
- d. Open an SSH session to the primary Database Server. To pause SL1, enter the following command at the shell prompt:

```
sudo touch /etc/.proc_mgr_pause
```

- e. In the SSH session for the secondary Database Server, restart MariaDB:

```
crm resource restart mysql
```

- f. After MariaDB has restarted successfully on the secondary Database Server, return to the SSH session on the primary Database Server. Remove the pause file for SL1 using the following command:

```
sudo rm /etc/.proc_mgr_pause
```

- g. In the SSH session on the secondary Database Server, take the Database Server out of maintenance. At the shell prompt, enter:

```
coro_config
```

- h. Select **1**.
- i. When prompted to take the Database Server out of maintenance, select **y**.

9. To verify that jemalloc is running on the Database Server, enter the following command at the shell prompt:

```
siilo_mysql -e 'show global variables like "version_malloc_library"'
```

If the Database Server is currently running jemalloc, the shell will display something like the following:

Variable Name	Value
version_malloc_library	jemalloc 3.6.0-0-g46c0af68bd248b04df75e4f92d5fb804c3d75340

10. Perform these steps on each Database Server in your SL1 system.

Licensing and Configuring an Appliance

Overview

This chapter describes how to license an SL1 appliance and add an SL1 appliance to your SL1 system.

There are two utilities you can use to perform various functions for the setup and editing of your SL1 appliance.

These two utilities include:

- The Classic Web Configuration Utility (default)
- The Node Configuration Application

Upon installation, SL1 appliances are automatically licensed for 90 days, with a capacity of 1,000 devices. During these 90 days, you can perform the steps to obtain a permanent license from ScienceLogic.

SL1 appliances automatically generate a Registration Key file. This file is used by ScienceLogic to generate a unique License Key file. **You must not edit or alter the Registration Key file.** While performing the steps described in this chapter, you must obtain a License Key file by providing the Registration Key file to ScienceLogic.



For distributed SL1 systems, you **must** license the Database Server first. All other SL1 appliances in a distributed SL1 system depend on the Database Server for registration. Be sure to license your appliances before using the latest release of SL1.

NOTE: In SL1 version 11.2.0, the **Licensing** pages were removed from the Web Configuration Utility. However, this inadvertently caused several issues, including an inability to license Database Server and All-In-One Appliances and, in some cases, an inability to log in to the SL1 user interface.

The **Licensing** page was restored in SL1 version 11.3.1. If you are using a version between 11.2.0 and 11.3.1, you might still experience the above issues. If you do, contact ScienceLogic Support.

For more information, including if you get an "Appliance is not licensed" error message, see Knowledge Base article: <https://support.sciencelogic.com/s/article/9617>.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ().
- To view a page containing all of the menu options, click the Advanced menu icon ().

This chapter covers the following topics:

<i>Navigating the Classic Web Configuration Utility</i>	61
<i>Licensing and Configuring a Database Server or All-In-One Appliance</i>	62
<i>Navigating the Node Configuration Utility</i>	73

Navigating the Classic Web Configuration Utility

The default utility application for configuring your appliance is the Classic Web Configuration Utility. This utility allows you to perform many different functions surrounding the configuration of your appliance.

In the Classic Web Configuration Utility, you can:

- Configure an Administration Portal
- Configure a Data Collector or Message Collector
- Register the Data Collector or Message Collector with the Database Server
- Define a Syslog, NTP, and/or Proxy Server(s)
- Create a Bonded Interface

Logging into the Classic Web Configuration Utility

Perform the following steps to log in to the Web Configuration Utility:

1. You can log in to the Web Configuration Utility using any web browser supported by SL1. The address of the Web Configuration Utility is in the following format:

```
https://<ip-address-of-appliance>:7700
```

NOTE: For AWS instances, *ip-address-of-appliance* is the public IP for the AWS instance. To locate the public IP address for an AWS instance, go to AWS, go to the **Instances** page, and highlight an instance. The **Description** tab in the lower pane will display the public IP.

2. When prompted to enter your user name and password, log in as the "em7admin" user with the appropriate password.
3. After logging in, the main **Configuration Utility** page appears.

NOTE: In SL1 version 11.2.0, the **Licensing** pages were removed from the Web Configuration Utility. However, this inadvertently caused several issues, including an inability to license Database Server and All-In-One Appliances and, in some cases, an inability to log in to the SL1 user interface.

The **Licensing** page was restored in SL1 version 11.3.1. If you are using a version between 11.2.0 and 11.3.1, you might still experience the above issues. If you do, contact ScienceLogic Support.

For more information, including if you get an "Appliance is not licensed" error message, see Knowledge Base article: <https://support.sciencelogic.com/s/article/9617>.

Changing the Password for the Classic Web Configuration Utility

If you want to change the password for the Web Configuration Utility on all SL1 appliances, you must log in to the Web Configuration Utility on each node or appliance and perform the steps in this section.

You cannot change the username for the Web Configuration Utility. The username remains **em7admin**.

To change the password for the Web Configuration Utility:

1. Log in to the Web Configuration Utility. The **Configuration Utilities** page appears.
2. Click the **[Device Settings]** button. The **Settings** page appears.
3. In the **Settings** page, type the following:
 - **Web Config Password (change only)**. Type the new password.
 - **Confirm Web Config Password**. Type the new password again.
4. Click **[Save]**.
5. Perform steps 1-4 for each node or appliance for which you want to change the password for the Web Configuration Utility.

Licensing and Configuring a Database Server or All-In-One Appliance

NOTE: In SL1 version 11.2.0, the **Licensing** pages were removed from the Web Configuration Utility. However, this inadvertently caused several issues, including an inability to license Database Server and All-In-One Appliances and, in some cases, an inability to log in to the SL1 user interface.

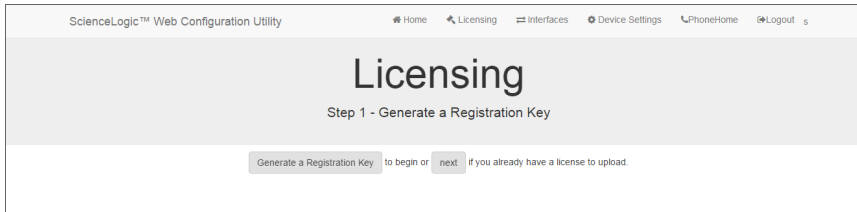
The **Licensing** page was restored in SL1 version 11.3.1. If you are using a version between 11.2.0 and 11.3.1, you might still experience the above issues. If you do, contact ScienceLogic Support.

For more information, including if you get an "Appliance is not licensed" error message, see Knowledge Base article: <https://support.sciencelogic.com/s/article/9617>.

You must perform the following steps in the Web Configuration Utility to license an All-In-One Appliance or Database Server:

1. Log in to the Web Configuration Utility by navigating to `https://<ip-address-of-appliance>:7700` and entering your credentials. The **Configuration Utilities** page appears.

2. Click the **[Licensing]** button. The **Licensing Step 1** page appears.



3. In the **Licensing Step 1** page, click the **[Generate a Registration Key]** button.
4. When prompted, save the Registration Key file to your local disk.
5. Log in to the ScienceLogic Support Site (<https://support.sciencelogic.com>).
 - Click your user name and from the menu select **My Support and Customer Success**.
 - On the next page, click the **[Submit a License Request]** button.
 - Fill out the **Appliance Information** form and click the **[Submit License Request]** button.
 - In the **Upload Appliance Registration Key** field, click the **[Upload Files]** button and navigate to the file where you saved the Registration Key file.
 - ScienceLogic Customer Support will generate a license for the All-In-One Appliance or Database Server.
6. When you have the license for the All-In-One Appliance or Database Server, return to the Web Configuration Utility.
7. In the **Licensing Step 2** page, click the **[Upload]** button to upload the license file.
8. After navigating to and selecting the license file, click the **[Submit]** button to finalize the license. If the license key is correct and has been saved successfully, the message "Success: Thank you for licensing your ScienceLogic product!" appears.

Configuring an Administration Portal

You must perform the following steps in the Web Configuration Utility to configure an Administration Portal:

1. Log in to the Web Configuration Utility by navigating to <https://<ip-address-of-appliance>:7700> and entering your credentials. The **Configuration Utilities** page appears.
2. Click the **[Device Settings]** button in the upper-right of the page. The **Settings** page appears.

3. On the **Settings** page, enter the following:


- **Database IP Address.** The IP address(es) of the primary ScienceLogic Database Server(s). If this is a High Availability or Disaster Recovery (HA/DR) system, use the Virtual IP address in this field.
 - For an All-In-One Appliance with multiple Administration Portals, enter the IP address for the All-In-One Appliance.
 - If the Administration Portal and Database Server are AWS instances, supply the private IP address for the Database Server. To find the private IP of an AWS instance, go to AWS, go to the **Instances** page, and highlight an instance. The **Description** tab in the lower pane will display the private IP.
- **Database Username.** Username for the database account that the Administration Portal will use to communicate with the Database Server.
- **Accept the default values in all other fields.**

4. Click the **[Save]** button. You may now log out of the Web Configuration Utility.

5. In SL1, go to the **Appliance Manager** page (System > Settings > Appliances).

6. Supply values in the following fields:

- **Host Name.** Enter the hostname of the Administration Portal, where relevant.
- **IP Address.** Enter the IP address of the Administration Portal. If this is a High Availability or Disaster Recovery (HA/DR) system, use the Virtual IP address in this field. If the Administration Portal is an AWS instance, supply the private IP address for the Administration Portal. To find the private IP of an AWS instance, go to AWS, go to the **Instances** page, and highlight an instance. The **Description** tab in the lower pane will display the private IP.
- **Model Type.** Select *Administration Portal [3]* from the drop-down list.
- **Description.** Enter a description of the Administration Portal. This field is optional.

6. Click the **[Save]** button. If the save is successful, the message "Appliance Registered" appears.
7. If you are using an AWS RDS system, select the wrench icon () for the newly created Administration Portal. Supply values in the **DB User** field and the **DB Password** field.
8. If all information is valid and the Database Server can communicate with the Administration Portal, the appliance page will display "Yes" in the **Validated** column. If the **Validated** column displays "No" for longer than five minutes, double-check your settings and network connection.

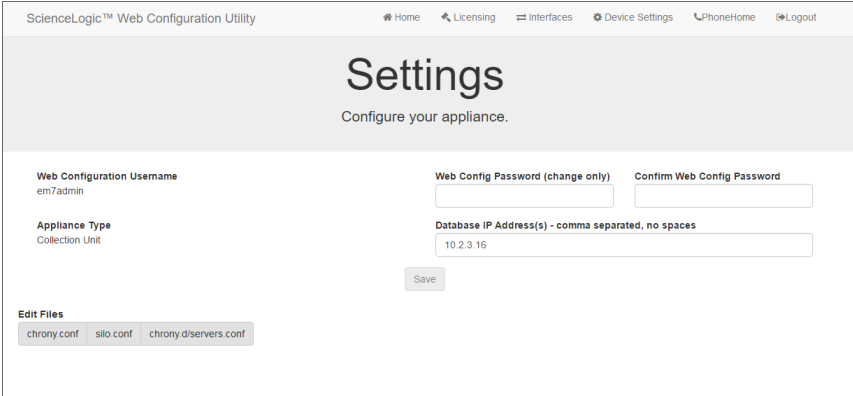
Configuring a Data Collector or Message Collector

NOTE: The instructions for configuring a Data Collector or Message Collector for PhoneHome configuration differ from the instructions in this section. For details on configuring a Data Collector or Message Collector for PhoneHome configuration, see the chapter on [PhoneHome](#).

NOTE: If you are configuring a Data Collector or a Message Collector using SL1 version 11.2.0 or later, skip the procedures in this section and go to [Installing and Configuring an SL1 Collector](#).

You must perform the following steps in the Web Configuration Utility to configure a Data Collector or a Message Collector:

1. [Log in to the Web Configuration Utility](#) on the Data Collector or the Message Collector. The **Configuration Utilities** page appears.
2. Click the **[Device Settings]** button. The **Settings** page appears.



ScienceLogic™ Web Configuration Utility

Home Licensing Interfaces Device Settings PhoneHome Logout

Settings

Configure your appliance.

Web Configuration Username: em7admin

Web Config Password (change only):

Confirm Web Config Password:

Appliance Type: Collection Unit

Database IP Address(s) - comma separated, no spaces: 10.2.3.16

Save

Edit Files

chrony.conf silo.conf chrony d/servers.conf

3. In the **Settings** page, update the following field:

- **Database IP Address.** The IP address of the ScienceLogic Database Server(s). If more than one Database Server will manage this appliance, type the IP addresses of the Database Servers, separated by commas. If the Data Collector or the Message Collector and the Database Server are AWS instances, supply the private IP address for the Database Server. To find the private IP of an AWS instance, go to AWS, go to the **Instances** page, and highlight an instance. The **Description** tab in the lower pane will display the private IP.

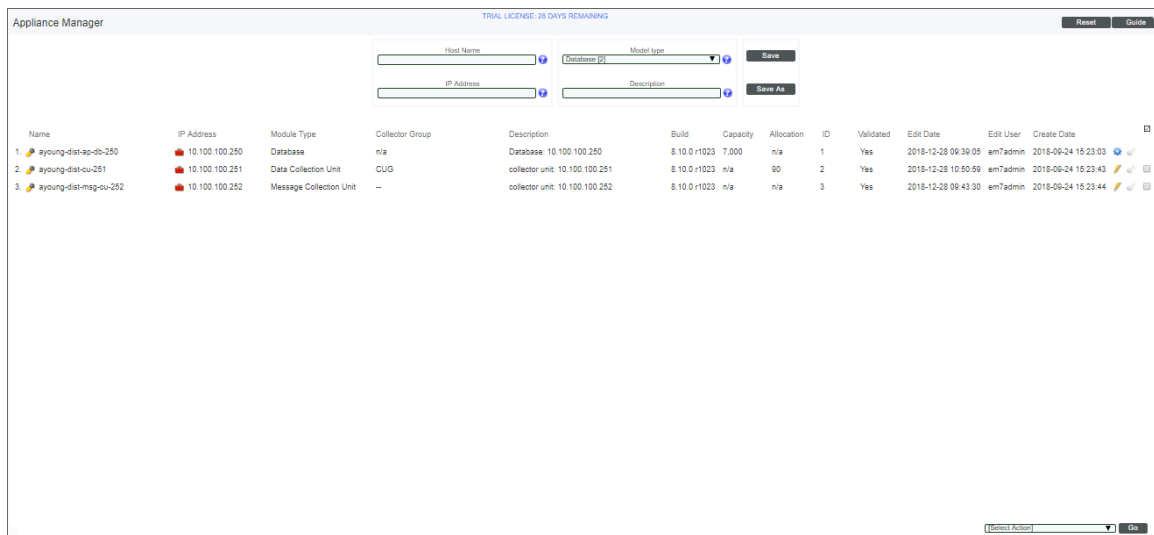
4. Click the **[Save]** button. You may now log out of the Web Configuration Utility.
5. Perform these steps for each Data Collector and Message Collector in your PhoneHome configuration.

Registering the Data Collector or Message Collector with the Database Server

After configuring a Data Collector or Message Collector in the Web Configuration Utility, you must register the appliance with the main Database Server in your SL1 system.

To register a Data Collector or Message Collector with the main Database Server, perform the following steps:

1. In the address bar of your browser, type the IP address of the SL1 appliance that provides the user interface for your SL1 system. The user interface is provided by either the Database Server or an Administration Portal. The login screen appears.
2. Log in as the "em7admin" user with the appropriate password.
3. If this is your first successful login, you will be asked to agree to the End-user License Agreement. Read the End-user License Agreement then click the **[I Agree to The Terms Outlined Above]** button.
4. Go to the **Appliance Manager** page (System > Settings > Appliances):

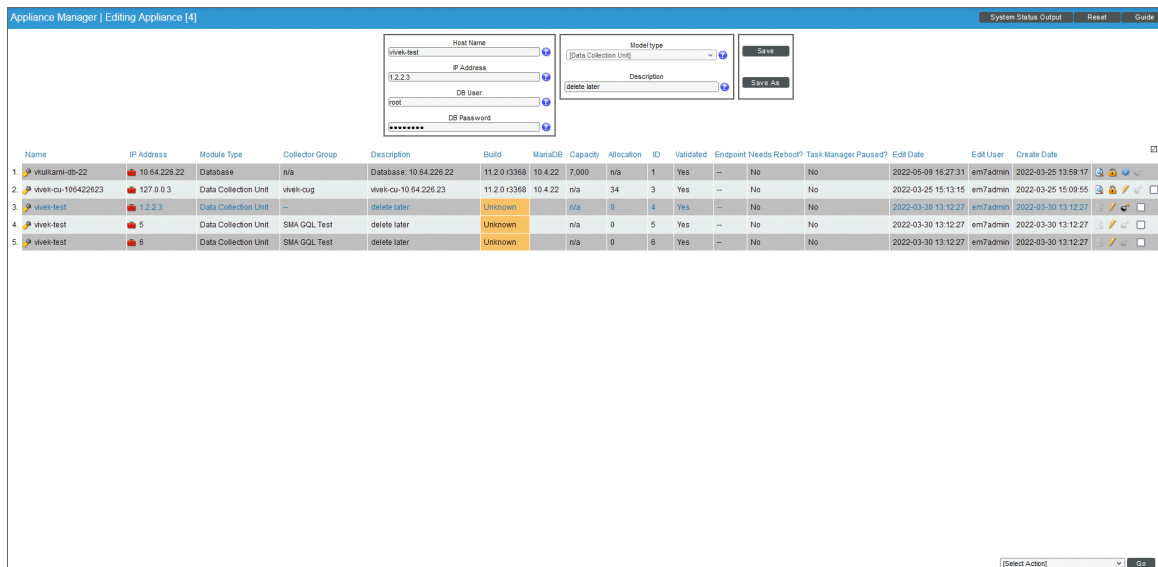


5. Supply values in the following fields:

- **Host Name.** Enter the hostname of the Data Collector or Message Collector.
- **IP Address.** Enter the IP address of the Data Collector or Message Collector. If the Data Collector or the Message Collector are AWS instances, supply the private IP address for the Data Collector or the Message Collector. To find the private IP of an AWS instance, go to AWS, go to the **Instances** page, and highlight an instance. The **Description** tab in the lower pane will display the private IP.
- **Model Type.** If you are configuring a Data Collector, select *Data Collection Unit [5]* from the drop-down list. If you are configuring a Message Collector, select *Message Collection Unit [6]* from the drop-down list.
- **Description.** Enter a description for the Data Collector or Message Collector. This field is optional.

6. Click the **[Save]** button. If the save is successful, the message "Appliance Registered" appears.

7. If you are using an AWS RDS system, select the wrench icon (🔧) for the newly created Data Collector or Message Collector. Supply values in the **DB User** field and the **DB Password** field.



8. If all information is valid and the Database Server can communicate with the Data Collector or Message Collector, the appliance page will display "Yes" in the **Validated** column. If the **Validated** column displays "No" for longer than five minutes, double-check your settings and network connection.

Defining the Syslog Server

WARNING: This method of defining the syslog server was deprecated in SL1 version 11.3.0 and later. For more information on the new method of defining the syslog server, see [Logging in SL1 Version 11.3.0 and Later](#).

For each device except for Message Collectors and All-In-One Appliances, you must specify the IP address of the server to which the SL1 appliance will send syslog messages. Enter the IP address of the syslog server that will monitor this SL1 appliance. Usually, this is the IP address of a Message Collector, Data Collector, or All-In-One Appliance.

NOTE: A device configured with Transport Layer Security (TLS) support for an rsyslog server can successfully exchange messages with a SL1 appliance configured with TLS support for an rsyslog client.

To specify the syslog server:

1. Either go to the console of the SL1 appliance or use SSH to access the server.
2. Log in as user **em7admin** with the password you configured during setup.
3. Install the required Transport Layer Security (TLS) certificates by typing the following lines at the shell prompt:

```
mkdir -pv /etc/rsyslog.d/keys/ca.d
```

```
cd /etc/rsyslog.d/keys/ca.d/
```

NOTE: You might need to create a **ca.d** directory to contain the certificates needed for TLS encryption.

4. To define the syslog server, type the following at the shell prompt:

```
sudo vi /etc/rsyslog.d/siteconfig.conf
```

5. On a line of its own, add the following entry:

```
facility.priority@ip address of syslog server
```

where:

- *facility* specifies a valid facility value. These categories provide a general description of the originator of the message.
- *priority* specifies a valid priority value. These values specify severity.
- *ip address of syslog server* specifies the IP address of the syslog server that will monitor this SL1 appliance, usually a Data Collector or Message Collector.

NOTE: For details on valid facility and priority values, see https://docs.oracle.com/cd/E37670-01/E36387/html/ol_log_sec.html.

6. Save your changes and exit the file (:wq).
7. At the command line, type the following:

```
sudo service rsyslog restart
```

- Repeat steps 1-7 on each SL1 appliance in your system.

Defining the NTP Server

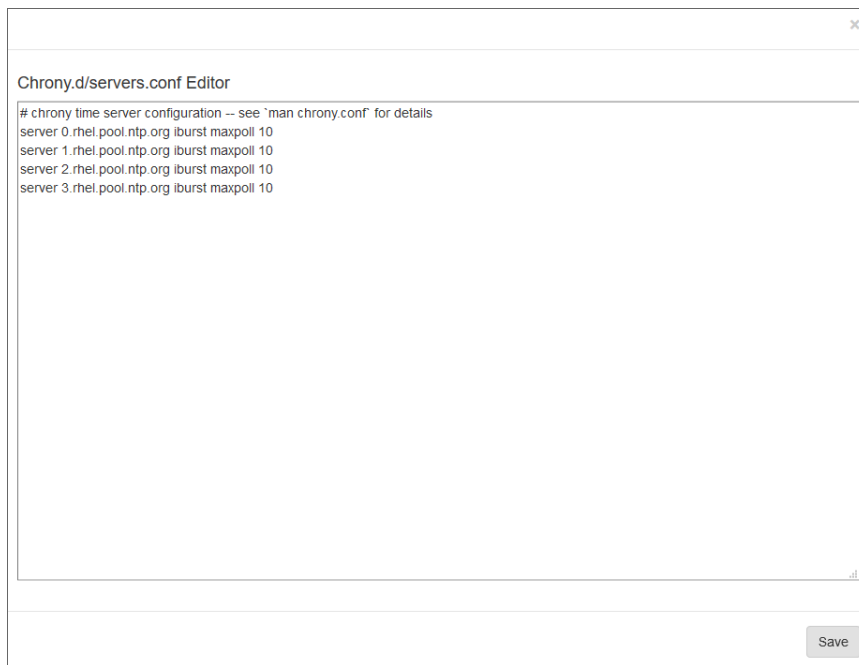
By default, SL1 uses the time servers in the Red Hat Linux pool of time servers. If you want to use a different time server, you can edit the configuration files for the time server.

From the **Device Settings** page of the Web Configuration Utility, you can edit the following time server files:

- **chrony.d/servers.conf**. This configuration file contains additional settings for the various chrony time servers.
- **chrony.conf**. This configuration file contains settings related to the time server (chrony.d) used by SL1.

To configure a time server file:

- Log in to the Web Configuration Utility. The **Configuration Utilities** page appears.
- Click the **[Device Settings]** button. The **Settings** page appears.
- In the Edit Files section, click **chrony.d/servers.conf**. The **Chrony.d/servers.conf Editor** modal appears:



- In the Chrony.d/servers.conf modal page, copy the first line that begins with **server**, such as **server 0.rhel.pool.ntp.org iburst maxpoll 10**.
- Paste that line *above* the first line that begins with **server**.
- Replace the hostname portion of the line with the IP address or fully qualified domain name of your preferred time server.
- You can delete the additional lines or leave them as additional time servers.
- To save your changes, click **Save** and then close the modal window.

9. If you need to configure the time server (chrony.d) used by SL1, click **chrony.conf** in the Edit Files section of the Settings page.

Creating a Bonded Interface

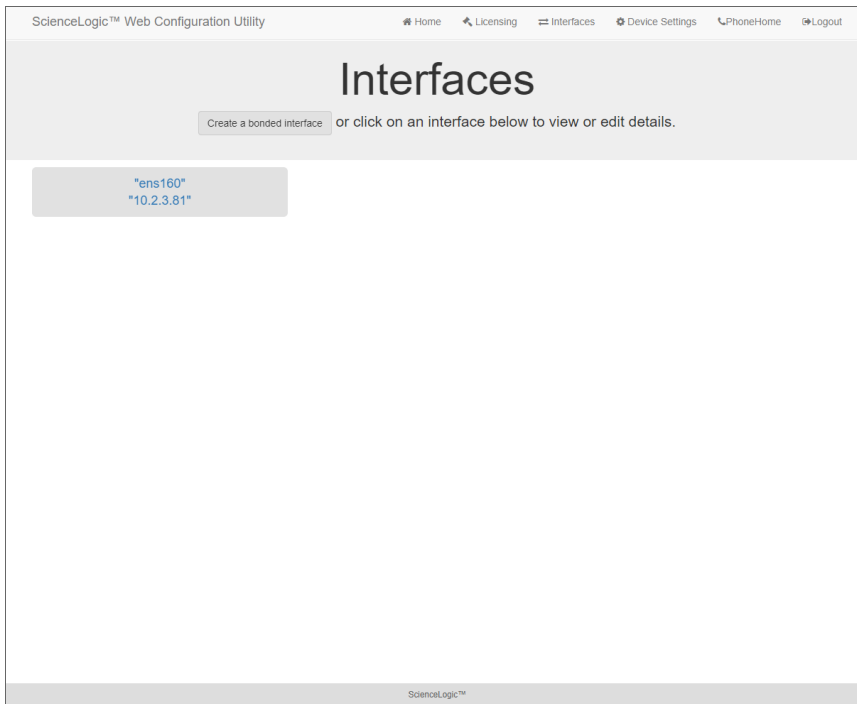
A bonded interface (also known as port trunking, channel bonding, link aggregation, and NIC teaming) allows you to combine multiple network interfaces (called "slave interfaces") into a single logical interface (called a "master interface"). A bonded interface can:

- increase available bandwidth
- provide redundancy

To the operating system, a bonded interface appears as a normal network interface. However, the bonded interface uses a round-robin protocol to assign network traffic to the slave interfaces that make up the bonded interface.

To create one or more bonded interfaces:

1. [Log in to the Web Configuration Utility](#). The **Configuration Utilities** page appears.
2. Click the **[Interfaces]** button. The **Interfaces** page appears.



- In the **Interfaces** page, click the **[Create a bonded interface]** button. The **Create a Bonded Interface** page appears.

- In the **Create a Bonded Interface** page, enter the following:

- Device ID.** Required. ID for the bonded interface. Enter a string with the format:

```
bondN
```

where **N** is a number. For example, you could enter **bond0**, **bond1**, or **bond64**.

If the device ID already exists in the SL1 System, the SL1 system will display an error message.

- Name.** Required. Enter a user name for the bonded interface.
- Interface IP Address.** Required. Enter the IP address for the bonded interface in standard IPv4, dotted-octet format.
- Netmask IP Address.** Required. Enter the netmask for the bonded interface in standard IPv4, dotted-octet format.
- Slave Interfaces.** Required. Select one or more interfaces from the list of available interfaces. The selected interfaces will be used by the new bonded interface.
- DNS1.** Optional. Enter the IP address of the DNS server that the bonded interface will use. Enter the IP address in standard IPv4, dotted-octet format.
- Gateway IP Address.** Optional. Enter the IP address of the gateway device or router that the bonded interface will use. Enter the IP address in standard IPv4, dotted-octet format.

- **IPv6 Address.** Optional. Enter the IP address for the bonded interface, in IPv6 format.
- **Bonding Options.** Optional. You can enter one or more bonding options. For each option, enter the name of the option in the *key* field and the value in the *value* field.


For details on bonding options, see the Red Hat documentation on Bonding Interface Parameters: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/sec-Specific_Kernel_Module_Capabilities.html#s3-modules-bonding-directives

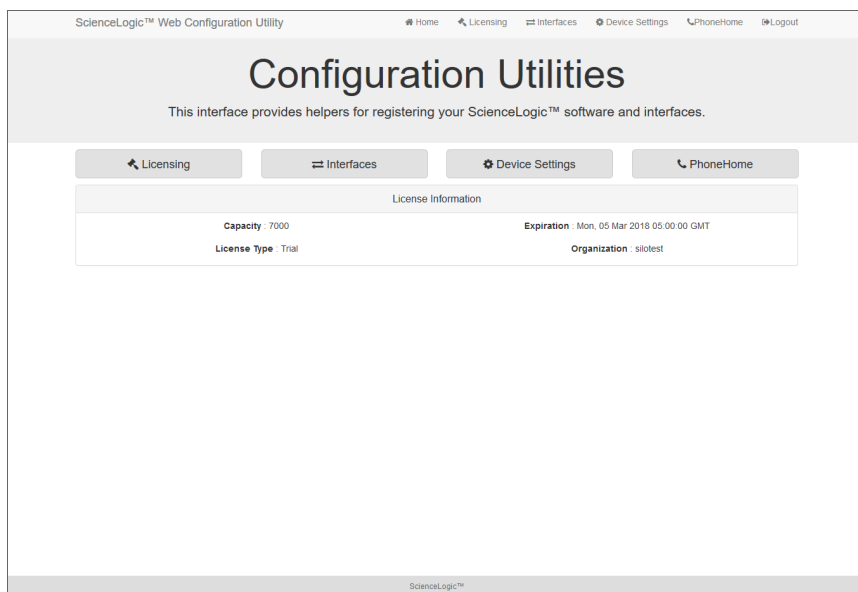
Defining a Proxy Server

A proxy server enables SL1 appliances to get system updates when the appliance does not have a direct connection to the internet. A proxy server also enables ScienceLogic Database Servers to send subscription licensing data to ScienceLogic.

Each SL1 appliance can define its own proxy server.

To define a proxy server:

1. Go to the **Appliance Manager** page (System > Settings > Appliances).
2. Find the appliance for which you want to define a proxy server. Click its toolbox icon ().
3. When prompted to enter your username and password, log in as the "em7admin" user with the appropriate password.
4. After logging in, the main **Configuration Utility** page appears:



5. Click the **[Device Settings]** button. The **Settings** page appears.

6. Enter values in the following fields:

- **Server URL.** Type the URL of the proxy server. For example, "http://10.2.12.51".
- **Port.** Type the port on the proxy server to which the SL1 appliance will talk.

7. Click **[Save]**.

Navigating the Node Configuration Utility

The Node Configuration Utility is the other utility application you can use to configure and edit your SL1 appliance.

In the Node Configuration Utility, you can:

- View the Collector Connection Status
- Configure the Proxy Server
- Add and edit a Bonding Interface

Logging into the Node Configuration Utility

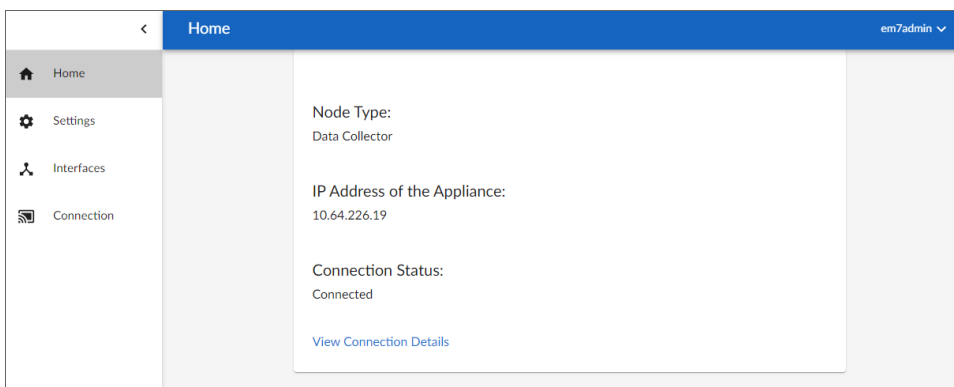
Perform the following steps to access the Node Configuration Utility:

1. You can log in to the Node Configuration Utility using any web browser supported by SL1. The address of the Node Configuration Utility is in the following format:

`https://<ip-address-of-appliance>:7700/node-config`

NOTE: For AWS instances, *ip-address-of-appliance* is the public IP for the AWS instance. To locate the public IP address for an AWS instance, go to AWS, go to the **Instances** page, and highlight an instance. The **Description** tab in the lower pane will display the public IP.

2. When prompted to enter your user name and password, log in as the "em7admin" user with the appropriate password.
3. After logging in, the main **Node Configuration Utility** home page appears:



Changing the Password for the Node Configuration Utility

If you want to change the password for the Node Configuration Utility on all SL1 appliances, you must log in to the Node Configuration Utility on each node or appliance and perform the steps in this section.

You cannot change the username for the Node Configuration Utility. The username remains **em7admin**.

To change the password for the Node Configuration Utility:

1. Log in to the Node Configuration Utility. The **Configuration Utilities** home page appears.
2. Click the drop-down arrow icon next to the username credential in the top-right corner and select **[Change Password]**.
3. On the **Change Password** page, type the following:
 - **Current Password.** Type the current password.
 - **New Password.** Type the new password.
 - **Confirm New Password.** Type the new password again.
4. Click **[Change Password]**.

Viewing the Collector Connection Status

You can view the connection status for a Data Collector from multiple places in the Node Configuration Utility. You can view connection details for both the Collector and the Database Server in the utility.

To view the collector connection status:

1. Click the **[Connection]** icon located in the left-side navigation menu of the Node Configuration Utility. The **Collector Connection Status** page appears:.

2. From this page, you can perform a few functions. You can:
 - Click **[Refresh Status]** to troubleshoot your collector's connection.
 - Click **[Disconnect & Clear Configuration]** to close the outgoing connection from this collector to all configured destinations. It will also clear all local configurations. A warning prompt will appear that asks you to confirm your action.

You can also access the **Collector Connection Status** page from the Node Configuration home page by clicking *View Connection Details* on the home page.

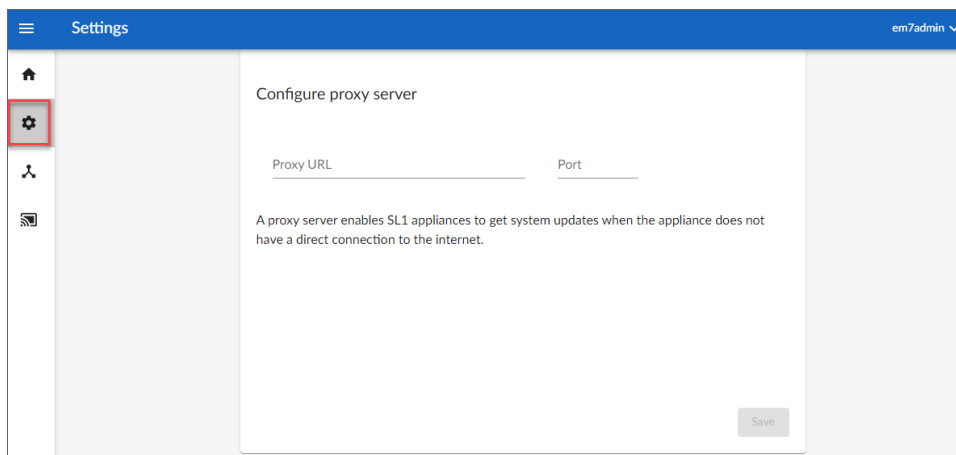
Configuring the Proxy Server from the Node Configuration Utility

A proxy server enables SL1 appliances to get system updates when the appliance does not have a direct connection to the internet. A proxy server also enables ScienceLogicDatabase Servers to send subscription licensing data to ScienceLogic.

Each SL1 appliance can configure its own proxy server.

To configure a proxy server:

1. Click the **[Settings]** icon located in the left-side navigation menu of the Node Configuration Utility.



2. Enter values in the following fields:
 - **Server URL.** Type the URL of the proxy server. For example, "http://10.2.12.51".
 - **Port.** Type the port on the proxy server to which the SL1 appliance will talk.
3. Click **[Save]**.

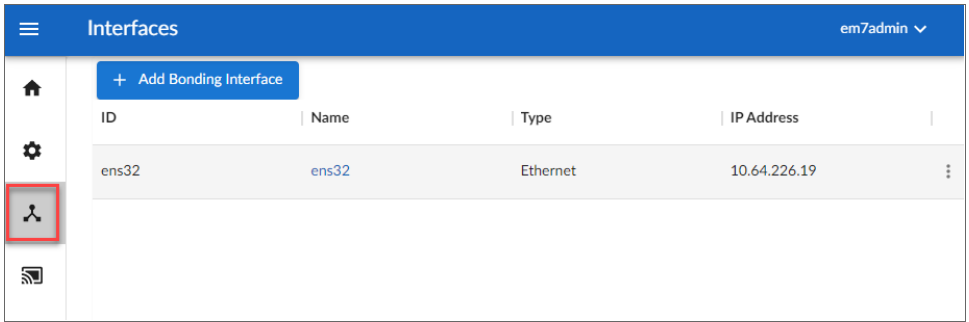
Adding a Bonded Interface from the Node Configuration Utility

A bonded interface, which is also known as port trunking, channel bonding, link aggregation, and NIC teaming, allows you to combine multiple network interfaces (called "slave interfaces") into a single logical interface (called a "master interface").

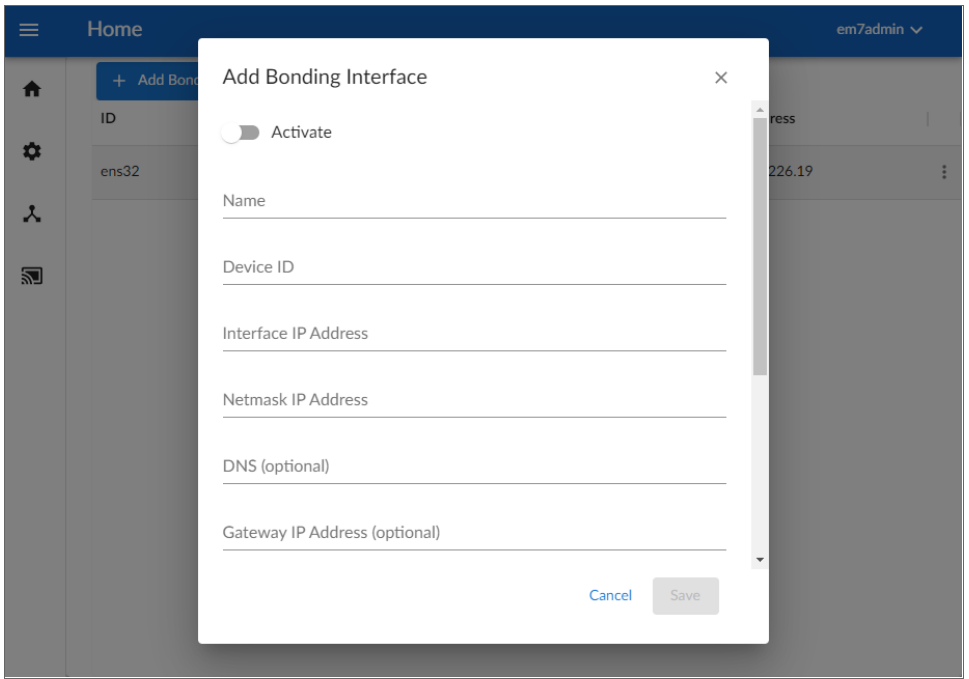
To the operating system, a bonded interface appears as a normal network interface. However, the bonded interface uses a round-robin protocol to assign network traffic to the slave interfaces that make up the bonded interface.

To add one or more bonded interfaces:

1. Click the **[Interfaces]** icon located in the left-side navigation menu of the Node Configuration Utility. The **Interfaces** page appears.



2. Click **[Add Bonding Interface]**. The **Add Bonding Interface** page appears.



3. Select the **[Activate]** button if you want this interface to be activated after you add it.
4. Complete the following fields:

- **Name**. Required. Enter a user name for the bonded interface.
- **Device ID**. Required. ID for the bonded interface.
- **Interface IP Address**. Required. Enter the IP address for the bonded interface in standard IPv4, dotted-octet format.
- **Netmask IP Address**. Required. Enter the netmask for the bonded interface in standard IPv4, dotted-octet format.
- **DNS**. Optional. Enter the IP address of the DNS server that the bonded interface will use. Enter the IP address in standard IPv4, dotted-octet format.
- **Gateway IP Address**. Optional. Enter the IP address of the gateway device or router that the bonded interface will use. Enter the IP address in standard IPv4, dotted-octet format.
- **IPv6 Address**. Optional. Enter the IP address for the bonded interface, in IPv6 format.
- **Choose Bonded Interface**. Select your bonded interface from the drop-down list.
- **Bonding Options**. Optional. You can enter one or more bonding options. For each option, enter the name of the option in the *key* field and the value in the *value* field. Click **Add Another Option** for the addition of multiple bonding options.

5. Click **[Save]**.

For details on bonding options, see the Red Hat documentation on Bonding Interface Parameters: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/sec-Specific_Kernel_Module_Capabilities.html#s3-modules-bonding-directives

Editing an Interface from the Node Configuration Utility

You can also edit an already existing bonded interface from the Node Configuration Utility.

1. From the **[Interfaces]** page, click the ellipses icon (⋮) located in the column to the right of your bonded interface.

2. Click **[Edit]**. The Interface Configuration window appears for editing.

Interface Configuration

INTERFACE

ID	Device	Name
ens32	ens32	ens32
UUID	Type	Bonding or Bonded Interface
67533061-68d5-4bed-a7b4-4c404cb8f433	Ethernet	-
Bonding Options		
-		

IP ADDRESSES

IPv4 Address	IPv4 Fatal Failure	IPv4 Default Route
10.64.226.19	no	yes
Interface IPv6 Address	Prefix	IPv6 Fatal Failure
	24	no
IPv6 Default Route	IPv6 Gen Mode	IPv6 Auto Conf
yes	stable-privacy	yes
IPv6 Router	IPv6 Forwarding	IPv6 Init
-	-	yes

CONFIGURATION AND NETWORK

DNS Address	Peer DNS	Netmask IP Address
127.0.0.1	-	
Gateway IP Address	Network Manager Controlled	On Boot
10.64.226.1	-	yes
Boot Protocol	Proxy Method	Browser Only
none	none	no

Cancel Save



3. Complete the **Interface**, **IP Address**, **Configuration**, and **Network** fields as needed for your interface.
4. Click **[Save]**.

Navigating the Setup and Config Page

Overview

This chapter describes how to navigate the **Setup and Config** page in SL1.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ().
- To view a page containing all of the menu options, click the Advanced menu icon ().

The steps to navigate the **Setup and Config** page are described throughout this chapter.

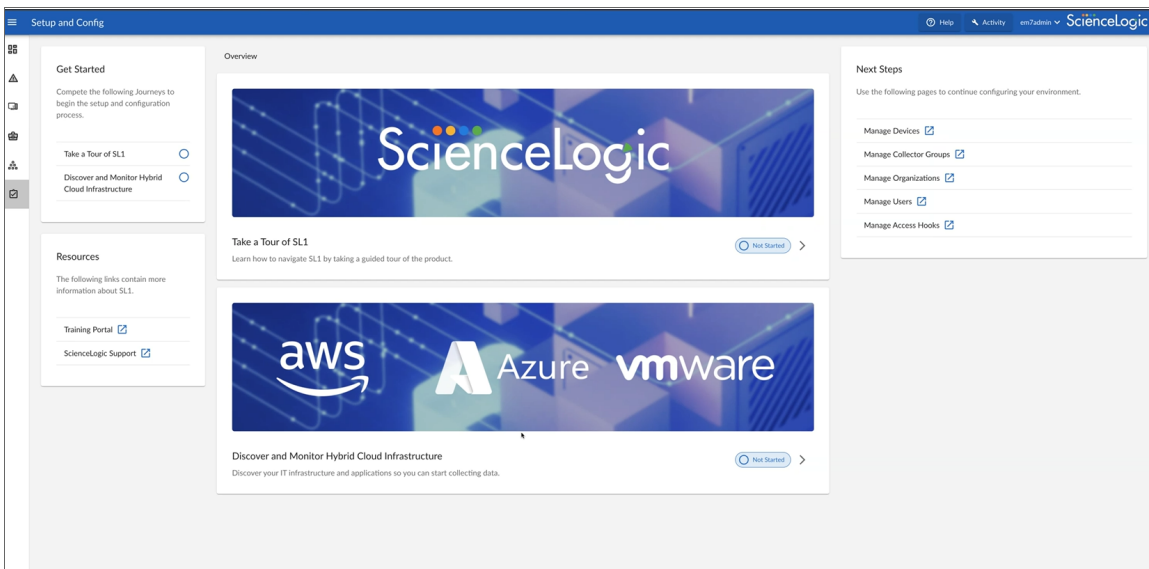
This chapter covers the following topics:

<i>What is the Setup and Config Page?</i>	81
<i>Setup and Config Journey Workflows</i>	82

What is the Setup and Config Page?

The **Setup and Config** page (📄) displays all information relevant to getting started in SL1 for administrator-level users. Included on this page are a number of intuitive self-service workflows that will guide you through the most common SL1 system tasks. You can access this page through left-hand navigation menu in SL1.

This page is designed with informational cards that provide you with the proper resources for SL1 setup and configuration.



The page's informational cards include:

- **Get Started.** Displays a list of available user journeys and their journey status.
 - Take a Tour of SL1
 - Discover and Monitor Hybrid Cloud Infrastructure
- **Resources.** Hosts additional external resources to help you with setup and configuration; these links include:
 - Training Portal
 - ScienceLogic Support
- **Overview.** Provides links to two user journeys. These journeys include guided tours and interactive wizards that help you set up and refine your SL1 environment:
- **Next Steps.** Contains links to other pages in SL1 where you can continue working after completing some or all of a journey:
 - Manage Devices

- Manage Collector Groups
- Manage Organizations
- Manage Users
- Manage Access Hooks

Setup and Config Journey Workflows

This section provides the information you need to follow the Setup and Config user journeys. You can use the Setup and Config page's journey cards as a guide to the overall SL1 setup and configuration process.

For the best experience in following the Setup and Config journeys, it is recommended that you:

1. Familiarize yourself with the SL1 product as whole by clicking through the **[Take a Tour of SL1]** journey and tracking your knowledge process with the journey's status buttons.
2. Follow the steps in the **[Discover and Monitor Hybrid Cloud Infrastructure]** journey card for a proper understanding of the setup and configuration process for your specific infrastructure. This space provides all of the information required for a successful setup in SL1 ; track your progress throughout with the journey's status buttons.

Helpful journey-card status buttons allow you to apply a specific status for an activity.

You can apply the following statuses for each journey card's individual activities:

- **[Not Started]**. This status serves as a "to-do" status for an activity that hasn't been attempted yet.
- **[In Progress]**. This status allows you to track and re-enter activities that have been started, but not completed.
- **[Complete]**. This status should be applied to any activity that is finished. You can also reset a completed workflow if you need to be guided through a workflow again. To do this, see the **Resetting a Completed Journey Workflow** section below.

IMPORTANT: A workflow can be set as **Not Applicable** if that workflow and its activities do not apply to you. This status removes that infrastructure's workflow from your "to-do" list and the workflow will not be tracked. To do this, see the **Setting a Journey Workflow as "Not Applicable"** section below.

Taking a Tour of SL1

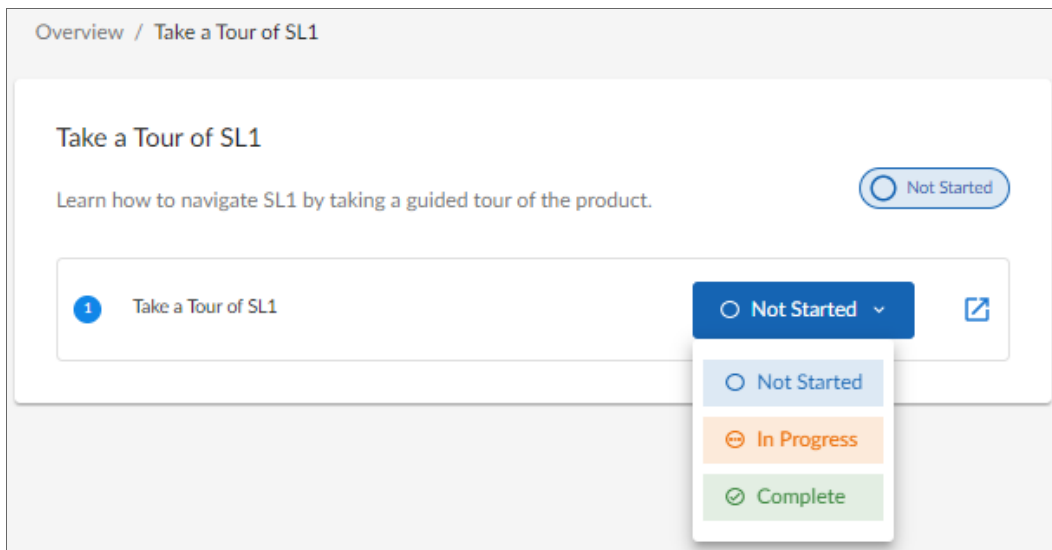
The first journey you can view in the **Overview** information card is the **[Take a Tour of SL1]** journey. This journey provides you a space to access product videos and track your progress as you learn the SL1 system.

To access SL1 educational product videos:

1. Click the arrow ([>]) button next to the status in the [**Take a Tour of SL1**] journey card.
2. Click the pop-out redirect button (🔗) to be redirected to a SL1 product video landing page. The videos located on this page contain informational walk-throughs for SL1's key features and use cases.

To update your [**Take a Tour of SL1**] status:

1. Click the arrow ([>]) button next to the status in the [**Take a Tour of SL1**] journey card.
2. As you progress in familiarity with the product and informational videos, click to update the status button drop-down. You can select [**Not Started**], [**In Progress**], or [**Complete**]. Your selected status then updates and appears across the entire workflow and **Setup and Config** pages.



Discover and Monitor Hybrid Cloud Infrastructure

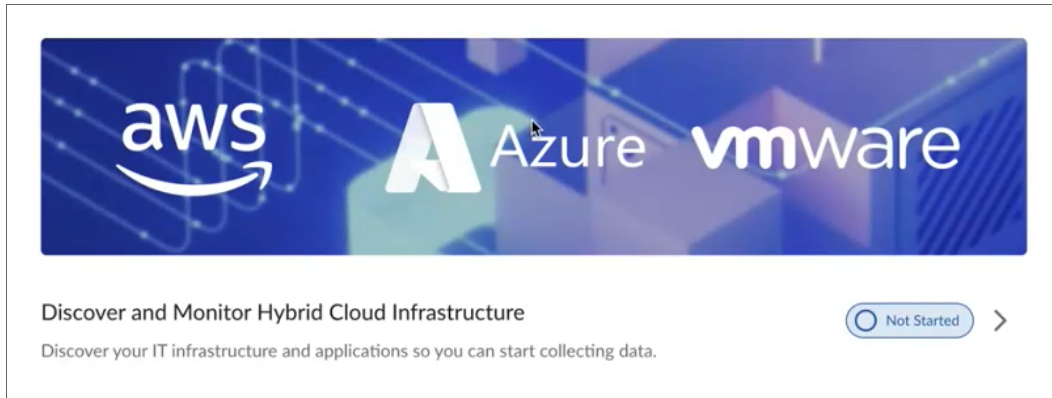
The second journey card available allows you to onboard AWS, Azure, or VMware applications in order to begin data collection. The workflow for each application provides a checklist of onboarding workflow activities.

Onboarding your Hybrid Cloud Infrastructure

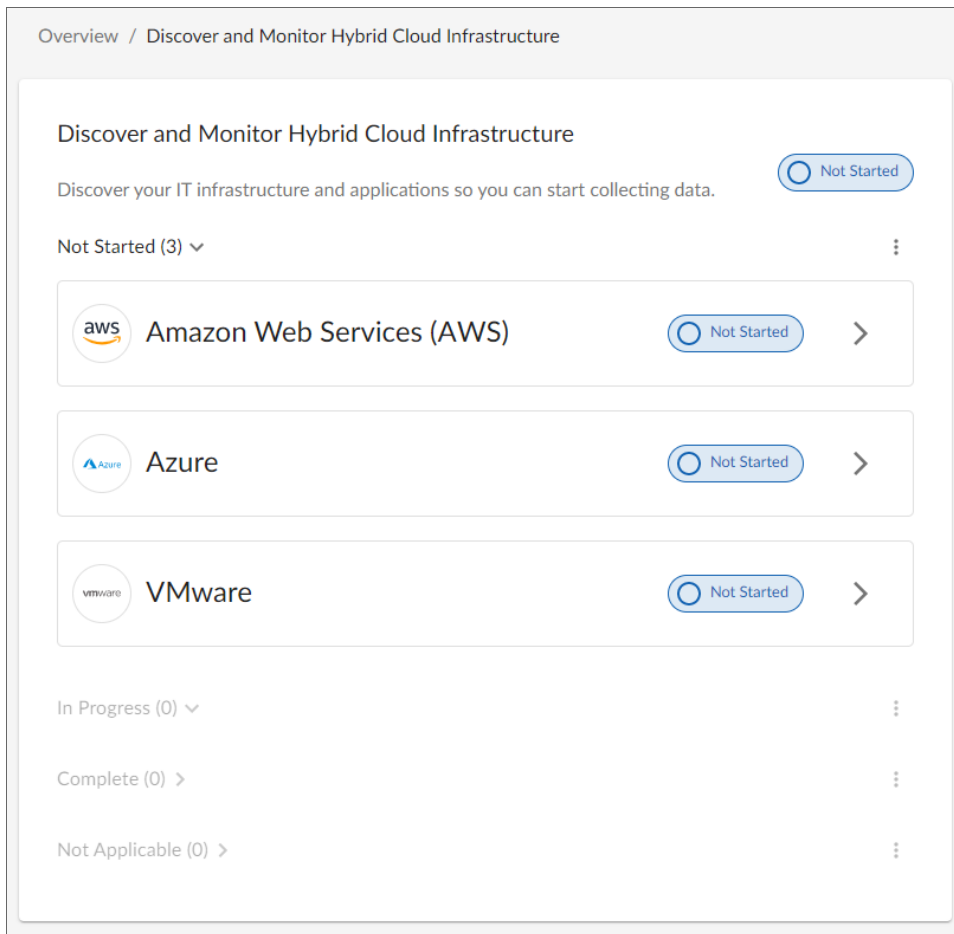
The onboard workflow for this Setup and Config user journey guides and points you to the correct pages for your infrastructure's setup.

To onboard your hybrid cloud infrastructure:

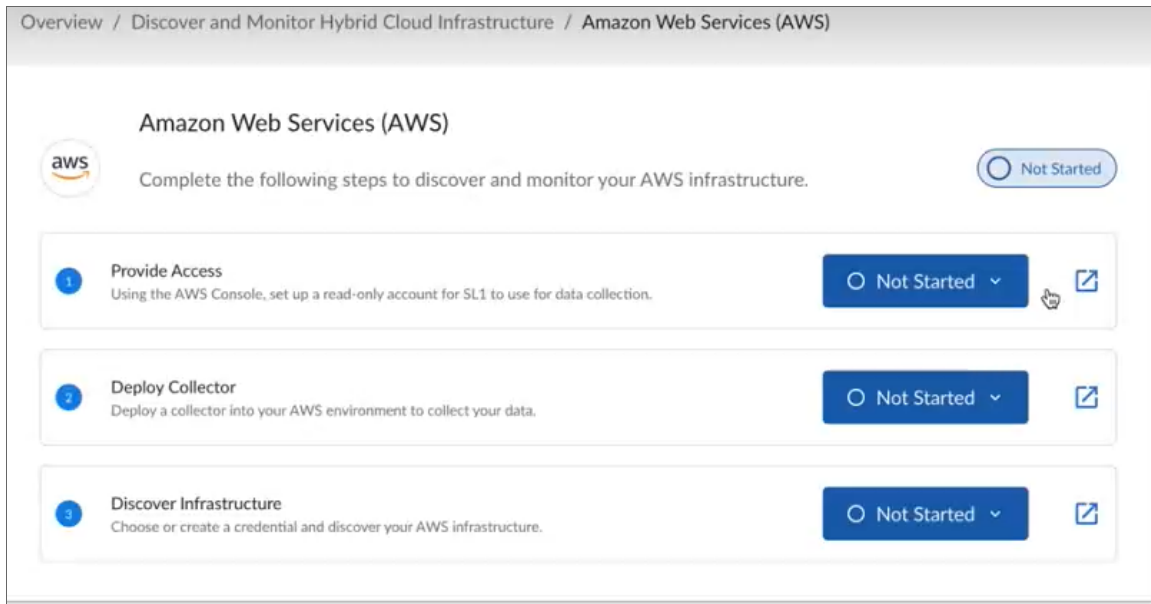
1. Click the arrow ([>]) next to the status button in the **[Discover and Monitor Hybrid Cloud Infrastructure]** journey card.



2. Click the arrow ([>]) to select your service infrastructure.



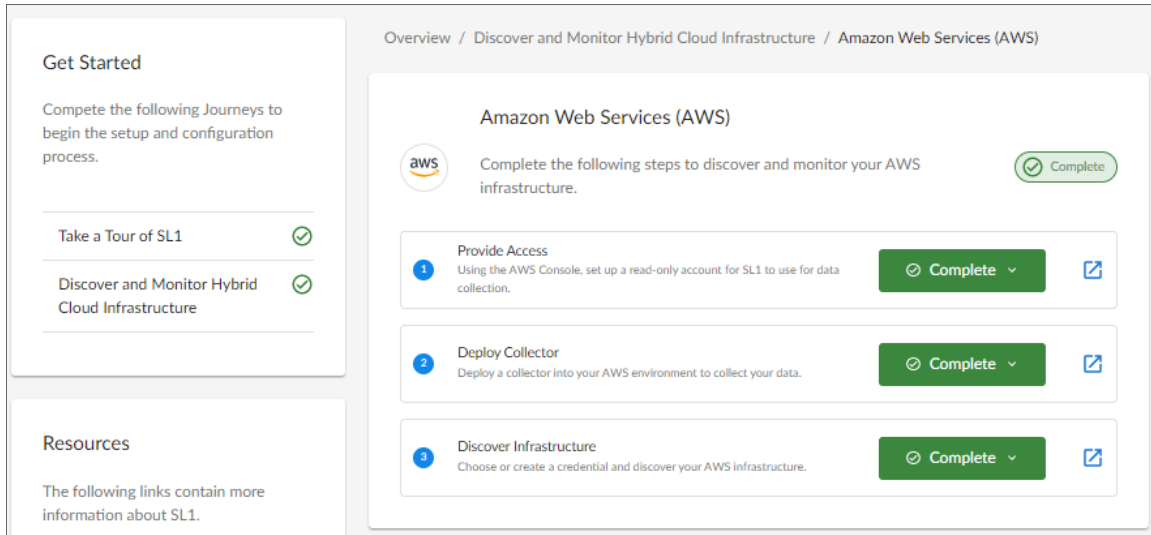
3. A checklist of activities appears. Click the pop-out redirect button (🔗) to review how to complete each individual activity for your specific infrastructure (i.e. AWS in the below image). This button redirects you to an SL1 Product Documentation page with the relevant information to walk-through the on-boarding activity.



4. The **[Deploy Collector]** and **[Discover Infrastructure]** workflow activities point you to the appropriate on-boarding wizard for each individual activity. For these two activities, find their relevant walk-through information in these sections:

- **Deploy Collector:** See the *Installing and Configuring an SL1 Collector* section in the Installation manual.
- **Discover Infrastructure:**
 - For Amazon Web Services: See the *AWS Guided Discovery* section in the *Monitoring Amazon Web Services* manual.
 - For Azure: See the *Microsoft Azure Guided Discovery* section in the *Monitoring Microsoft Azure* manual.
 - For VMware: See the *VMware Guided Discovery* section in the *Monitoring VMware* manual.

- Once you have completed the activities and their wizards, you can return to the workflow pictured below and mark your progress as **[Complete]**. The workflow status updates in both the **[Discover and Monitor Hybrid Cloud Infrastructure]** journey card and the **[Get Started]** information card.



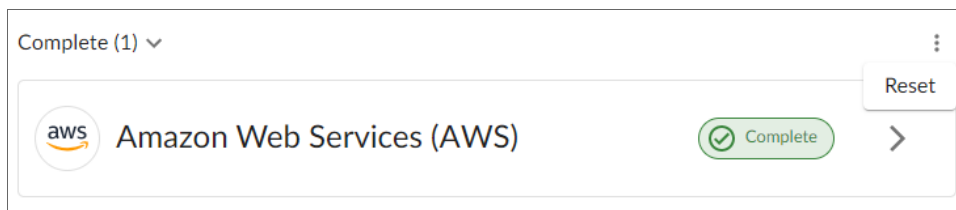
TIP: When you update the activity status to **[In Progress]**, the workflow status updates in both the **[Discover and Monitor Hybrid Cloud Infrastructure]** journey card and the **[Get Started]** information card as well.

Resetting a Completed Journey Workflow

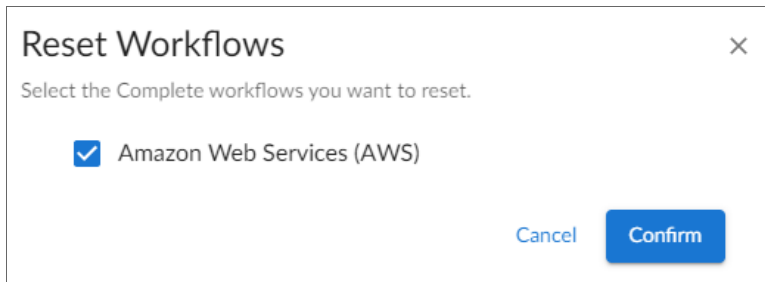
The onboard workflow for this Setup and Config user journey allows you to reset an already completed infrastructure setup if needed. You can also select more than one workflow if multiple are needed to reset.

To reset your journey's workflow:

- From the **Discover and Monitor Hybrid Cloud Infrastructure** page, click the ellipses icon and select **[Reset]**.



2. Select your desired infrastructure in the **Reset Workflows** model and click **[Confirm]**. That infrastructure will then appear with the **Not Started** status on your **Discover and Monitor Hybrid Cloud Infrastructure** page.

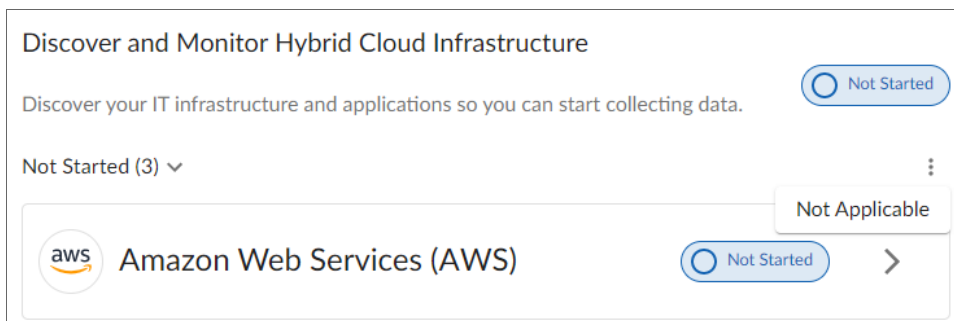


Setting a Journey Workflow as "Not Applicable"

You have the option to set an individual journey's workflow as **Not Applicable** on the **Discover and Monitor Hybrid Cloud Infrastructure** page. By setting a workflow as **Not Applicable**, the journey's workflow page moves that activity's workflow to the bottom of the page along with any other **Not Applicable** workflows. This keeps your activity workflows organized and allows for easy tracking.

To set an activity's workflow as **Not Applicable**:

1. From the **Discover and Monitor Hybrid Cloud Infrastructure** page, click the ellipses icon next to your infrastructure and select **[Not Applicable]**.



2. A **Dismiss Workflows** model appears. Select the workflow(s) that are not applicable to you. SL1 will then organize that selection as **Not Applicable** and remove it from your immediate view on the page.

Dismiss Workflows ✕

Select the workflows that are not applicable to you. This will remove from your immediate view.

- Amazon Web Services (AWS)
- Azure
- VMware


[Cancel](#) [Confirm](#)


3. Click **[Confirm]**. The infrastructure(s) workflow will then appear as **Not Applicable** on the **Discover and Monitor Hybrid Cloud Infrastructure** page.

Discover and Monitor Hybrid Cloud Infrastructure

Discover your IT infrastructure and applications so you can start collecting data. Not Started

Not Started (2) ⌵ ⋮


 **Azure** Not Started ➤

 **VMware** Not Started ➤

In Progress (0) ⌵ ⋮


Complete (0) ➤ ⋮

Not Applicable (1) ⌵ ⋮


 **Amazon Web Services (AWS)** Not Applicable ➤




4. If you click the arrow button (>) next to the **Not Applicable** workflow, that workflow and its subsequent workflow activities will appear greyed out. To undo the **Not Applicable** status from this page and display the workflow again, click **[Display]** and confirm your changes.

Overview / Discover and Monitor Hybrid Cloud Infrastructure / Amazon Web Services (AWS)

 This workflow has been marked as Not Applicable. Display

Amazon Web Services (AWS)

 Complete the following steps to discover and monitor your AWS infrastructure. Not Applicable

- 1 Provide Access**
Using the AWS Console, set up a read-only account for SL1 to use for data collection. Not Applicable 
- 2 Deploy Collector**
Deploy a collector into your AWS environment to collect your data. Not Applicable 
- 3 Discover Infrastructure**
Choose or create a credential and discover your AWS infrastructure. Not Applicable 

Configuring SL1 for PhoneHome Communication



Overview

This chapter explains how to configure SL1 to use PhoneHome Communication.

IMPORTANT: Starting with SL1 version 11.2.0, the PhoneHome Communication configuration process for SL1 Collectors has been moved to [Installing and Configuring an SL1 Collector](#). The procedures in this chapter are not compatible with the new procedures for SL1 version 11.2.0 or later that are covered in that chapter.

IMPORTANT: The PhoneHome command-line interface for SL1 version 11.2.0 and later was extensively updated, with many new and removed commands. For more information, see [Using the Command-Line Interface for PhoneHome Collection in SL1 Version 11.2.0 and Later](#).

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (.
- To view a page containing all of the menu options, click the Advanced menu icon (.

This chapter covers the following topics:

What is PhoneHome Communication?	92
Prerequisites	94
Overview of the PhoneHome Configuration	94

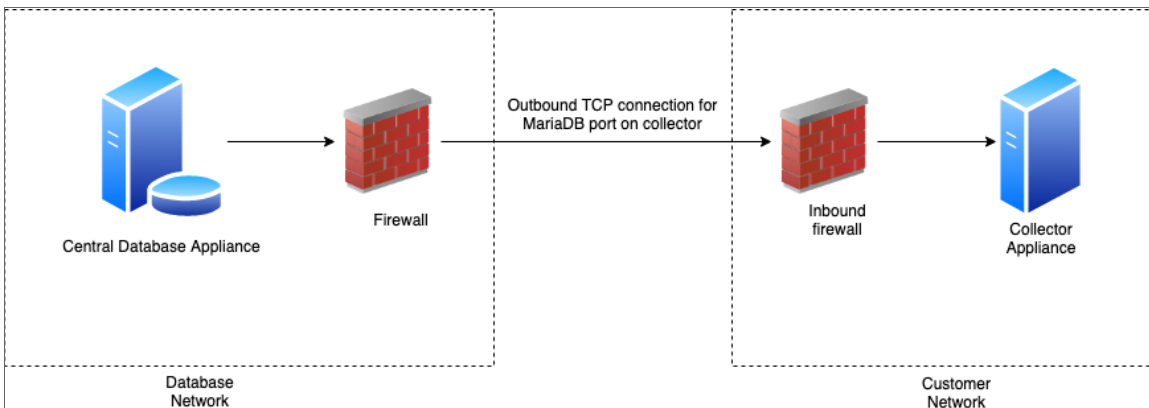
<i>Configuring the Database Server for PhoneHome</i>	95
<i>Configuring the Data Collectors and Message Collectors for PhoneHome</i>	99
<i>Registering the Data Collectors and Message Collectors</i>	101
<i>Managing Port Forwarding for PhoneHome Communication in SL1 Version 11.2.0 and Later</i>	103
<i>Defining Port Forwarding for PhoneHome Communication in SL1 Version 11.1.x and Earlier</i>	105
<i>Using Custom Options for AutoSSH</i>	105
<i>Configuring PhoneHome for High Availability and Disaster Recovery</i>	106
<i>Managing Destinations</i>	111
<i>Managing Proxy Connections for PhoneHome Communication in SL1 Version 11.2.0 and Later</i>	113
<i>Managing Proxy Connections for PhoneHome Communication in SL1 Version 11.1.x and Earlier</i> ..	115
<i>Deleting a PhoneHome Collector</i>	121
<i>Deleting a PhoneHome Database Server</i>	122
<i>Using the Watchdog Service with SL1 11.1.x and Earlier</i>	123
<i>Logging PhoneHome Configuration Information</i>	124
<i>Using the Command-Line Interface for PhoneHome Collection in SL1 Version 11.2.0 and Later</i>	125
<i>Tuning PhoneHome Settings in SL1 Version 11.2.0 and Later</i>	128
<i>Using the Command-Line Interface for PhoneHome Collection in SL1 Version 11.1.x and Earlier</i> ...	129
<i>Troubleshooting the PhoneHome Configuration in SL1 Version 11.1.x and Earlier</i>	136

What is PhoneHome Communication?

SL1 supports two methods for communication between a Database Server (an SL1 Central Database or an SL1 Data Engine) and the Data Collectors and Message Collectors:

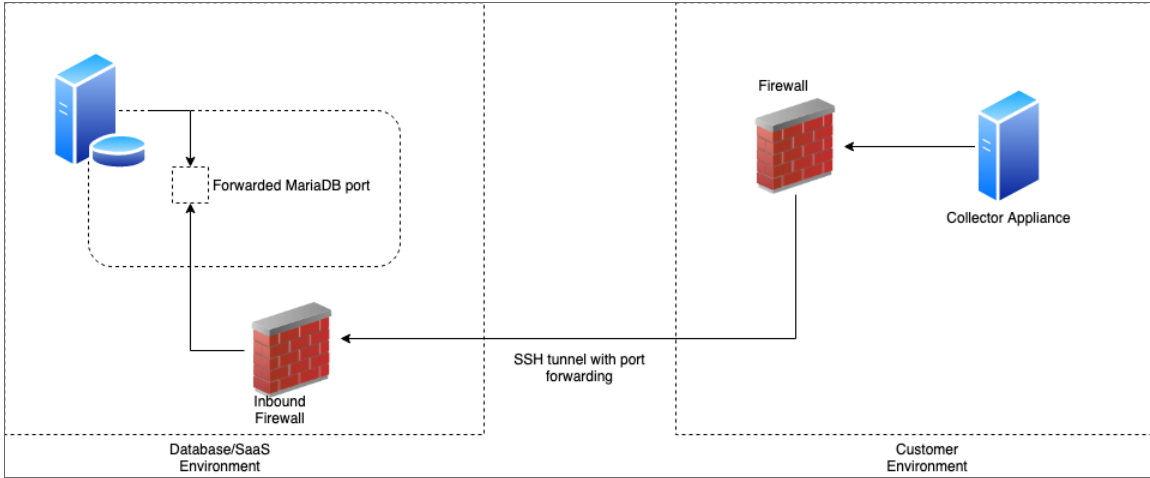
- Traditional
- PhoneHome

In the **Traditional** method, the SL1 services on the Database Server initiate a new connection to the MariaDB port on the collector to read and write data. The connection request traverses the network, including the Internet if necessary, eventually reaching the collector. For this approach to work, the collector administrator must allow ingress communication from the Database Server on port 7707 (the MariaDB port on the collector). The communication is encrypted using SSL whenever possible.



The benefit of the traditional method is that communication to the Database Server is extremely limited, so the Database Server remains as secure as possible.

In the **PhoneHome** method, the collectors initiate an outbound connection to the Database Server over SSH. After authenticating, the client forwards the local MariaDB port onto the Database Server using a loopback remote IP address. A corresponding SL1 appliance is added using the loopback IP. When the SL1 services on the database try to make a connection to the collector's MariaDB, they connect locally to the loopback IP address, in contrast to reaching out to the collector's IP or DNS name. The communication is encrypted.



The benefits of this method are that no ingress firewall rules need to be added as the collector initiates an outbound connection, and no new TCP ports are opened on the network that contains the Data Collectors.

The PhoneHome configuration uses public key/private key authentication to maintain the security of the Database Server. Each Data Collector is aligned with an SSH account on the Database Server and uses SSH to communicate with the Database Server. Each SSH account on the Database Server is highly restricted, has no login access, and cannot access a shell or execute commands on the Database Server.

Prerequisites

Before configuring PhoneHome communication in your ScienceLogic environment, you must:

- Have SSH access or console access to each Database Server.
- On each ScienceLogic appliance, know the username and password for access to the console. Note that the MySQL password matches the login password for SL1 unless one or both of the passwords were manually changed after installation.
- Ensure that all SL1 appliances are running the same version of SL1 that the Database Server is running.
- Ensure that the Database Server opens a port for PhoneHome communication. The default port used by the Configuration Utility is **7705**, but you can use other ports besides 7705.

CAUTION: Allow-listing port 7705 in the firewall is not enough. If the firewall does a layer 7 (application layer) filtering, you must create an exception rule to allow any outgoing traffic from the Data Collector to all the Database Servers on the control port, which is port 7705 by default. Some firewalls enable this by default and, as a result, those firewalls will drop SSH traffic on a non-standard port like 7705 in this situation.

NOTE: If you use a proxy in your PhoneHome configuration, [perform the steps in the proxy section](#) before configuring the other steps in the PhoneHome configuration. The remaining configuration steps require the proxy for communication.

Overview of the PhoneHome Configuration

For a configuration that includes one or more Database Servers, perform the following steps in the SL1 user interface to use PhoneHome communications:

1. [Configure one or more Database Servers for PhoneHome.](#)

NOTE: If you are using a High Availability and Disaster Recovery configuration, see [Configuring PhoneHome for High Availability and Disaster Recovery](#) to configure Database Servers.

2. [Configure the Data Collectors and Message Collectors for PhoneHome](#). If needed, update the collector to the same version of SL1 that the Database Server is running.

IMPORTANT: Starting with SL1 version 11.2.0, the PhoneHome Communication configuration process for SL1 Collectors has been moved to [Installing and Configuring an SL1 Collector](#). The procedures in this chapter are not compatible with the new procedures for SL1 version 11.2.0 or later that are covered in that chapter.

3. [Define the Database Server](#) associated with each Data Collector or Message Collector appliance.
4. [Register the Data Collectors and Message Collectors](#) in SL1.
5. As needed, [define port forwarding](#) for each collector to use SSH from the Database Server to access that collector.
6. See the [Troubleshooting section](#) for additional help.

IMPORTANT: The PhoneHome command-line interface for SL1 version 11.2.0 was extensively updated, with many new and removed commands. For more information, see [Using the Command-Line Interface for PhoneHome Collection in SL1 Version 11.2.0 and Later](#).

Configuring the Database Server for PhoneHome

In PhoneHome communication, the Database Server communicates with the Data Collectors and the optional Message Collectors. The Database Server stores all the configuration information for the PhoneHome configuration. The Database Server can be a Central Database (CDB) appliance or a Data Engine (DE) appliance.

Setting up a Database Server prepares the server to listen to incoming connections from a PhoneHome collector. This process also opens the firewall rules on the configured port and labels the configured port for SSH traffic in the SE Linux subsystem.

In 8.14.0 or later releases, PhoneHome configuration is stored in tables on the Database Server. The information is accessible to all Database Servers in the SL1 system. Any Database Server in the SL1 system can provide network access.

Before Configuring the Database Server

Make sure you have answers to the following questions before setting up the Database Server:

- Is the Database Server a single CDB or DE, or is there a High Availability (HA) or Disaster Recovery (DR) pair?
- Is the CDB or DE behind a NAT gateway?
- Do you want the PhoneHome server to listen on to the default port 7705, or do you want to customize the port?

- Does the Database Server have multiple routable IP addresses to it, and do you plan to have PhoneHome collectors from different subnets connect to the Database Server?

IMPORTANT: Each Database Server must have SL1 installed, have an IP address assigned to it, and be licensed with ScienceLogic. For more information about licensing, see [Licensing and Configuring a Database Server](#).

Configuring the Database Server in SL1 Version 11.2.0 and Later

The following sections explain how to configure the Database Server based on your SL1 environment.

NOTE: After you configure the Database Server for PhoneHome communication, you must configure the Data Collectors and Message Collectors in your network. For more information, see [Configuring the Data Collectors and Message Collectors for PhoneHome](#).

Configuring a Single Database

The most basic SL1 environment is with a single database appliance. This setup makes the following assumptions:

- The database appliance has a public IP address assigned to one of its network interfaces or has a private IP address.
- All the PhoneHome collectors will be on the same network and will be able to reach the private IP address of the PhoneHome Database Server.
- The user intends to configure the PhoneHome Database Server to listen on port 7705.
- The user intends to name the PhoneHome server as "ph-db-1". Naming the PhoneHome device is optional, but recommended.

To configure a single database appliance for PhoneHome communication:

1. Go to the console of the Database Server or use SSH to access the server and log in as user **em7admin** with the password you configured during setup.
2. Run the following command:

```
sudo phonehome setup -n ph-db-1
```

Configuring a Database with a Non-default Address or Port

Use this setup in the following situations:

- You want the PhoneHome server to listen on a non-default port, or on an address that is different than the output of the `getaddrbyhostname` syscall.
- The database appliance is behind a NAT gateway

- The database appliance is set up on a cloud host, like AWS, where the public IP is not assigned directly to the network interface of the virtual host.

To configure a Database Server with a non-default address or port:

1. Go to the console of the Database Server or use SSH to access the server and log in as user **em7admin** with the password you configured during setup.
2. Run the following command:

```
sudo phonehome setup -n ph-db-1 -a <addr>
```

where `<addr>` is an IPv4 or DNS same in "host:port" format, such as `203.65.33.22:7809` or `ph-db1.example.com:8899`.

The PhoneHome server process runs as an unprivileged user that will not be able to bind to a privileged port (1-1023). So when you choose a custom port, you must choose port 1024 or higher.

Configuring a Database with Multiple IP Addresses

To configure a Database Server with multiple IP addresses:

1. Go to the console of the Database Server or use SSH to access the server and log in as user **em7admin** with the password you configured during setup.
2. Run the following command:

```
sudo phonehome setup -n ph-db-1
```

3. Run the following command:

```
sudo phonehome destination add <id> <addr>
```

where `<id>` is the resulting device ID for the PhoneHome database and `<addr>` is an actual address string in "host:port" format. The port in all addresses must be the same, because a PhoneHome server is by design not capable of listening on multiple ports.

4. Repeat this command for every address that you want to add to the destination.

Configuring Additional Databases in a HA or DR Environment

In this setup, configure the Database Server the same as setting up a single database using `setup` command where you customize the name and the address as needed.

Configuring the Database Server in SL1 Version 11.1.x and Earlier

To configure the Database Server for PhoneHome communication in SL1 version 11.1.x and earlier:

1. Go to the console of the Database Server or use SSH to access the server and log in as user **em7admin** with the password you configured during setup.

2. Run the following command to open a port to accept incoming connection requests.:

```
sudo phonehome open-control-port <port_number>
```

where `<port_number>` is an unused port number greater than 1024. The Configuration Utility uses port 7705 as the default port. If you want to use the default port, specify **7705** in this command. To use a *different* port, specify that port number in this command.

3. To define the Database Server (to itself), type the following at the shell prompt:

```
sudo phonehome add database
```

4. Review the output, which should look like the following:

```
Created local: #0
```

```
Reloading sshd configurations
```

```
Created database: #11
```

```
Changing password for user: "phonehome11"
```

```
Created Device Id: "11"
```

```
Created token: "phonehome://11@71.97.6.197/ee4sdRRK8yNu"
```

5. Note the ID number for the database (**11** in our example).
6. If the database is behind a firewall, you need to define the public-facing IP address of the Database Server and also define the port to use for SSH communication from PhoneHome servers to the Database Server. To do this, type the following at the shell prompt:

```
sudo phonehome set <appliance_ID> -ip=<IP_address> -port=<port_number>
```

where `<appliance_ID>` is the value you noted in step 6, `<IP_address>` is the public-facing IP address, and `<port_number>` is the port you want to use for SSH communication to and from the Database Server.

For example:

```
sudo phonehome set 11 -ip=71.197.6.197 -port=7705
```

8. You must now configure the Data Collectors and Message Collectors in your network. To do this, go the next section.

Configuring the Data Collectors and Message Collectors for PhoneHome

IMPORTANT: Starting with SL1 version 11.2.0, the installation and configuration process for SL1 Collectors was updated. For detailed procedures about configuring a collector, see [Installing and Configuring an SL1 Collector](#).

This section describes how to configure a Data Collector and a Message Collector for use in a PhoneHome configuration running a version of SL1 before version 11.2.0.

IMPORTANT: Each Data Collector and Message Collector must have SL1 installed, and each Data Collector and Message Collector must have an IP address assigned to it. Also, make sure that the Data Collector and Message Collector you are using in a PhoneHome configuration is running the same version of SL1 that the Database Server is running.

NOTE: If your PhoneHome configuration uses proxy servers, do not use this section to configure a Data Collector or Message Collector. See the [section on proxy servers](#) instead.

To configure a Data Collector or Message Collector as part of a PhoneHome configuration in SL1 before version 11.2.0:

1. On the Data Collector or Message Collector, log in to the Web Configuration Utility using any web browser supported by SL1. The address of the Web Configuration Utility is in the following format:
`https://<IP_address_of_collector>:7700`
where `<IP_address_of_collector>` is the IP address of the Data Collector or Message Collector.
2. When prompted to enter your user name and password, log in as the "em7admin" user with the appropriate password. The **Configuration Utilities** page appears.
3. Click the **[PhoneHome]** button. The **PhoneHome - Collector** page appears.
4. Complete the following fields:
 - **Hostname/IP.** Type the Hostname or IP address of the Database Server that is configured for PhoneHome.

- **Port (if not 7705).** Optional. Port number for SSH communications with the Database Server that is configured for PhoneHome. If you are using a port *other* than 7705 on the Database Server, type the port number in this field. Otherwise, leave this field blank.

IMPORTANT: The PhoneHome connection between a Collector and the Database Server requires that you initiate outbound communication on TCP/443 and TCP/7705. Both ports must be open for this connection to work. You can use the `nmap` command to make sure the ports are open before attempting the connection:

```
nmap -p 443 x.x.x.x
nmap -p 7705 x.x.x.x
```

- **Make request via HTTPS.** Optional. If you select this checkbox, the Data Collector will send the PhoneHome request to the Database Server using an HTTPS request. The Data Collector will send the request directly to the ScienceLogic Web Configuration Utility (port 7700) on the Database Server. This option works only if the Data Collector has direct access to port 7700 on the Database Server.
 - **Verify SSL Cert.** Optional. When you use HTTPS, the Database Server sends an SSL certificate. If the certificate is from a Certificate Authority and must be verified, select this checkbox. If the certificate is internal and does not require verification, do not select this checkbox.
5. Click the **[Send Connection Request]** button to send the request from the Data Collector to the Database Server that is configured for PhoneHome. This option uses SSH to send the request. After clicking the **[Send Connection Request]** button, the **PhoneHome - Collector** page displays the status *Pending database approval*. Do not close the browser window or navigate away from this page while the connection request is being processed. Do not close the browser window or navigate away from this page while the connection request is being processed.
 6. In a new browser window, open the ScienceLogic Web Configuration Utility for the Database Server. To do this, type the following, replacing "*ip-address-of-database*" with the IP address of the Database Server:

```
https://<IP_address_of_database>:7700
```

7. When prompted to enter your username and password, log in as the "em7admin" user with the appropriate password. The main **Configuration Utility** page appears.
8. Click the **[PhoneHome]** button. The **PhoneHome Database - Master** page appears.
9. Note that the list of Collectors includes a request. Click the **[Accept]** button for that collector. The Status for the Collector now displays as *Approved*.
10. On the Data Collector or Message Collector, open the ScienceLogic Web Configuration Utility and click the **[PhoneHome]** button. The **PhoneHome - Collector** page appears.
11. Note that the Status message is now *Configured - ID [phonehome_user_number]*. If you refresh the page, the status field displays the message *Synced and Connected*.

If you have a large number of collectors, you can perform the following steps to approve multiple collectors at the same time:

1. On each Data Collector or Message Collector, follow steps 1-7 in the [previous procedure](#) to send the connection request for each collector.
2. Open the ScienceLogic Web Configuration Utility for the Database Server and click the **[PhoneHome]** button.
3. Click the **[Accept All Collector Requests]** button.
4. Open the ScienceLogic Web Configuration Utility for each collector, click the **[PhoneHome]** button, and then click the **[Check Approval]** button.
5. Repeat step 4 until you have approved all of your collectors.

Registering the Data Collectors and Message Collectors

NOTE: Perform the steps in this section after you have successfully established a PhoneHome connection between Data Collectors or Message Collectors and the main Database Server. The steps in this section ensure that the SL1 system uses the loopback address that is assigned to each Data Collector and Message Collector upon [successful completion of a phonehome connection request](#).

IMPORTANT: Starting with SL1 version 11.3.0 and later, you only need to license a Database Server, whether it is a central database (CDB) or a data engine (DE). SL1 automatically licenses Data Collectors, Message Collectors, and Administration Portal appliances when they are added to the environment.

To register a Data Collector or Message Collector with the main Database Server:

1. In the address bar of your browser, type the IP address of the SL1 appliance that provides the user interface for your SL1 system. The user interface is provided by either the Database Server or an Administration Portal. The login page appears.
2. Log in as the "em7admin" user with the appropriate password.
3. If this is your first successful login, you will be asked to agree to the End-user License Agreement. Read the End-user License Agreement and then click the **[I Agree to The Terms Outlined Above]** button.
4. Go to the **Appliance Manager** page (System > Settings > Appliances).

<p>Host Name cu-106422623</p> <p>IP Address 127.0.0.0</p> <p>DB User</p> <p>DB Password</p>	<p>Model type [Data Collection Unit]</p> <p>Description Collector 1064</p>	<p>Save</p> <p>Save As</p>
---	--	----------------------------

5. Complete the following fields:

- **Host Name.** Type the host name of the Data Collector or Message Collector.
- **IP Address.** Type the **loopback IP address** of the Data Collector or Message Collector. The loopback IP address is a special, virtual network interface that your computer uses to communicate with itself. This address also allows you to view content on a server in the same way a client would. In most cases, the loopback address is 127.0.0.1, although the loopback address can be any IP address in the 127.0.0.0/8 block.

TIP: If you go to the Web Configuration Utility of the Database Server and click the **PhoneHome** button, you can view a list of all the connected collectors, along with their IDs. The ID indicates the loopback address. For example, if the ID of a given collector is 12, then its loopback address is 127.0.0.12.

- **Model Type.** Select the type of appliance (Data Collector or Message Collector) you are registering.
- **Description.** Type a description for the Data Collector or Message Collector. This field is optional.
- **DB User.** User name that can access the MariaDB database on the Data Collector or Message Collector.
- **DB Password.** Password that allows access the MariaDB database on the Data Collector or Message Collector.

NOTE: In SL1 version 11.2.0, SL1 automatically set the default database credentials when adding an SL1 collector to the stack. Starting with SL1 version 11.3.0, SL1 no longer specifies the credentials. As a result, you will need to specify the credentials for the collector on the **Appliances** page (System > Settings > Appliances), in the **DB User** and **DB Password** fields.

6. Click the **[Save]** button. If the save is successful, the message "Appliance Registered" displays.

7. If all information is valid and the Database Server can communicate with the Data Collector or Message Collector, the **Appliance Manager** page displays the ScienceLogic version installed on the collector in the **Build** column. If the **Build** column remains blank for longer than five minutes, double-check your settings and network connection.
8. Perform these steps for each Data Collector and Message Collector in your PhoneHome configuration.

Managing Port Forwarding for PhoneHome Communication in SL1 Version 11.2.0 and Later

A port forward is a configuration that allows a PhoneHome client to "copy" a local port from the SL1 Collector to the Database Server, essentially making the local port available on the Database Server appliance as if it was physically present on that appliance itself.

NOTE: The local MariaDB port 7707 on the collector is forwarded to the Database Server by default.

Viewing a List of Port Forwards

IMPORTANT: This section applies only to SL1 version 11.2.0 and later.

To view a list of ports forwarded from an SL1 Collector to the Database Server:

1. Go to the console of the SL1 Collector.
2. Run the following command on the SL1 Collector:

```
phonehome forwards list
```

NOTE: This list will not include the MariaDB port 7707, which is forwarded by default.

Adding a Port Forward

IMPORTANT: This section applies only to SL1 version 11.2.0 and later.

To add a port forward:

1. Go to the console of the SL1 Collector.
2. Run the following command on the SL1 Collector, replacing `<Remote Address>` with the port on the Database Server onto which the local port will be forwarded and `<Local Address>` with the local port to forward from the SL1 Collector:

```
phonehome forward add <Remote Address> <Local Address>
```

NOTE: Addresses should be in the format `:<port>`.

NOTE: The remote port should be an unprivileged port (a port greater than 1023).

For example, if you want to forward SSH port 22 from the SL1 Collector to the Database Server appliance as port 10022 to enable a Database Server administrator to SSH into the SL1 Collector from the Database Server appliance, you would run the following command:

```
phonehome forward add :10022 :22
```

NOTE: New forwards do not take effect until the PhoneHome client is restarted or the next watchdog cycle occurs.

Removing a Port Forward

IMPORTANT: This section applies only to SL1 version 11.2.0 and later.

To remove a port forward:

1. Go to the console of the SL1 Collector.
2. Run the following command on the SL1 Collector, replacing `<Remote Address>` with the port on the Database Server appliance onto which the local port was forwarded and `<Local Address>` with the local port that was forwarded from the SL1 Collector:

```
phonehome forward remove <Remote Address> <Local Address>
```

NOTE: Addresses should be in the format `:<port>`.

For example, if you want to no longer forward SSH port 22 from the SL1 Collector to the Database Server appliance as port 10022, run the following command:

```
phonehome forward remove :10022 :22
```

NOTE: Deleted forwards do not take effect until the PhoneHome client is restarted or the next watchdog cycle occurs.

Defining Port Forwarding for PhoneHome Communication in SL1 Version 11.1.x and Earlier

If you define port forwarding for each Data Collector or Message Collector in the PhoneHome configuration, you can use SSH from the Database Server to access the Data Collector or Message Collector.

To define port forwarding:

1. Either go to the console of the Database Server or use SSH to access the server.
2. Log in as user **em7admin** with the password you configured during setup.
3. For each Data Collector and/or Message Collector, type the following at the shell prompt:

```
sudo phonehome set <appliance_ID> -forwards=<port_number>
```

where `<appliance_ID>` is the device ID for the Data Collector or Message Collector and `<port_number>` is the port you want to use for SSH communication from the Database Server to the Data Collector or Message Collector.

For example:

```
sudo phonehome set 12 -forwards=22
```

4. For every other server in the PhoneHome configuration, go to the console of the Database Server or use SSH to access the server.
 5. Log in as user **em7admin** with the password you configured during setup.
 6. Type the following at the shell prompt:
- ```
sudo phonehome sync
```
7. Now, whenever you are SSHed in to the Database Server, you can SSH to the Data Collector or Message Collector.
  8. To use the forward port, append "100" to the front of the port you defined in step #3 and use the loopback IP of the Data Collector or Message Collector using port 10022:

```
ssh -p 10022 root@127.0.0.12
```

---

## Using Custom Options for AutoSSH

By default, SL1 stores settings for AutoSSH for PhoneHome configurations in the file `/opt/em7/backend/phonehome/em7_ph_tunnels` on each Data Collector and Message Collector in your configuration.

If you want to use custom AutoSSH settings for a specific Data Collector or Message Collector in your configuration, you can create the file `/etc/phonehome/local.conf` and define custom AutoSSH options for that server.

To define custom SSH options for a server:

1. Log in to the console of the Data Collector or Message Collector as the root user.
2. Open the file `/etc/phonehome/local.conf` with a text editor like vi:

```
vi /etc/phonehome/local.conf
```

3. Add one or more custom settings for AutoSSH. You can define:

- `TCPKeepAlive = "yes or no"`. Specifies whether the client will send a null packet to the server (to keep the connection alive). Uses the TCP layer to send the packet. The default value is "no". If you set this value to zero (0), this feature is disabled. Your connection will drop if idle for too long.
- `ServerAliveInterval = "number of seconds"`. The number of seconds the client will wait before sending a null packet to the server (to keep the connection alive). Uses the SSH layer to send the packet. The default value is "10". If you set this value to zero (0), this feature is disabled.
- `StrictHostKeyChecking = "yes or no"`. If this flag is set to "yes", AutoSSH will never automatically add host keys to AutoSSH configuration and will refuse to connect to hosts whose host key has changed. This option forces the user to manually add all new hosts. If this flag is set to "no", ssh will automatically add new host keys to the known hosts files. The default value is "no".
- `ServerAliveCountMax = "number of messages"`. The maximum number of unacknowledged null packets the client will send to the server (to keep the connection alive). After the maximum number of unacknowledged null packets, the client will drop the SSH connection to the server. The default value is "2". If you set this value to zero (0), this feature is disabled. Your connection will drop if idle for too long.
- `CUSTOM_PARAMS = "-o parameter = argument"`. Any additional SSH parameters can be configured with this option. For example:

```
CUSTOM_PARAMS="-o ExitOnForwardFailure=yes"
```

**NOTE:** To determine the format for entries in the `/etc/phonehome/local.conf` file, see the file `/opt/em7/backend/phonehome/em7_ph_tunnels`.

4. Save your changes and exit the file.

---

## Configuring PhoneHome for High Availability and Disaster Recovery

This section describes how to configure the Database Servers in your system for use in a PhoneHome configuration.

**NOTE:** You can use the same Database Servers in both a PhoneHome configuration and a traditional configuration.

After performing the steps in this section, go the section on [Configuring the Data Collectors and Message Collectors](#) to complete the configuration.

## Configuring the Primary Database Server for High Availability and Disaster Recovery

To configure the primary Database Server for PhoneHome communication:

1. Go to the console of the primary Database Server or use SSH to access the server.
2. Log in as user **em7admin** with the password you configured during setup.
3. For the primary Database Server, you must first open a port to accept incoming connection requests. To do this, type the following at the shell prompt:

```
sudo phonehome open-control-port <port_number>
```

where `<port_number>` is an unused port number greater than 1024. The default value in the Configuration Utility is 7705. If you want to use the default port later in the Configuration Utility, specify "7705" in this command.

4. To define the primary Database Server (to itself), type the following at the shell prompt:

```
sudo phonehome add database
```

5. Review the output, which should look like the following:

```
Created local: #0
```

```
Reloading sshd configurations
```

```
Created database: #11
```

```
Changing password for user: "phonehome11"
```

```
Created Device Id: "11"
```

```
Created token: "phonehome://11@71.97.6.197/ee4sdRRK8yNu"
```

6. Note the ID number for the primary Database Server (**11** in our example).

7. To define the public-facing IP address of the primary Database Server and the port to use for SSH communication from PhoneHome servers to the primary Database Server, type the following at the shell prompt:

```
sudo phonehome set <appliance_ID> -ip=<IP_address> -port=<port_number>
```

where `<port_number>` is an unused port number greater than 1024. The Configuration Utility uses port 7705 as the default port. If you want to use the default port, specify **7705** in this command. To use a *different* port, specify that port number in this command.

For example:

```
sudo phonehome set 11 -ip=71.197.6.197 -port=7705
```

8. Start the PhoneHome watchdog. To do so, type the following at the shell prompt:

```
sudo systemctl enable em7_ph_watchdog
```

```
sudo systemctl start em7_ph_watchdog
```

9. If your SL1 System uses multiple databases for high availability and/or disaster recovery, you must create a record for the secondary Database Server on the primary Database Server. To do so, type the following at the shell prompt:

```
sudo phonehome add database
```

10. The output will look like this:

```
Reloading sshd configurations
```

```
Created database: #13
```

```
Changing password for user: "phonehome13"
```

```
Created Device Id: "13"
```

```
Created token: "phonehome://13@10.64.68.31:22/GmHtYvDd900V"
```

11. Note the ID number for the secondary Database Server. You will need this value later in the configuration.
12. Copy and save the token for the secondary Database Server. You will need this value later in the configuration.
13. To define the public-facing IP address of the secondary Database Server and the port to use for SSH communications from PhoneHome servers to the secondary Database Server, type the following at the shell prompt:

```
sudo phonehome set <appliance_ID> -ip=<IP_address> -port=<port_number>
```

where:

- `<appliance_ID>` is the value you noted in step 5.
- `<IP_address>` is the public-facing IP address.

- `<port_number>` is the port you want to use for SSH communication to and from the primary Database Server.

For example, we could enter:

```
sudo phonehome set 13 -ip=71.197.6.198 -port=7705
```

## Configuring the Secondary Database Server for High Availability and Disaster Recovery

To configure a secondary Database Server as part of a PhoneHome configuration:

1. Either go to the console of the secondary Database Server or use SSH to access the server.
2. Log in as user **em7admin** with the password you configured during setup.
3. For the secondary Database Server, you must first open a port to accept incoming connection requests. To do this, type the following at the shell prompt:

```
sudo phonehome open-control-port <port_number>
```

where `<port_number>` is an unused port number greater than 1024. The default value in the Configuration Utility is 7705. If you want to use the default value, specify "7705". ScienceLogic recommends that you use the same port number on each database in your PhoneHome configuration.

4. To register the secondary Database Server, type the following at the shell prompt:

```
sudo phonehome register <appliance_token>
```

where `<appliance_token>` is the URL you saved during step 11 in the section [Configuring the Primary Database for High Availability and Disaster Recovery](#).

5. The output looks like the following:

```
Registered device successfully
```

6. Type the following at the shell prompt:

```
sudo phonehome sync
```

7. The output looks like the following:

```
Started synchronization
```

```
Synchronized: collectors
```

```
Synchronized: databases
```

```
Reloading sshd configurations
```

```
Finished synchronizations
```

# Configuring Data Collectors and Message Collectors for High Availability and Disaster Recovery

You must now configure the Data Collectors and Message Collectors in your network. To do this, see [Configuring the Data Collectors and Message Collectors](#).

**NOTE:** If your PhoneHome configuration uses proxy servers, do not use this section to configure a Data Collector or Message Collector. See the [section on proxy servers](#) instead.

## Syncing the High Availability and Disaster Recovery System

After adding Data Collector(s) or Message Collector(s) to your PhoneHome configuration, you must once again execute the sync command on all **Database Servers** and then on the newly configured Collectors in the PhoneHome configuration.

To sync your PhoneHome configuration:

1. Either go to the console of the Database Server (or the new Collectors) or use SSH to access the server.
2. Log in as user **em7admin** with the password you configured during setup.
3. At the shell prompt, type the following:  

```
sudo phonehome sync
```
4. Perform these steps on each Database Server, Data Collector, and Message Collector in your PhoneHome configuration.

## Adding a New Secondary Database Server

To add a new secondary Database Server to an existing PhoneHome configuration:

1. On the primary Database Server, perform the steps from the section [Configuring the Primary Database Server](#). These are the steps that define the secondary Database Server, including saving the token and saving the new configuration.
2. On the new secondary Database Server, perform the steps from the section [Configuring the Secondary Database Server for High Availability and Disaster Recovery](#).
3. Either go to the console of the SL1 appliance or use SSH to access the new secondary Database Server. Log in as "root".
4. At the shell prompt, type the following:  

```
phonehome status
```
5. The new secondary Database Server should be connected to each Data Collector in the PhoneHome configuration.

---

## Managing Destinations

A destination is a list of addresses associated with a Database Server. A PhoneHome Database Server can have one or more destination addresses associated with it.

**NOTE:** Destination addresses can be IPv4 addresses or DNS names, or a combination of both.

## Viewing a List of Destinations

**IMPORTANT:** This section applies only to SL1 version 11.2.0 and later.

To view a list of all destinations in your stack:

1. Go to the console of the SL1 Collector.
2. Run the following command on the SL1 Collector:

```
phonehome destination list
```

This command provides a list of all Database Servers with their device IDs, addresses, and priorities. Priorities define the order in which an SL1 Collector will try to connect to the individual addresses. It will keep trying until it can connect to one of them.

**NOTE:** To view a list of destinations on a specific PhoneHome Database Server, run the following command, where *<Device ID>* is the ID of the PhoneHome Database Server:

```
phonehome destination list --id <Device ID>
```

## Adding a Destination Address

**IMPORTANT:** This section applies only to SL1 version 11.2.0 and later.

To add a new destination address:

1. Go to the console of the SL1 Collector.
2. Run the following command on the SL1 Collector, where *<Device ID>* is the ID of the device to which you want to add a new address and *<Address>* is the destination address:

```
phonehome destination add <Device ID> <Address>
```

**NOTE:** Addresses should be in the format `<host>:<port>`.

**NOTE:** Host addresses can be IPv4 addresses or DNS names.

If successful, you will get a message confirming that the new address was successfully added to the destination.

For example, if you wanted to add the destination address 192.168.0.13, with port 7705 open, to the device with the device ID 2, run the following command:

```
phonehome destination add 2 192.168.0.13:7705
```

**NOTE:** The port you open must match the port that is open for the original device. Otherwise, you will receive an error.

**NOTE:** Optionally, you can add the suffix `--priority <Priority>` to establish the destination's priority, or use the suffix `--force` to force add a destination address, even if the port does not match with the device's listed port.

## Removing a Destination

**IMPORTANT:** This section applies only to SL1 version 11.2.0 and later.

To remove an existing address from a destination:

1. Go to the console of the SL1 Collector.
2. Run the following command on the SL1 Collector, where `<Device ID>` is the ID of the device from which you want to remove a destination address and `<Address>` is the destination address:

```
phonehome dest remove <Device ID> <Address>
```

**NOTE:** Addresses should be in the format `<host>:<port>`.

**NOTE:** Host addresses can be IPv4 addresses or DNS names.

**NOTE:** You cannot remove an address from a destination if it is the destination's only address.



---

# Managing Proxy Connections for PhoneHome Communication in SL1 Version 11.2.0 and Later

If your organization requires that you use a proxy for outbound requests, you can configure one or more proxy connections between the an SL1 Collector and the Database Server.

For example, you might use a proxy connection if your SL1 Collector does not have a direct outbound internet connection to reach the Database Server. A PhoneHome proxy configuration includes the destination address—either the address of the Database Server or that of the next proxy host—and the address of the proxy server to which the client must connect to reach the destination.

There can be one or more proxy hosts in between an SL1 Collector and a Database Server, thus forming a proxy chain.

**NOTE:** If you use a proxy in your PhoneHome configuration, perform the steps in the section about [Adding a Proxy Connection](#) before you configure the other steps in this chapter. The other steps in the PhoneHome configuration will require the proxy for communication.

## Viewing a List of Proxy Connections

To view a list of proxy connections from an SL1 Collector to the Database Server:

1. Go to the console of the SL1 Collector.
2. Run the following command on the SL1 Collector:

```
phonehome proxy list
```

## Adding a Proxy Configuration

To add a proxy connection between an SL1 Collector to the Database Server:

1. Go to the console of the SL1 Collector.
2. Run the following command on the SL1 Collector, replacing `<Destination Address>` with the address and port of the Database Server appliance to which you want to connect, `<Proxy Address>` with the proxy host address and port you want to use as a tunnel, and `<Proxy User>` with the username used to log in to the proxy host:

```
phonehome proxy new <Destination Address> <Proxy Address> <Proxy User>
```

**NOTE:** Addresses should be in the format `<host>:<port>`. The host can be either an IP address or a DNS name.

For example, if you want to configure the SL1 Collector to connect to the Database Server with an address of 202.35.52.71 through a proxy host with the address 10.1.17.68 with the user em7admin, you would run the following command:

```
phonehome proxy new 202.35.52.71:7705 10.1.17.68:22 em7admin
```

If you are connecting to the Database Server through a chain consisting of multiple proxies, you should add the proxy configurations in reverse order, starting with the destination address and last proxy host address, then the last proxy host address and previous proxy host address, and so forth, until you get to the first proxy host.

For example, if you want to connect to the Database Server with an address of 202.42.63.79 through proxy host A with an address of 192.168.0.3 with the user proxyuser, and also proxy host B with an address of 10.2.13.79 with the user em7admin, then you would run the following commands:


```
phonehome proxy new 202.42.63.79:7705 10.2.13.79:22 em7admin
```

```
phonehome proxy new 10.2.13.79:22 192.168.0.3 proxyuser
```

**NOTE:** New proxy configurations do not take effect until the PhoneHome client is restarted or the next watchdog cycle occurs.

**NOTE:** When you run the command, the system prompts you for a password for the proxy host. The system uses this password to automatically configure and validate SSH key-based authentication to the host; the next time you need to run anything via the proxy host, it will use the collector's private key for authentication rather than prompting you for the password. Optionally, you can disable this behavior by adding "-n" to the end of the command. If you do so, you must then manually configure the proxy's SSH key-based authentication.

If you get a "handshake failed: ssh..." error message when adding a new proxy:

1. In SL1, go to the **Appliances** page (System > Settings > Appliances) and click the edit button (  ) for that appliance.
2. Review the collector's MariaDB credentials. This error can occur if the collector and the Database Server (CDB) use different credentials.

For example, if the Database Server has been updated and the ISO for the Database Server is before SL1 version 11.3.0, while the collector was deployed with SL1 version 11.3.0 or later. In this situation, the Database Server will be using **root/<password>**, and the collector would be using **clientdbuser/<password>**.

## Deleting a Proxy Configuration

To add a proxy configuration between an SL1 Collector to the Database Server:

1. Go to the console of the SL1 Collector.
2. Run the following command on the SL1 Collector, replacing `<Destination Address>` with the address and port of the Database Server appliance to which the proxy is connecting:  

```
phonehome proxy delete <Destination Address>
```

**NOTE:** Addresses should be in the format `<host>:<port>`. The host can be either an IP address or a DNS name.

**NOTE:** Removed proxy configurations do not take effect until the PhoneHome client is restarted or the next watchdog cycle occurs.

---

## Managing Proxy Connections for PhoneHome Communication in SL1 Version 11.1.x and Earlier

If your organization requires that you use a proxy for outbound requests, you can configure one or more Data Collectors to act as proxy servers. These proxy servers will sit between the Data Collectors in your PhoneHome configuration and the Database Server in your PhoneHome configuration.

To use one or more Data Collectors as proxy servers in a PhoneHome configuration:

- Ensure that the SSH port is open on each Data Collector that acts as a proxy server.
- Ensure that the SSH port is open on each Database Server in the PhoneHome configuration.

**NOTE:** If you use a proxy in your PhoneHome configuration, **perform the steps in this section before you configure the other steps in this chapter**. The other steps in the PhoneHome configuration will require the proxy for communication.

To configure your PhoneHome configuration to use a proxy server, you must:

1. Configure a Database Server for PhoneHome configuration as either a stand-alone Database Server ([Configuring the Database Servers](#)) or a High Availability Database Server ([Configuring the Database Servers for High Availability](#))
2. [Edit the ssh\\_config file](#).
3. Use the command line to configure Data Collectors [that connect via proxy](#).
4. [Copy the SSH key to each proxy](#).
5. [Synchronize the](#) Data Collectors with the Database Server.

## Editing ssh\_config

To edit the `ssh_config` file:

**IMPORTANT:** Perform these steps on the Data Collector that will be part of the PhoneHome configuration, *not on the Data Collector that will serve as a proxy server.*

1. Either go to the console of the Data Collector that will be part of the PhoneHome configuration or use SSH to access the server.
2. Log in as user **em7admin** with the password you configured during setup.
3. Open the file `/etc/ssh/ssh_config` with vi or another text editor:

```
sudo vi /etc/ssh/ssh_config
```

4. Add the following lines to the file:

```
Host <hostname_of_primary_Database_Server>
```

```
ProxyCommand ssh -q em7admin@<proxy_hostname> nc %h %p
```

where:

- `<hostname_of_primary_Database_Server>` is the hostname for the primary Database Server.
- `proxy_hostname` is the hostname of the proxy server that directly communicates with the Database Server. If you have a chain of proxy servers, this value is the hostname of the last proxy server in that chain (the proxy server that connects to the Database Server).

**NOTE:** If you use hostnames to configure proxy servers, you must use hostnames for all PhoneHome configuration. If you use IP addresses to configure proxy servers, you must use IP addresses for all PhoneHome configuration. You cannot mix hostnames and IP addresses in `ssh_config` and in PhoneHome configuration.

5. If applicable, for all secondary databases, add the following lines to the file:

```
Host <hostname_of_secondary_Database_Server>
```

```
ProxyCommand ssh -q em7admin@<proxy_hostname> nc %h %p
```

where:

- `<hostname_of_secondary_Database_Server>` is the hostname for the secondary Database Server.
- `<proxy_hostname>` is the hostname of the proxy server that directly communicates with the secondary Database Server. If you have a chain of proxy servers, this value is the hostname of the last proxy server in that chain (the proxy server that connects to the Database Server).

6. If you have more than one proxy server, add the following lines to the file:

```
Host <hostname_of_proxy_server>
```

```
ProxyCommand ssh -q em7admin@<proxy_hostname> nc %h %p
```

where:

- `<hostname_of_proxy_server>` is the hostname of the current proxy server (the proxy server for which you are creating an entry). For example, you could create an entry for "ProxyServer2".
- `<proxy_hostname>` is the hostname of the proxy server that is previous in the chain and communicates with the current proxy server. If your entry is for "ProxyServer2", you would specify "ProxyServer1" in this field.

For example, if you had the following configuration:

PhoneHome Data Collector -> ProxyServer1 -> ProxyServer2 -> ProxyServer3 -> Database Server

You would add the following entries to `/etc/ssh/ssh_config`:

```
Host ProxyServer2
```

```
ProxyCommand ssh -q em7admin@ProxyServer1 nc %h %p
```

```
Host ProxyServer3
```

```
ProxyCommand ssh -q em7admin@ProxyServer2 nc %h %p
```

```
Host EM7_DB1
```

```
ProxyCommand ssh -q em7admin@ProxyServer3 nc %h %p
```

For another example, if you had the following configuration:

PhoneHome Data Collector -> ProxyServer1 -> ProxyServer2 -> ProxyServer3 -> primary Database Server

PhoneHome Data Collector -> ProxyServer1 -> ProxyServer2 -> ProxyServer3 -> secondary Database Server

You would add the following entries to `/etc/ssh/ssh_config`:

```
Host ProxyServer2
```

```
ProxyCommand ssh -q em7admin@ProxyServer1 nc %h %p
```

```
Host ProxyServer3
```

```
ProxyCommand ssh -q em7admin@ProxyServer2 nc %h %p
```

```
Host EM7_DB1
```

```
ProxyCommand ssh -q em7admin@ProxyServer3 nc %h %p
```

```
Host EM7_DB2
```

```
ProxyCommand ssh -q em7admin@ProxyServer3 nc %h %p
```

7. Save (:wq) your changes to the `/etc/ssh/ssh_config` file.

## Configuring Data Collectors that Connect to the PhoneHome Database Server Through a Proxy

To configure a Data Collector that connect to the PhoneHome Database Server through a Proxy:

1. Either go to the console of the Database Server or use SSH to access the server.
2. Log in as user **em7admin** with the password you configured during setup.
3. For the Database Server, you must first open a port to accept incoming connection requests. To do this, type the following at the shell prompt:

```
sudo phonehome open-control-port <port_number>
```

where `<port_number>` is an unused port number greater than 1024.

4. To define the Data Collector (to the Database Server), type the following at the shell prompt:

```
sudo phonehome add collector
```

The output will look like the following:

```
Created collector: #12
```

```
Changing password for user: "phonehome12"
```

```
Created Device Id: "12"
```

```
Created token: "phonehome://12@10.64.68.31:22/om3Odt3iPEAD"
```

5. Note the token for the Data Collector.
6. Either go to the console of the Data Collector or use SSH to access the server.

**IMPORTANT:** Perform these steps on the Data Collector that will be part of the PhoneHome configuration, *not on the Data Collector that will serve as a proxy server.*

7. Register the Data Collector with the Database Server . To do this, type the following at the shell prompt:

```
sudo phonehome register <token>
```

where *<token>* is the value you noted in step 5.

## Copying the SSH key to Each Proxy

You must now copy the SSH key to each proxy server. To do this:

1. Either go to the console of the Data Collector that will be part of the PhoneHome configuration (not the proxy server) or use SSH to access the server.
2. Log in as user **em7admin** with the password you configured during setup.
3. At the shell prompt, type the following:

```
ssh-copy-id -i /home/phonehome0/.ssh/id_rsa.pub em7admin@[IP_address_of_proxy_server]
```

4. Perform step 3 for each proxy server in your PhoneHome configuration.

## Synchronize the Data Collectors with the Database Server

After adding Data Collector(s) or Message Collector(s) to your PhoneHome configuration, you must execute the sync command on all **Database Servers** in the PhoneHome configuration.

To execute the sync command on all Database Servers:



1. Either go to the console of the Database Server or use SSH to access the server.
2. Log in as user **em7admin** with the password you configured during setup.
3. At the shell prompt, type the following:

```
sudo phonehome sync
```
4. Perform these steps on each Database Server in your PhoneHome configuration.

---

## Deleting a PhoneHome Collector

**IMPORTANT:** This section applies only to SL1 version 11.2.0 and later.

You can delete a PhoneHome SL1 Collector only if it has no corresponding SL1 appliance.

Therefore, to delete a PhoneHome SL1 Collector, you must also perform the following steps, if applicable:

- If the SL1 Collector has a corresponding SL1 appliance, you must delete that appliance before you can delete the SL1 Collector.
- If the corresponding SL1 appliance is included in a collector group, you must delete that collector group before you can delete the appliance and then the SL1 Collector. If there are more than one collectors in the collector group, you can edit the collector group to deselect that collector instead of deleting the collector group.
- If the SL1 appliance's collector group includes other devices, you must move those devices to a different collector group before you can delete the appliance's collector group, then the appliance, and finally the SL1 Collector.

**WARNING:** Once you delete a PhoneHome SL1 Collector, you cannot undelete it. Deleting an SL1 Collector will delete all configuration related to the device and cause all Database Servers to close incoming connections from the device.

To delete a PhoneHome SL1 Collector:

1. Go to the console of the SL1 Collector.
2. Run the following command on the SL1 Collector, replacing `<id>` with the PhoneHome device ID of the device you want to delete:

```
phonehome delete <id>
```



**NOTE:** This command only works for deleting a collector. You cannot use this command to delete a Database Server.

One of the following will occur:

- If the device does not have a corresponding SL1 appliance on the stack, a confirmation prompt appears, asking you to confirm that you want to delete the device. Type "Y" and press Enter. The device is deleted and you can skip the rest of this section.
- If the device does have a corresponding SL1 appliance, a message similar to the following appears:
 

```
Error: Cannot delete a phonehome device that has a corresponding appliance: [Module ID: 10, Name: example-device-cu1, CUG(s): cug-dc09]
```

If you receive an error message, proceed to the next step.

3. Go to the **Appliance Manager** page (System > Settings > Appliances).
4. Locate the device with the **ID** that matches the `Module ID` value that was returned in the error message in step 2, and then do one of the following:
  - If the appliance is not part of a collector group, click its bomb icon () to delete it. You can then repeat steps 1 and 2 to delete the SL1 Collector.
  - If the appliance is part of a collector group, the bomb icon is disabled. Proceed to the next step.
5. Go to the **Collector Group Management** page (System > Settings > Collector Groups).
6. Locate the collector group with the name that matches the `CUG` value that was returned in the error message in step 2, and do one of the following:
  - If the collector group does not contain any devices, click its bomb icon () to delete it. You can then repeat steps 3 and 4 to delete the appliance.
  - If the collector group contains devices, the bomb icon is disabled. Proceed to the next step.
7. Go to the **Device Manager** page (Registry > Devices > Device Manager).
8. Select the checkbox for each device that you want to move to a different collector group.
9. In the **Select Action** field (in the lower right), select *Change Collector Group* and then select a collector group.
10. Click the **[Go]** button. The selected devices will now be aligned with the selected collector group.
11. Repeat steps 5 and 6, and then work your way backwards as needed, completing steps 3 and 4, followed by steps 1 and 2. Repeat these steps as needed until the device is deleted successfully in step 2.

---

## Deleting a PhoneHome Database Server

**IMPORTANT:** This section applies only to SL1 version 11.2.0 and later.

To delete a PhoneHome Database Server:

1. Go to the console of the Database Server that you want to delete.
2. Run the following command:

```
sudo phonehome clear -d
```

A confirmation prompt appears, asking you to confirm that you want to delete the device. Type "delete" and press Enter.

**NOTE:** You must run this command from the Database Server that you want to delete. You cannot run it from any other Database Server or the Administration Portal.

**WARNING:** Once you delete a PhoneHome Database Server, you cannot undelete it. Deleting a Database Server will delete all configuration related to the device and close all incoming connections from PhoneHome SL1 Collectors.

---

## Using the Watchdog Service with SL1 11.1.x and Earlier

**IMPORTANT:** This section applies only to SL1 version 11.1.x and earlier.

Each Database Server, Data Collector and Message Collector in a PhoneHome configuration runs a service called watchdog. The watchdog process automatically checks the connection between the Data Collector or Message Collector and the Database Server. If the connection is stale, the watchdog service automatically forces the Database Server to reconnect to the Data Collector or Message Collector.

The watchdog service can also detect configuration changes. If the PhoneHome configuration changes, the watchdog service will detect the changes and synchronize the configuration data on each device in the PhoneHome configuration.

The watchdog service is started automatically on each Data Collector, Message Collector, and secondary Database Server.

To view information about the watchdog service:

1. Log in to the console of the Data Collector, Message Collector, and secondary Database Server as the root user.
2. At the command line, type the following:

```
phonehome watchdog view
```

3. You should see something like the following:

```
Current settings:
```

```
autosync: yes
```

```
interval: 20
```

```
state: enabled
```

```
autoreconnect: yes
```

```
timeoutcount: 2
```

```
check: default
```

4. You can change any of these settings by typing the following at the command line:

```
phonehome watchdog set -settingvalue
```

where *setting* is one of the settings displayed with the view command and *value* is the value to assign to that setting.

5. For details about the watchdog service, type the following at the command line:

```
phonehome watchdog help
```

For details about the arguments and settings for watchdog, see the section on [Using the Command Line Interface](#).

---

## Logging PhoneHome Configuration Information

**IMPORTANT:** This following section applies only to SL1 version 11.2.0 and later.

In SL1 version 11.2.0 and later, the server hosts are stored in the **journald** log for the **phd** service on the Database Server and in the **journald** log for the **phc** service on the Collector.

To view those logs, run the following commands on the Database Server or Collector:

```
sudo journalctl -u phd.service
```

```
sudo journalctl -u phc.service
```

## Viewing PhoneHome Logs in SL1 version 11.1.x and Earlier

**IMPORTANT:** The following section applies only to SL1 version 11.1.x and earlier.

The PhoneHome configuration logs information to the following files:

- **`/var/log/phonehome/phonehome0.log`**. Resides on each device in the PhoneHome configuration. This log file stores the date and time that devices are added to or removed from the PhoneHome configuration and each configuration action, including token generation, device registration, and configuration data synchronization, performed for each device. This log is rotated daily.
- **`/var/log/phonehome/phonehome<device ID>.log`**. Resides on the Database Server. This log file stores an entry for each action requested by or performed on a specific device (specified by device ID). This log is rotated daily.
- Log files that store information about registration operations and periodic checks performed by the Data Collectors reside in the directories listed below. These log files are auto-rotated when they exceed 10MB.
  - `/var/log/ph_shell_collector`. Contains shell logs from users in group em7-ph-collectors (Data Collectors).
  - `/var/log/ph_shell_local`. Contains shell logs for users in group em7-ph-local (the phonehome0 and phonehomerequest users).
  - `/var/log/ph_shell_database/`. Contains shell logs for users in group em7-ph-cdb (Database Servers)
  - `/var/log/phonehome/commands.log`. Stores the log entries about each phonehome command executed on that appliance.
  - `/var/log/phonehome/`
- **`/var/log/phonehome/ph_watchdog.log`**. Resides on the Database Server. This log file stores information about the watchdog service. This log is rotated daily.

---

## Using the Command-Line Interface for PhoneHome Collection in SL1 Version 11.2.0 and Later

If you have access to the console for each appliance in the PhoneHome configuration, or if you have SSH access to each appliance in the PhoneHome configuration, you can use the **phonehome** command to configure and troubleshoot your PhoneHome configuration.

**IMPORTANT:** The following list of commands includes new commands that were available with SL1 version 11.2.0 and later. The new server and client does not use OpenSSH tooling. If you are running a version of SL1 earlier than 11.2.0, see [Using the Command-Line Interface for PhoneHome Collection in SL1 Version 11.1.0 and Earlier](#).

To use the **phonehome** command:

1. Either go to the console of the SL1 appliance or use SSH to access the server. Log in as "root".
2. At the command prompt, type the following:

```
phonehome <command>
```

where `<command>` is one of the following commands:

- `clear`. Clears the PhoneHome configuration on a PhoneHome device.
- `check`. Checks the state of the connection from an SL1 Collector to the Database Server, visualizing the network path from the SL1 Collector to the Database Server as well as any proxy hops in between, if applicable. The output indicates any failures connecting to any hop.
- `client`. Runs the PhoneHome client (installed as a systemd service `phc`). New in SL1 11.2.0.
- `config`. Displays and enables you to edit PhoneHome configuration related to the server and client. New in SL1 11.2.0.
- `delete`. Deletes a PhoneHome SL1 Collector. This argument prevents you from deleting any SL1 Collector with an associated SL1 appliance.
- `destination`. Enables you to add, remove, or view addresses to a PhoneHome Database Server. New in SL1 11.2.0.
- `forwards`. Enables you to add, remove, or view ports forwarded from an SL1 Collector to the Database Server. New in SL1 11.2.0.
- `list`. Displays a list of PhoneHome devices (Database Servers and Collectors). New in SL1 11.2.0.
- `migrate`. Migrates the configuration from the classic PhoneHome setup to the new PhoneHome setup. This is done automatically during upgrade. New in SL1 11.2.0.
- `proxy`. Enables you to add, remove, or view proxy configurations along the network path from an SL1 Collector to the Database Server. New in SL1 11.2.0.
- `register`. Registers a new SL1 Collector as a PhoneHome collector with a token.
- `rename`. Renames an existing Phone Home device: `phonehome rename <new name>`. Previously this was available with the `phonehome set <id>` command
- `request`. Enables you to send, view, accept, or reject an SL1 Collector registration request. New in SL1 11.2.0.
- `server`. Runs the PhoneHome server (installed as a systemd service `phd`). New in SL1 11.2.0.
- `setup`. Configures a new PhoneHome Database Server. New in SL1 11.2.0.
- `status`. Displays the status of the PhoneHome SL1 Collectors. The output is tabular by default but supports JSON output as well. The output does not contain the remote loopback IP address of PhoneHome SL1 Collectors, nor does it list PhoneHome Database Servers.
- `sync`. Syncs the configuration from the Database Server. This command does not restart the SSH tunnel to the Database Server.
- `token`. Enables you to create, view, or delete registration tokens. New in SL1 11.2.0.
- `view`. Displays the state of an SL1 Collector. This argument must be run on a Database Server.

## Additional New Command-line Features in SL1 version 11.2.0

The following features are new or updated in SL1 version 11.2.0 or later:

- Adding a Database Server or Collector does not require the creation of users on the operating system of the Database Server.
- The authentication of the server and client happens over the configuration store in MariaDB on the server, rather than flat files on the filesystem of the Database Server.
- There is no notion of a control node. Every Database Server in a HA/DR setup can participate in all operations.
- You can assign multiple addresses to a destination if required. The list of addresses can be a mix of IPv4 and DNS names.
- There is now a command in the command-line interface to manage proxy configuration that validates and assists in setting up proxy.
- Onboarding a PhoneHome Collector automatically adds a corresponding SL1 Appliance and also adds it to the predefined SL1 Collector Group.
- For the token registration workflow, the token is a signed JSON Web Token (JWT) that expires after a predefined time from the time of generation. The token expires after 30 minutes by default, but it can be extended to a maximum of 2 hours. The token encodes all destination addresses
- To generate a token, you now need to execute the `phonehome token new` command. You need to know the model type, collector group ID, name, and description of the collector you are trying to onboard.
- The token request workflow includes the following:
  - A collector registration request does not expire until it is deleted by a database administrator.
  - Creates a one-time password to accept a request. This one-time password must be shared with the database administrator so that the administrator can accept the request
  - An additional human-friendly identifier or label can be passed along with the request to uniquely identify the request
- The control of port forwarding is with the collector administrator. A PhoneHome collector forwards the local MariaDB port (7707) by default. The collector administrator can forward other local ports as needed. The database cannot instruct the collector to forward an arbitrary port.
- When setting up a Database Server, the `open-control-port` command is no longer available. The `setup` command creates a PhoneHome device in the config store along with its corresponding RSA host key. It also adds the default non-loopback IP corresponding to the hostname as the default destination address. The user can define a custom destination address if required. The command also adds a firewall rule to allow incoming connections on the specified port and labels it as SSH port (`ssh_port_t`) in the SELinux subsystem.
- Systemd services:
  - The `em7_ph_tunnels` service is no longer available, and it was replaced by the `phc` (phonehome client) service.
  - The OpenSSH service for the control port is replaced by the `phd` service. OpenSSH will not be listening anymore on the control port after the migration.
  - The `em7_ph_watchdog` is no longer available. Both the server and client run in-process watchdog in separate threads.

---

## Tuning PhoneHome Settings in SL1 Version 11.2.0 and Later

A PhoneHome setting is a customizable configuration that impacts how a PhoneHome server or client behaves. Some settings impact both the server and client; others are localized to either just the server or just the client.

**NOTE:** Updated PhoneHome settings do not take effect until the PhoneHome server or client is restarted or the next watchdog cycle occurs.

### Viewing a List of Current PhoneHome Settings

**IMPORTANT:** This section applies only to SL1 version 11.2.0 and later.

To view a list of current PhoneHome settings:

1. Go to the console of the SL1 Collector or Database Server.
2. Run the following command on the SL1 Collector or Database Server:

```
phonehome config list
```

When you run the command, the system returns a list that includes each configuration setting, its value, a description, and an indication of whether the setting affects the client, the server, or both.

### Updating PhoneHome Settings

**IMPORTANT:** This section applies only to SL1 version 11.2.0 and later.

To set a new value for an existing PhoneHome setting:

1. Go to the console of the SL1 Collector or Database Server.
2. Run the following command on the SL1 Collector or Database Server:

```
phonehome config set <setting_name> <new_value>
```

For example, if you want to change the client timeout value to 30 seconds, you would run the following command:

```
phonehome config set client_timeout 30s
```

You can update the following settings:



| Configuration                   | Setting                                 | Description                                                                                                                                                                                                                                                                                                | Default Value | Affects |
|---------------------------------|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|---------|
| Client Timeout                  | <code>client_timeout</code>             | Maximum amount of time allowed for the client to connect to a Database Server, after which the connection times out. The value is an actual time value, such as 30s, 5m, or 2h.                                                                                                                            | 30s           | Client  |
| Exit on Forward Failure         | <code>exit_on_forward_failure</code>    | Indicates whether to close the connection to the Database Server if any custom ports fail to forward. This is not applicable to MariaDB port forwarding (port 7707). If the MariaDB port fails to forward, the client closes the connection regardless of this setting. The value is either true or false. | false         | Client  |
| Watchdog Frequency Duration     | <code>watchdog_freq</code>              | Amount of time between watchdog service cycles. The value is an actual time value, such 30s, 5m, or 2h.                                                                                                                                                                                                    | 1m0s          | Both    |
| Port Ping Timeout               | <code>port_ping_timeout</code>          | Maximum allowed time for a Database Server's watchdog to connect to the forwarded port before it marks the SL1 Collector as disconnected and closes the incoming client connection. The value is an actual time value, such as 30s, 5m, or 2h.                                                             | 10s           | Server  |
| Token Time to Live (TTL)        | <code>token_ttl</code>                  | Default amount of time a token is valid before it expires. The value is an actual time value, such as 30s, 5m, or 2h. The maximum value is 2h.                                                                                                                                                             | 30m0s         | Server  |
| Expired Token Cleanup Frequency | <code>expired_token_cleanup_freq</code> | Amount of time after which an expired token is deleted by the server. The value is an actual time value, such as 30s, 5m, or 2h.                                                                                                                                                                           | 48h0m0s       | Server  |

## Using the Command-Line Interface for PhoneHome Collection in SL1 Version 11.1.x and Earlier

If you have access to the console for each appliance in the PhoneHome configuration, or if you have SSH access to each appliance in the PhoneHome configuration, you can use a shell session and the **phonehome** command to configure and troubleshoot your PhoneHome configuration.

### The phonehome Command

To use the **phonehome** command:

1. Either go to the console of the SL1 appliance or use SSH to access the server. Log in as "root".
2. At the command prompt, you can type the following:

## **phonehome** *argument*

where *argument* is one of the following:

- **add** *appliance\_type* or *request\_file*. Run this command on the primary Database Server. Adds an appliance to the current PhoneHome configuration.

**IMPORTANT:** This command is not available in SL1 version 11.2.0 or later; in this situation, use the token or the request workflows.

- *appliance\_type*. Type one of the following:
  - *collector*. Adds a Data Collector or Message Collector to the PhoneHome configuration.
  - *database*. Adds a primary Database Server or a secondary Database Server to the PhoneHome configuration.
- *request\_file*. When the Data Collector or Message Collector sends a request to the Database Server, the Database Server creates a request file in the directory **/home/phonehomerequest/requests**. You can specify the full pathname of a request file to accept a request and add a new Data Collector or Message Collector to the PhoneHome configuration.

**NOTE:** The **phonehome add request\_file** command performs the same operations as selecting the **[ Accept ]** button for a request in ScienceLogic Web Configuration Utility.

- **check -json** *yes*. Run this command on any appliance in the PhoneHome configuration. Executes diagnostic steps to aid in troubleshooting.
  - **-json** *yes*. Displays output in json format.

The **phonehome** command first tries to connect to the primary Database Server.

If you issue this command from a Database Server, the command checks the status of the database port, the SSH port, and port for the web configuration tool for each Data Collector and Message Collector.

If you issue this command from a Data Collector or Message Collector, the command checks the status of the database port, the SSH port, and port for the web configuration tool for each Database Server.

- **clear** *clear\_type*. Clears the PhoneHome configuration, as specified in the *clear\_type* argument.
  - *clear\_type*. Specifies which configuration to remove. Can be one of the following:
    - *client*. Run this command on the secondary Database Server, Data Collector, or Message Collector. Removes the PhoneHome connection (SSH tunnel). The appliance can then no longer connect to the primary Database Server.
    - *users*. Run this command on the primary Database Server. Removes the PhoneHome configuration for all appliances except the primary Database Server.
    - *all*. Run this command on the primary Database Server. Removes the PhoneHome configuration for each Data Collector, Message Collector, secondary Database Server, and the primary Database Server.
- **close-control-port** *port\_number*. Run this command on Database Servers (primary and secondary). Blocks future connection requests from Data Collectors and secondary Database Servers.

**IMPORTANT:** The **close-control-port** command is not available in SL1 version 11.2.0 or later; in this situation, use the **clear** command on a Database Server.

- **connect**. Run this command from the Data Collectors, Message Collectors, or secondary Database Server. Starts communication between the primary Database Server and the Data Collector, Message Collector, or secondary Database Server.
- **delete** *appliance\_ID*. Run this command on the primary Database Server. Deletes an appliance from the current PhoneHome configuration.
  - *appliance\_ID*. Enter the numeric ID of the appliance. You can find this ID with the **phonehome status** command.
- **disconnect**. Run this command from the Data Collector(s), Message Collector(s), or secondary Database Server. Stops communication between the primary Database Server and the Data Collector, Message Collector, or secondary Database Server.
- **help**. Run this command from any appliance in the PhoneHome configuration. Displays information about each parameter for the phonehome command.
- **help extra**. Run this command from any appliance in the PhoneHome configuration. Displays information about the basic steps to configure a PhoneHome configuration.

- **mysql** *appliance\_id*. Run this command on the primary Database Server. Tests the connection to the MySQL database. If the *appliance\_ID* specifies a Data Collector or Message Collector, the **phonehome** command will test the MySQL connection using the loopback address of the Data Collector or Message Collector and port 7707. If the *appliance\_ID* specifies a Database Server, the **phonehome** command will test the MySQL connection using the public IP address of the Database Server and port 7706.
  - *appliance\_ID*. Enter the numeric ID of the appliance. You can find this ID with the **phonehome status** command.
- **open-control-port** *port\_number*. Run this command on Database Servers (primary and secondary). Adds an entry for the specified SSH port to the /etc/sysconfig/iptables file on the current server.

**IMPORTANT:** This command is not available in SL1 version 11.2.0 or later; in this situation, use the **setup** command on a Database Server.

- **reconnect**. Run this command from the Data Collector(s), Message Collector(s), or secondary Database Server. Stops and then restarts communication between the primary Database Server and the Data Collector(s), Message Collector(s), or secondary Database Server.
- **register** *device\_token*. Run this command from the Data Collector(s), Message Collector(s), or secondary Database Server. Registers the appliance with the primary Database Server.

After you generate a **token** for a Data Collector or Message Collector (either with **phonehome token** or **phonehome add**), go to the Data Collector or Message Collector and use the **phonehome register** command to register the Data Collector or Message Collector with the primary Database Server. The Data Collector or Message Collector will then upload its public key to the primary Database Server and download its configuration for PhoneHome from the primary Database Server. After executing this command, the Data Collector or Message Collector will automatically connect to the Database Server.

In configurations that have multiple Database Servers: After you generate a **token** for a secondary Database Server (either with **phonehome token** or **phonehome add**), go to the secondary Database Server and use the **phonehome register** command to register the secondary Database Server with the primary Database Server. The secondary Database Server will then upload its public key to the primary Database Server and download its configuration for PhoneHome from the primary Database Server.

- *device\_token*. Enter the token you generated for the Data Collector, Message Collector, or secondary Database Server.
- **reload**. Can be run on any appliance in the PhoneHome configuration. Stops the em7\_sshd and em7\_ph\_service processes, finds and applies any configuration changes, and restarts the service.

- **request** [*protocol*]://[*database\_IP*] [*no\_verify*]. Run this command from the Data Collector or Message Collector to send a request to the Database Server.
  - *protocol*. Enter the protocol to use to send the request to the Database Server. Choices are *phonehome* or *https*.
  - *database\_IP*. The IP address of the Database Server in the PhoneHome configuration.
  - *no\_verify*. Optional. If you specified *https* in the **protocol** option, you can specify **no\_verify** to disable SSL verification.

**NOTE:** The **phonehome request** command performs the same operations as sending a request to the Database Server from the ScienceLogic Web Configuration Utility. Specifying **no\_verify** performs the same operation as not selecting the **Verify SSL Cert** checkbox.

You can use the **phonehome request** command and the **phonehome add request\_file** command to add a Data Collector or Message Collector to a PhoneHome Configuration. Go to the Data Collector or Message Collector and use the **phonehome request** command to send a request to join the PhoneHome configuration. Go to the Database Server and use the **phonehome add request\_file** command to accept the request from the Data Collector or Message Collector. Go to the Data Collector or Message Collector again and execute the **phonehome request** command a second time to retrieve the request approval and set up the connection.

- **set appliance\_ID -parameter=value**. Run on the primary Database Server. For a specific device, assigns a value to a parameter:
  - *appliance\_ID*. Enter the numeric ID of the appliance. You can find this ID with the **phonehome status** command.
  - *parameter*. Can be one of the following parameters, preceded by a dash:
    - *name*. Specifies the name of the device in the **Name** field in the Web Configuration Utility.
    - *ssh*. Specifies whether or not to enable port forwarding for the SSH port for this device. Possible values are "yes" or "no".
    - *ip*. Specifies the IP address of the device in the **IP Address** field in the Web Configuration Utility.
    - *forwards*. Enables port forwarding for one or more ports. Specify one or more port numbers, separated by a space.

- *value*. Value to assign to the parameter, surrounded by double quotes.

For example:

```
phonehome set 11 -ssh yes -name "Reston"
```

- This example affects the device with an appliance ID of "11".
- The example enables port forwarding for SSH.
- The example enables port forwarding for the Web Configuration Utility.
- The example sets the device's device name to "Reston".
- **ssh *appliance\_id***. Run on the primary Database Server. Tests the SSH connection to the specified appliance. If the *appliance\_ID* specifies a Data Collector or Message Collector, the **phonehome** command will test the SSH connection using the loopback address of the Data Collector or Message Collector and port 10022. If the appliance ID specifies a Database Server, the **phonehome** command will test the SSH connection using the public IP address of the Database Server and defined SSH port.
  - *appliance\_ID*. Enter the numeric ID of the appliance. You can find this ID with the **phonehome status** command.
- **status**. Can be run on any appliance in the PhoneHome configuration. Displays the name and status of each currently defined PhoneHome appliance.
- **sync**. Run this command from the Data Collectors or Message Collectors. Downloads the current configuration for PhoneHome from the primary Database Server to the Data Collector or Message Collector.
- **token *appliance\_ID***. Run this command from the primary Database Server. This command creates a URL that allows the Data Collector(s), Message Collector(s), or secondary Database Server to log in to the primary Database Server, upload a public key to the primary Database Server, and download the configuration for PhoneHome from the primary Database Server.
  - *appliance\_ID*. Enter the numeric ID of the Data Collector, Message Collector, or secondary Database Server. You can find this ID with the **phonehome status** command.
- **view *appliance\_id* -json *yes***. Run this command from the primary Database Server. Displays the name, type, loopback IP, port status, revision number, and SSH status of the Data Collector, Message Collector, or secondary Database Server specified in *appliance\_ID*.
  - *appliance\_ID*. Enter the numeric ID of the appliance that you want. You can find this ID with the **phonehome status** command.
  - **-json *yes***. Displays output in json format.

- **wake** *appliance\_id*. Run this command from the primary Database Server. Depending on the specified *appliance\_ID*, stops and then restarts communication between the Database Server and the Data Collector, Message Collector, or secondary Database Server.
  - *appliance\_ID*. Enter the numeric ID of the appliance that you want. You can find this ID with the **phonehome status** command.
- **watchdog option**. Run this command from the Data Collector, Message Collector, or secondary Database Server. The watchdog service runs automatically on each Data Collector, Message Collector, or secondary Database Server and checks the connection to the primary Database Server. If the connection is stale, the watchdog service automatically forces the primary Database Server to reconnect to the Data Collector, Message Collector, or secondary Database Server. The watchdog service can also detect configuration changes. If the PhoneHome configuration changes, the watchdog service will detect the changes and synchronize the configuration data on each device in the PhoneHome configuration.

**NOTE:** The **watchdog** and **autosync** services are not available for versions of SL1 **earlier than the 7.5.3 ISO**.

You can use this command to control the watchdog service. The options are:

- **start**. Starts the PhoneHome watchdog service.
- **stop**. Stops the PhoneHome watchdog service.
- **status**. Gets the status of the PhoneHome watchdog service.
- **view**. Displays the current settings for the watchdog service.
- **set -parameter value**. Sets the value of a parameter for the watchdog service. Parameters are:
  - **interval seconds**. Specify the interval, in seconds, at which to execute the watchdog service. The default value is "50".
  - **autosync (yes, no)**. Specifies whether or not you want the watchdog service to cause configuration data to be synchronized automatically at regular intervals.
  - **autoreconnect (yes, no)**. Specifies whether or not you want the watchdog service to reconnect stale connections automatically.
  - **state (enabled, disabled)**. Specifies whether or not the watchdog service is running.
  - **timeoutcount number**. Specifies the number of failed calls to the watchdog service before stopping and restarting the watchdog. The default value is "3".
  - **check (ssh, db, default)**. Specifies which port the watchdog service checks. The default value is "db".
  - **run -verbose (yes, no)**. Manually starts the watchdog service if it is not already running.
  - **-verbose (yes, no)**. Specifies whether or not to display verbose logging to standard output.

## The monitor\_phonehome Command

The `monitor_phonehome` utility is available to use when debugging or diagnosing PhoneHome related issues. It is especially useful when escalating a PhoneHome issue to ScienceLogic Support.

---

# Troubleshooting the PhoneHome Configuration in SL1 Version 11.1.x and Earlier

## Using the PhoneHome Troubleshooting Script

The troubleshooting tool for PhoneHome provides diagnostics about the connection between a Data Collector and a Database Server in the PhoneHome system.

**IMPORTANT:** This section applies only to SL1 version 11.1.0 and earlier.

To use the troubleshooting tool:

1. Either go to the console of a Data Collector or use SSH to access the Data Collector.
2. Enter the following at the shell prompt:

```
sudo phtb -h
```

## Available Commands

- This command checks the SSH connectivity between the Data Collector and the PhoneHome primary Database Server

```
sudo phtb destination
```

- If the connection is healthy, the output looks like this:

```
Executing phonehome destination check
```

```
Running check for destination with host 52.70.238.48, port 7705,
user phonehome13
```

```
=====
=====
```



```
Remote server 52.70.238.48 reported back the status of this device
(check command): [Status: forwarded, Summary: db (Alive),
Phonehome status: operational]
```

```
SSH test to destination (Name: Phone Home database 11, IP:
52.70.238.48, Port: 7705) is successful
```

```
Destination check summary: [Total: 1, Skipped: 0, Success: 1,
failed: 0]
```

- If the connection is not healthy, the output looks like this:

```
Executing phonehome destination check
```

```
Running check for destination with host 10.152.2.100, port 7705,
user phonehome13
```

```
=====
=====
```

```
Failed to check destination 10.152.2.100 on port 7705. Error: dial
tcp 10.152.2.100:7705: i/o timeout
```

```
Destination check summary: [Total: 1, Skipped: 0, Success: 0,
failed: 1]
```

- This command checks the SSH credentials.

```
sudo phtb probe-host <hostname or IP address of server> <port number>
<username> <-p password or -k path to private key> <options>
```

- Here is an example with output for correct credentials:

```
phtb probe-host 52.70.238.48 7705 phonehome13 -k
/home/phonehome0/.ssh/id_rsa.pub
```

```
Executing probe for host 52.70.238.48 on port 7705
```

```
Successfully established SSH connection to host 52.70.238.48 on
port 7705
```

- Here is an example with output for incorrect credentials:

```
phtb probe-host 52.70.238.48 7705 em7admin -p badpassword
```

```
Executing probe for host 52.70.238.48 on port 7705
```

```
Failed to obtain SSH connection to host 52.70.238.48 on port 7705.
Error: ssh: handshake failed: ssh: unable to authenticate,
attempted methods [none], no supported methods remain
```

- This command verifies the connection to a proxy server.

```
sudo phtb proxy <hostname or IP address of server> <port number>
<optional -u username>
```

- Here is an example with output for "no proxy found":

```
sudo phtb proxy 52.70.238.48 7705
```

```
Executing proxy check for host 52.70.238.48, port 7705
```

```
There is not any proxy configured for host 52.70.238.48. No
further action needed.
```

## Basic Troubleshooting

| Problem                                  | Possible Cause                                                                                     | Diagnostics                                                                                                                                                                                                                           |
|------------------------------------------|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Can't register a server or sync a server | Confirm that the Data Collector can "see" the phonehome port on the Database Server.               | At the command line of the server that can't sync or register:<br><pre>nmap -p port_number IP_ address_of_database_server</pre> For example:<br><pre>nmap -p 7705 71.197.6.197</pre>                                                  |
| Can't register a server or sync a server | Confirm that the PhoneHome port is open on the firewall on the Database Server.                    | At the command line of the Database Server:<br><pre>iptables -nL</pre> You should see output that specifies that the port accepts connections.<br>To open the port, run this command:<br><pre>sudo phonehome open-control- port</pre> |
| Can't register a server or sync a server | Ensure that the Data Collector has line-of-sight with the Database Server                          | <pre>sudo tcptraceroute &lt;IP_address_ of_database&gt;</pre>                                                                                                                                                                         |
| Can't register a server or sync a server | Ensure the Data Collector can initiate an SSH session to the phonehome port on the Database Server | <pre>sudo -u phonehome0 -s ssh -vvv - o StrictHostKeyChecking=no -p &lt;control_port_(usually_7705)&gt; phonehome&lt;device_id_of_ collector&gt;@&lt;IP_address_of_ database&gt;</pre> Output should include:                         |

| Problem                                                                                               | Possible Cause                                                                                                     | Diagnostics                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                       |                                                                                                                    | <ul style="list-style-type: none"> <li>Remote server string which specifies a version of OpenSSH</li> <li>SL1 trying various authentication methods until one succeeds or fails</li> <li>If authentication is attempted, this means that the Data Collector can establish a TCP connection on the control port to the Database Server</li> </ul>                                                                                                                        |
| Can't register a server                                                                               | Ensure that tunnel service is running on the Data Collector.                                                       | <pre>sudo systemctl status em7_ph_tunnels.service</pre> <p>If the services is not running, force a sync using the following command:</p> <pre>sudo phonehome sync</pre>                                                                                                                                                                                                                                                                                                 |
| Problem with authentication                                                                           | Ensure that the Data Collector is registered with the Database Server.                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Problem with authentication                                                                           | Check that that the public keys of the Data Collector (/home/phonehome0/.ssh/id_rsa.pub) are configured correctly. | <p>Ensure that the public keys of the Data Collector(/home/phonehome0/.ssh/id_rsa.pub) are present in the following places:</p> <p>On the Database Server, in /home/phonehome&lt;id&gt;/.ssh/authorized_keys</p> <p>On the Database Server, in /home/phonehome&lt;id&gt;/remote_key file</p> <p>On the Database Server, in the database table sysinfo..phonehome_devices, find the row for the Data Collector. The <b>pub</b> column should contain the public keys</p> |
| Forgot to copy the token for a server                                                                 |                                                                                                                    | <pre>phonehome token appliance_ID</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Confirm that Data Collector (s) and/or Message Collector(s) are successfully configured for PhoneHome |                                                                                                                    | <p>At the command line of the Database Server:</p> <pre>netstat -an  grep -i listen  grep "127.0.0."  grep 7707</pre> <p>Output displays each Data Collector and Message Collector that is listening for PhoneHome communications.</p>                                                                                                                                                                                                                                  |

---

# Chapter

# 10



## Installing SL1 on AWS

---

### Overview

This chapter describes how to install SL1 on an Amazon Web Services EC2 instances. An instance is a virtual server that resides in the AWS cloud.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ().
- To view a page containing all of the menu options, click the Advanced menu icon (  ).

This chapter covers the following topics:

|                                                               |     |
|---------------------------------------------------------------|-----|
| <i>AWS Instance Specifications</i> .....                      | 141 |
| <i>Deploying an SL1 System on AWS</i> .....                   | 141 |
| <i>What are the ScienceLogic AMIs?</i> .....                  | 141 |
| <i>Getting the ScienceLogic AMI</i> .....                     | 142 |
| <i>Launching the New Instance</i> .....                       | 144 |
| <i>Security Rules for Each Appliance Type</i> .....           | 150 |
| <i>Additional Configuration Steps</i> .....                   | 159 |
| <i>Assigning an EIP to the New Instance</i> .....             | 160 |
| <i>Accessing the Appliance Using SSH</i> .....                | 162 |
| <i>Web Configuration Tool</i> .....                           | 164 |
| <i>Rebooting Data Collectors and Message Collectors</i> ..... | 164 |

**NOTE:** For more information about monitoring Amazon Web Services in SL1, see the *Monitoring Amazon Web Services* manual.

---

## AWS Instance Specifications

For details about AWS and the requirements and specifications for each SL1 appliance, see the ScienceLogic Support Site: <https://support.sciencelogic.com/s/system-requirements?tabset-e65a2=f5872>.

---

## Deploying an SL1 System on AWS

For ease of configuration, create nodes or appliances in this order:

1. Database Server
2. Administration Portal (if applicable)
3. Data Collectors
4. Message Collectors (if applicable)

**NOTE:** The following instructions describe how to configure a ScienceLogic virtual machine in AWS. If you are looking for resources and support for AWS Cloud, see the Amazon AWS Marketplace: <https://aws.amazon.com/marketplace/>.

---

## What are the ScienceLogic AMIs?

An instance is a virtual server that resides in the AWS cloud. An Amazon Machine Image (AMI) is the collection of files and information that AWS uses to create an instance. A single AMI can launch multiple instances.

For details on AMIs, see <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html>.

The ScienceLogic AMIs are defined by ScienceLogic. ScienceLogic has created an AMI for each type of ScienceLogic appliance. You can use a ScienceLogic AMI to create Elastic Compute Cloud (EC2) instances for each type of ScienceLogic appliance.

**NOTE:** Elastic Compute Cloud (EC2) instances are virtual servers that come in a variety of configurations and can be easily changed as your computing needs change. For more information on EC2, see <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html>.

The ScienceLogic AMIs are private and are for ScienceLogic customers only. After you collect specific information about your AWS account, you can send a request (and the collected information) to ScienceLogic, and ScienceLogic will share the ScienceLogic AMIs with you.

**NOTE:** As of 8.10.0 and later releases, ScienceLogic AMIs support Enhanced Network Adapters (ENAs).

---

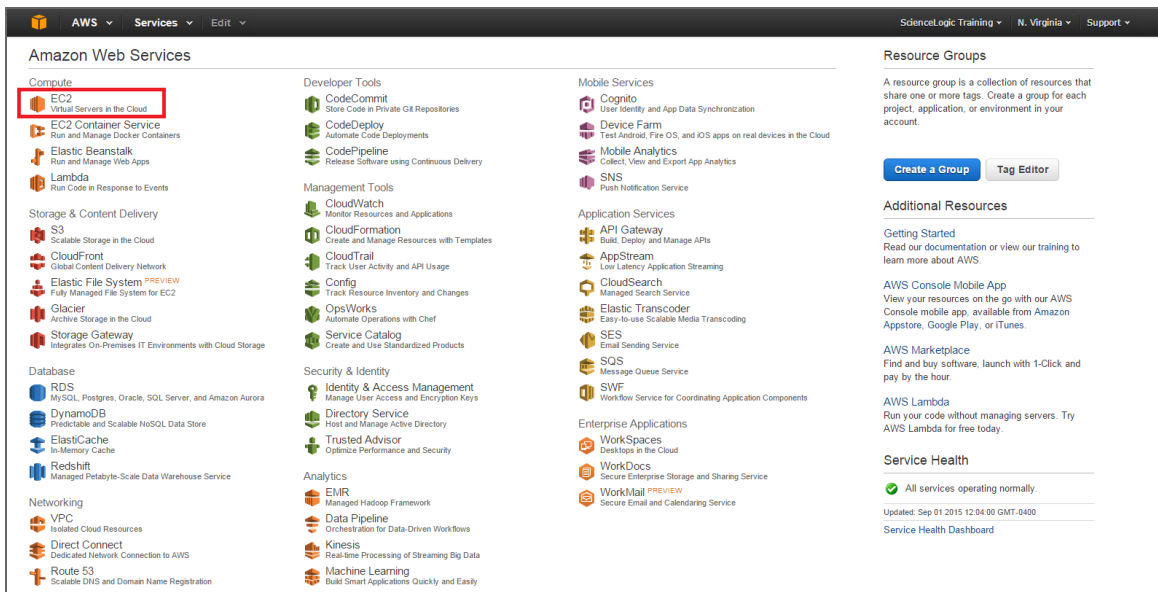
## Getting the ScienceLogic AMI

To get access to the ScienceLogic AMIs:

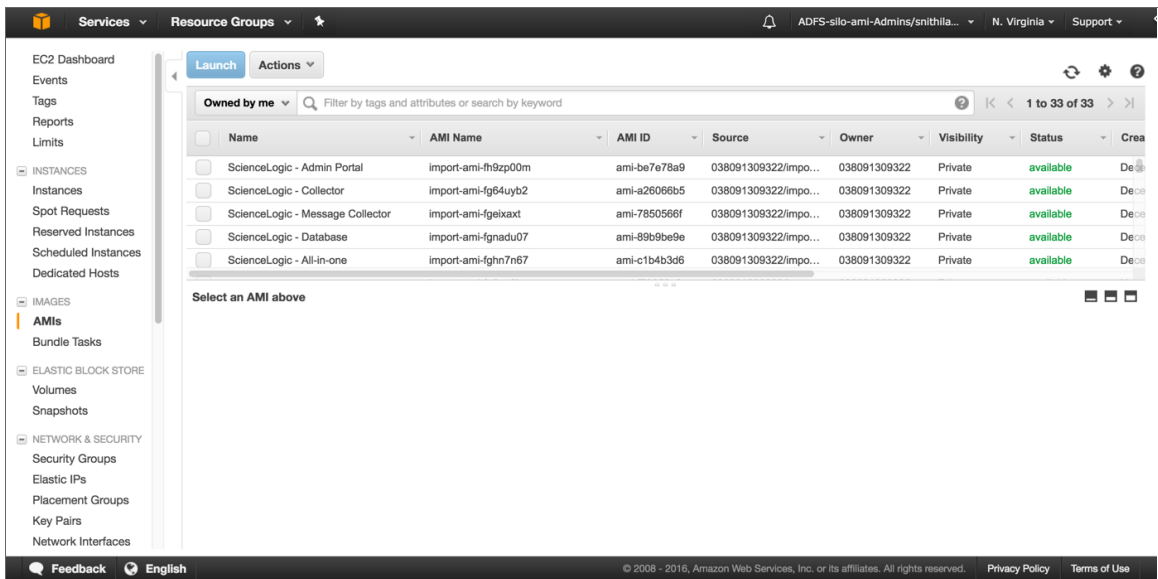
1. Log in to the [ScienceLogic Support Site](#).
2. Go to the **Product Downloads** menu and select *License Request*. The **Request a ScienceLogic License** page appears.

**NOTE:** If you are an Amazon Web Service GovCloud user, you will need to contact ScienceLogic Support to get the ScienceLogic AMI.

3. Scroll down to the **AMI Request** section and click the **[Submit AMI Request]** button. The **Request Amazon AMI** page appears.
4. Fill out the **Request Amazon AMI** form and click the **[Submit AMI Request]** button.
5. Repeat steps 2-4 for each type of SL1 appliance you want to install on AWS.
6. ScienceLogic Customer Support will send you an email confirming that they have shared the ScienceLogic AMI with your AWS account.
7. To view the ScienceLogic AMIs in your AWS account, go to the **AWS Management Console** page. Under the heading **Compute**, click **[EC2]**.

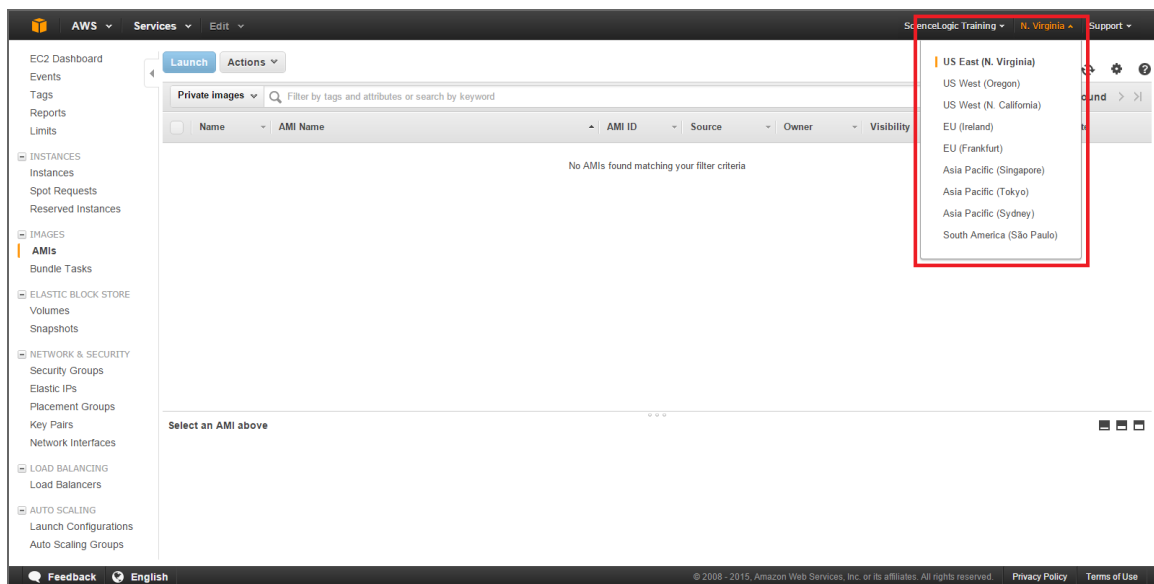


8. In the **EC2 Dashboard** page, go to the left navigation bar. Under the heading **Images**, click **[AMIs]**.
9. In the main pane, under **Filters**, click **[Owned by me]** and then select **Private images**.
10. You should see AMIs with names that begin with "EM7" and end with the current release number for SL1. You should see an AMI for each type of SL1 appliance.



11. If you do not see AMIs with names that begin with "EM7", your EC2 Dashboard might have a default region that does not match the region for the ScienceLogic AMIs. To change the current region in the EC2 dashboard, click the region pull-down in the upper right and choose another region. Do this until you find the ScienceLogic AMIs.

**NOTE:** A region is a geographic location. AWS has data centers that include multiple regions. You can specify that an instance reside in a specific region. For more details on regions, see <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>.



## Launching the New Instance

To complete the steps listed in this chapter, you must have *received the ScienceLogic AMIs*.

This chapter assumes that you will launch each new EC2 instance into a VPC subnet with a primary IP address that is static and private.

**NOTE:** For more information on VPCs and VPC subnets, see [http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC\\_Introduction.html](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html).

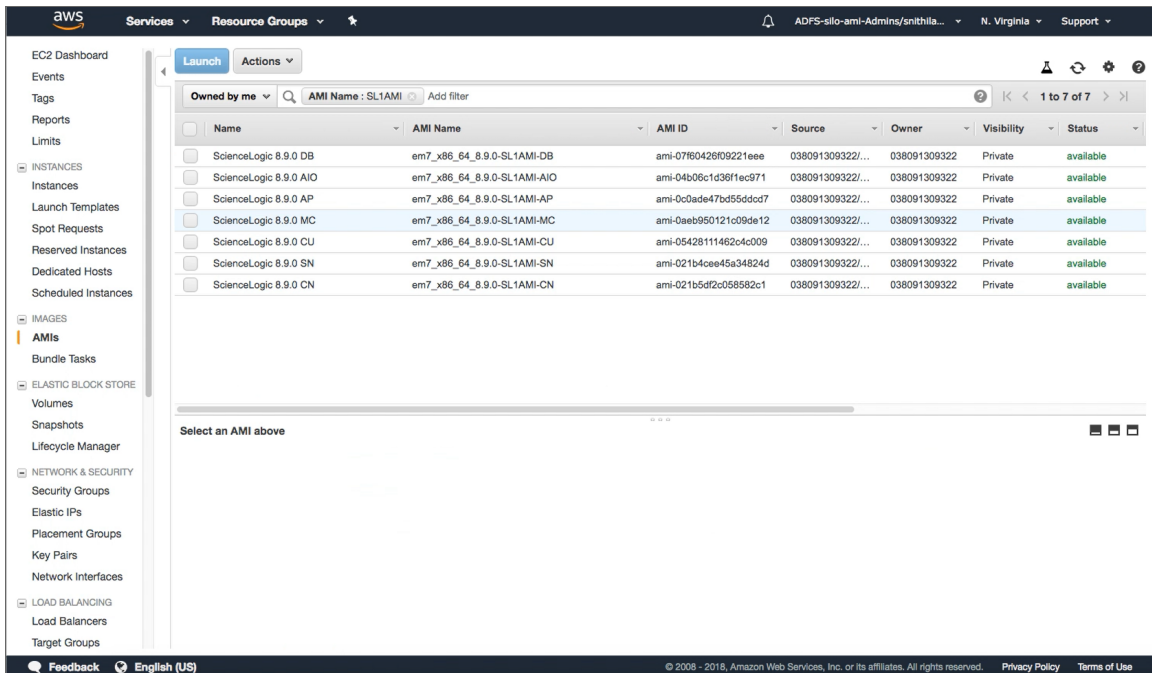
For details about the recommended instance type for each ScienceLogic appliance, see System Requirements page on the [ScienceLogic Support Site](#).

You can use multiple AWS instances to create a distributed SL1 System. For each instance, you must specify the correct instance type, storage size, and security rules. All these parameters are described in this chapter.



To launch the new EC2 instance from the ScienceLogic AMI:

1. Go to the [EC2 Dashboard](#):



2. Select the ScienceLogic AMI that matches the ScienceLogic appliance you want to create. Click the **[Launch]** button.
3. In the **Choose Instance Type** page, choose the instance type recommended for the AMI. Choose the size and type that fulfills your needs.

**NOTE:** For details about the recommended instance type for each ScienceLogic appliance, see the ScienceLogic Support Site. <https://support.sciencelogic.com/s/system-requirements?tabset-e65a2=f5872>

4. Click the **[Next: Configure Instance Details]** button.
5. In the **Configure Instance Details** page, define the following:
  - **Number of Instances.** Enter "1".
  - **Request Spot Instances.** Do not select.
  - **Network.** For VPC-enabled accounts, specify the network where the instance will reside. If you are unsure of the network, accept the default.
  - **Subnet.** For VPC-enabled accounts, specify the subnet where the instance will reside. If you are unsure of the subnet, accept the default.
  - **Auto-assign Public IP.** If you select *Enable*, AWS will assign an IP address from the public pool to this instance. If you select *Disable*, you must assign an **Elastic IP Address (EIP)** to the instance.

**NOTE:** If you select *Enable* in the **Auto-assign Public IP** field, the IP address will change each time the instance is stopped or terminated. For All-In-One Appliances and for Administration Portals, you might want to use an Elastic IP address (EIP), which is a persistent IP address. See the section on [Elastic IP Addresses \(EIP\)](#) for details.

**NOTE:** For more information on Elastic IP Addresses, see <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html>.

- **IAM role.** If your organization uses IAM roles, select the appropriate role.
- **Shutdown behavior.** Select *Stop*.
- **Enable termination protection.** Selecting this checkbox is not required. Configure this checkbox according to your organization's procedures.
- **Monitoring.** Do not select this checkbox.
- **EBS-optimized instance.** Do not select this checkbox.
- **Tenancy.** Select *Shared tenancy (multi-tenant hardware)*.

6. Click the **[Next: Add Storage]** button.

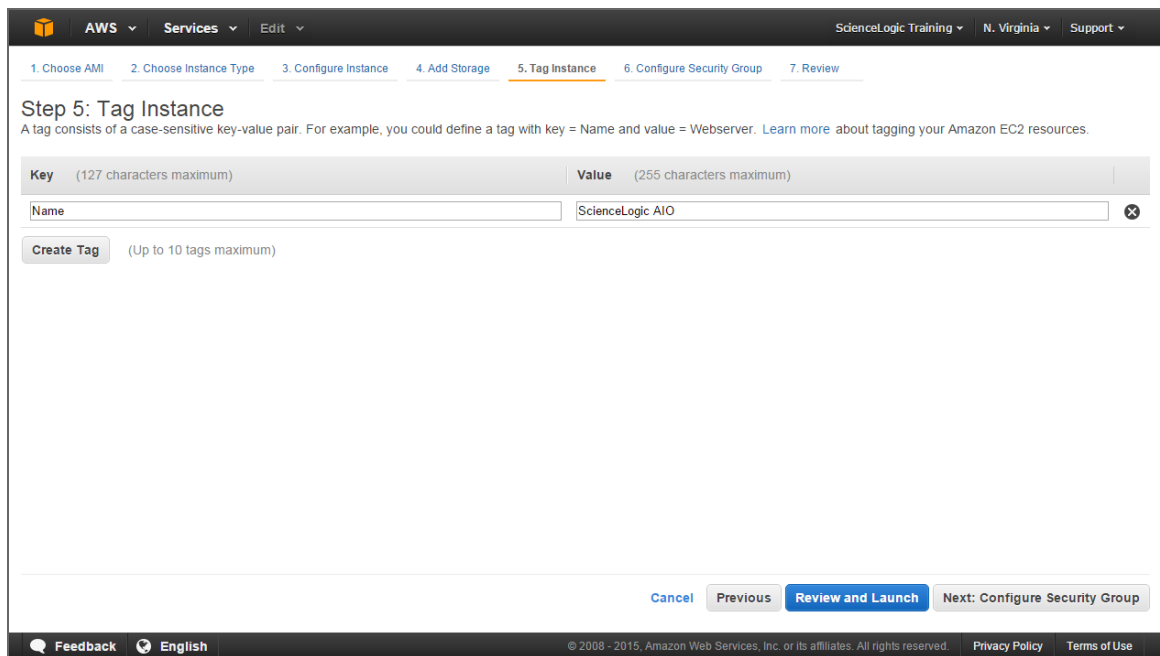
The screenshot shows the AWS Management Console interface for configuring an EC2 instance. The page is titled "Step 4: Add Storage" and includes a progress bar at the top with steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage (current step), 5. Add Tags, 6. Configure Security Group, and 7. Review. Below the title, there is a brief instruction: "Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2." A table lists the storage configuration for the "Root" volume, with columns for Volume Type, Device, Snapshot, Size (GiB), Volume Type, IOPS, Throughput (MB/s), Delete on Termination, and Encrypted. The root volume is configured with device /dev/sda1, snapshot snap-09bc19ec216a368, size 25 GiB, General Purpose SSD (GP2) volume type, 100 IOPS, N/A throughput, and is not encrypted. Below the table is an "Add New Volume" button and a blue informational box stating: "Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions." At the bottom of the page, there are navigation buttons: "Cancel", "Previous", "Review and Launch" (highlighted in blue), and "Next: Add Tags". The footer includes "Feedback", "English", and copyright information: "© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use".

- In the **Add Storage** page, select the checkbox in the **Delete on Termination** column.
- In the **Add Storage** page, increase the size of the /dev/sda1 partition as follows:

| SL1 Appliance                                | Type           | >Device   | Size in GB |
|----------------------------------------------|----------------|-----------|------------|
| Administration Portal                        | Instance Store | /dev/sda1 | 85         |
| Message Collector without ScienceLogic Agent | Instance Store | /dev/sda1 | 85         |
| Message Collector with ScienceLogic Agent    | Instance Store | /dev/sda1 | 85         |
| Database Server                              | EBS            | /dev/sda1 | 105        |
| All-In-One Appliance                         | EBSNVMe SSD    | /dev/sda1 | 105        |
| Data Collector                               | Instance Store | /dev/sda1 | 85         |

**NOTE:** The /dev/sda1 partition will contain the database.

- Click the **[Next: Tag Instance]** button.



- In the **Tag Instance** page, assign a descriptive tag to this instance. For example, you could enter "Name" in the **Key** field and "ScienceLogic AIO" in the **Value** field. This is optional.

**NOTE:** For more information on tags, see [http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using\\_Tags.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html).

11. Click the **[Next: Configure Security Group]** button.

**Step 6: Configure Security Group**

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

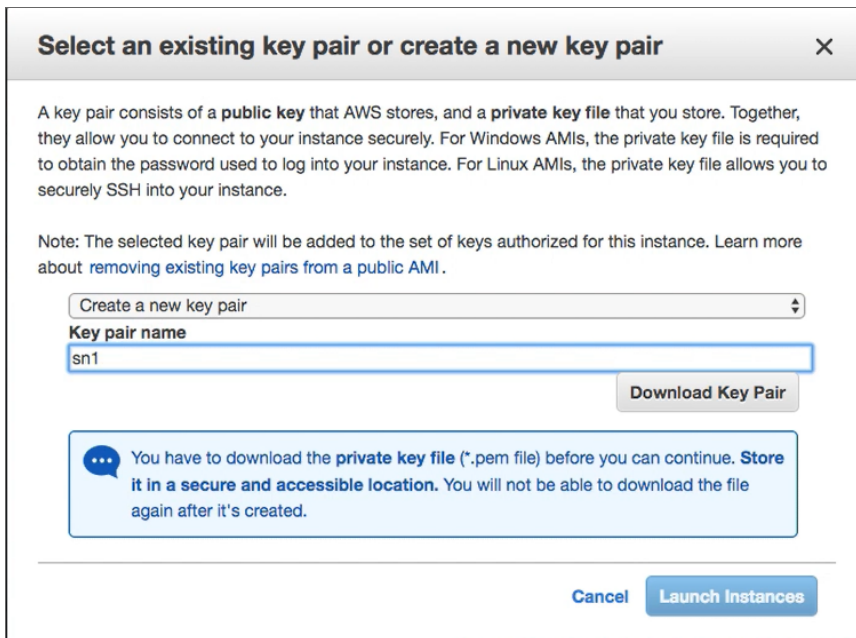
**Assign a security group:**  Create a **new** security group  
 Select an **existing** security group

**Security group name:**

**Description:**

| Type     | Protocol | Port Range | Source                   |
|----------|----------|------------|--------------------------|
| SSH      | TCP      | 22         | My IP   104.192.252.4/32 |
| All UDP  | UDP      | 0 - 65535  | My IP   104.192.252.4/32 |
| All ICMP | ICMP     | 0 - 65535  | My IP   104.192.252.4/32 |

12. A security group is a reusable set of firewall rules. In the **Configure Security Group** page, do the following:
- **Assign a security group.** Select *Create a new security group*.
  - **Security group name.** Enter a name or accept the default name.
  - **Description.** Accept the default value in this field.
13. Use the **following tables** to create security rules for each type of SL1 appliance. After completing each row, click the **[Add Rule]** button.
14. Click the **[Review and Launch]** button and review the details of the new instance. Fix any problems to meet the requirements of your organization.
15. Click the **[Launch]** button.
16. Amazon EC2 instances use public-key cryptography for authentication. Select **create a new key pair now**. You can enter a name for the private key. AWS will store the public key on its servers and automatically download the file that contains the private key to your browser. The private key is stored in a file that ends in `.pem`. You will need this file again when you **configure SSH** access to your AWS instances.



17. Amazon EC2 instances use public-key cryptography for authentication.

- Select **create a new key pair now**.
- **Key pair name**. Enter a name for the private key.
- **Download Key Pair**. AWS will store the public key on its servers and automatically download the file that contains the private key to your browser. The private key is stored in a file that ends in .pem. You will need this file again when you [configure SSH](#) access to your AWS instances.

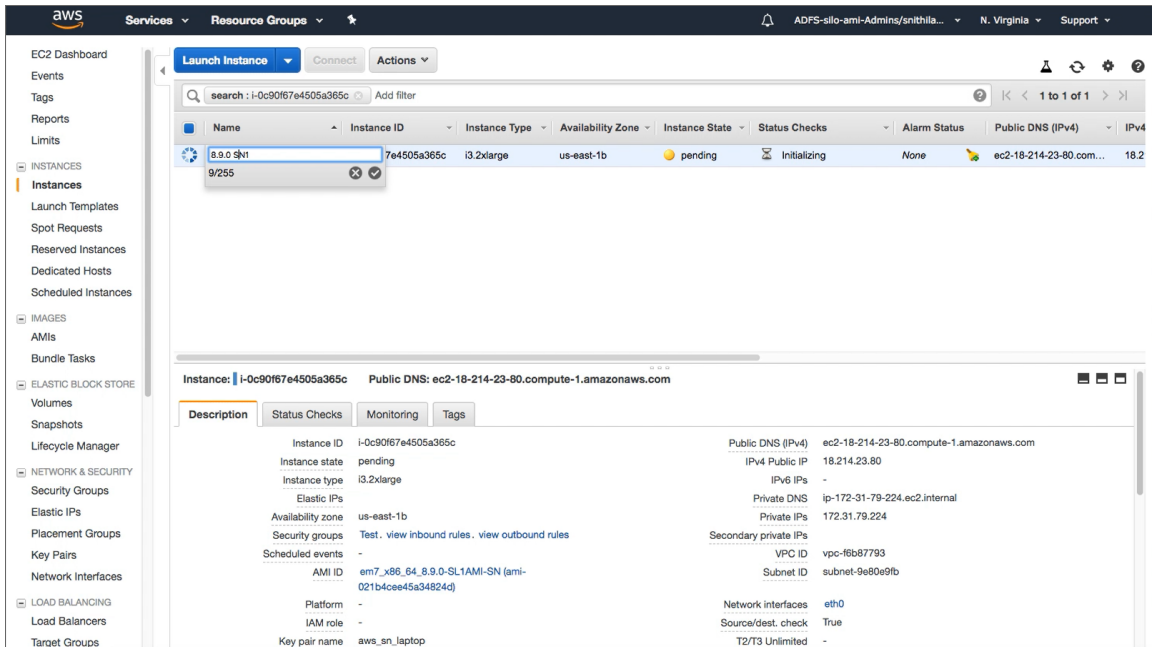
**NOTE:** Do not select an existing key unless you have previously downloaded and saved the key. You cannot retrieve an existing key a second time.

18. Click the **[Launch Instances]** button.

19. The **Launch Status** page displays the status of the new instance.

20. While the Launch runs in the background, go to the **Instances** page and provide a value in the **Name** field.

21. When the instance launch has completed, click the **[View Instances]** button to see your new instance.



22. When the instance launch has completed, click the **[View Instances]** button to see your new instance.
23. For all nodes, continue to the steps listed in [Additional Configuration Steps](#).

## Security Rules for Each Appliance Type

### All-In-One Appliance

#### Inbound

| Type                            | Protocol | Port Range | Source                                                                                                                                                                                                                                                                                                         | Description                                                                                                           |
|---------------------------------|----------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| SSH (edit the default SSH rule) | TCP      | 22         | If you will always log in from a single IP address, select <i>My IP</i> . If you will log in to the instance from multiple IP addresses, enter those IP addresses, separated by commas, in this field.<br>Configure this list according to your requirements, your AWS configuration, and your security rules. | SSH. For SSH sessions from the user workstation to the appliance. This is necessary to start the installation wizard. |

| Type            | Protocol | Port Range | Source                                                                                                                                                                                                                                                                                                         | Description                                                                                                                                |
|-----------------|----------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| HTTP            | TCP      | 80         | If you will always log in from a single IP address, select <i>My IP</i> . If you will log in to the instance from multiple IP addresses, enter those IP addresses, separated by commas, in this field.<br>Configure this list according to your requirements, your AWS configuration, and your security rules. | HTTP from browser session on user workstation.                                                                                             |
| HTTPS           | TCP      | 443        | If you will always log in from a single IP address, select <i>My IP</i> . If you will log in to the instance from multiple IP addresses, enter those IP addresses, separated by commas, in this field.<br>Configure this list according to your requirements, your AWS configuration, and your security rules. | HTTPS from browser session on user workstation.                                                                                            |
| Custom TCP Rule | TCP      | 7700       | If you will always log in from a single IP address, select <i>My IP</i> . If you will log in to the instance from multiple IP addresses, enter those IP addresses, separated by commas, in this field.<br>Configure this list according to your requirements, your AWS configuration, and your security rules. | ScienceLogic Web Configurator. Configuration Utility from browser session on user workstation. This is necessary to license the appliance. |
| Custom UDP Rule | UDP      | 162        | Specify a list of IP addresses for all managed devices from which you want to receive SNMP traps.<br>Configure this list according to your requirements, your AWS configuration, and your security rules.                                                                                                      | SNMP Traps. Necessary to receive SNMP traps from managed devices.                                                                          |

| Type            | Protocol | Port Range | Source                                                                                                                                                                                                      | Description                                                                              |
|-----------------|----------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Custom UDP Rule | UDP      | 514        | Specify a list of IP addresses for all managed devices from which you want to receive Syslog messages. Configure this list according to your requirements, your AWS configuration, and your security rules. | Syslog messages. Necessary to receive syslog messages from managed devices.              |
| SMTP            | TCP      | 25         | Specify a list of IP addresses for all managed devices from which you want to receive email messages. Configure this list according to your requirements, your AWS configuration, and your security rules.  | Necessary to receive inbound email for tickets, events, and email round-trip monitoring. |
| Custom TCP Rule | TCP      | 123        | Enter the IP address of the NTP server. Configure this list according to your requirements, your AWS configuration, and your security rules.                                                                | NTP. Communication between the All-In-One Appliance and configured NTP server.           |

## Database Server

### Inbound

| Type                            | Protocol | Port Range | Source                                                                                                                                                                                                                                                                                                      | Description                                                                                                       |
|---------------------------------|----------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| SSH (edit the default SSH rule) | TCP      | 22         | If you will always log in from a single IP address, select <i>My IP</i> . If you will log in to the instance from multiple IP addresses, enter those IP addresses, separated by commas, in this field. Configure this list according to your requirements, your AWS configuration, and your security rules. | SSH. For ssh sessions from user workstation to the appliance. This is necessary to start the installation wizard. |



| Type                                                                                          | Protocol | Port Range | Source                                                                                                                                                                                                                                                                                                      | Description                                                                              |
|-----------------------------------------------------------------------------------------------|----------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| SMTP                                                                                          | TCP      | 25         | Specify a list of IP addresses for all managed devices from which you want to receive email messages. Configure this list according to your requirements, your AWS configuration, and your security rules.                                                                                                  | Necessary to receive inbound email for tickets, events, and email round-trip monitoring. |
| HTTP<br><b>NOTE:</b> Required only if you are using the Administration Portal on the Database | TCP      | 80         | If you will always log in from a single IP address, select <i>My IP</i> . If you will log in to the instance from multiple IP addresses, enter those IP addresses, separated by commas, in this field. Configure this list according to your requirements, your AWS configuration, and your security rules. | HTTP from browser session on user workstation.                                           |
| Custom TCP Rule                                                                               | TCP      | 123        | Enter the IP address of the NTP server. Configure this list according to your requirements, your AWS configuration, and your security rules.                                                                                                                                                                | NTP. Communication between the Database Server and configured NTP server.                |
| Custom UDP Rule                                                                               | UDP      | 161        | Specify an IP address for each Data Collector that you will allow to can collect SNMP information about the Database Server. Configure this list according to your requirements, your AWS configuration, and your security rules.                                                                           | SNMP Agent. Allows SNMP information about the Database Server to be collected by SL1.    |

| Type                                                                                           | Protocol | Port Range | Source                                                                                                                                                                                                                                                                                                         | Description                                                                                                                                |
|------------------------------------------------------------------------------------------------|----------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| HTTPS<br><b>NOTE:</b> Required only if you are using the Administration Portal on the Database | TCP      | 443        | If you will always log in from a single IP address, select <i>My IP</i> . If you will log in to the instance from multiple IP addresses, enter those IP addresses, separated by commas, in this field.<br>Configure this list according to your requirements, your AWS configuration, and your security rules. | HTTPS from browser session on user workstation.                                                                                            |
| Custom TCP Rule                                                                                | TCP      | 7700       | If you will always log in from a single IP address, select <i>My IP</i> . If you will log in to the instance from multiple IP addresses, enter those IP addresses, separated by commas, in this field.<br>Configure this list according to your requirements, your AWS configuration, and your security rules. | ScienceLogic Web Configurator. Configuration Utility from browser session on user workstation. This is necessary to license the appliance. |
| Custom TCP Rule                                                                                | TCP      | 7706       | Specify an IP address for each Data Collector that you will allow to collect SNMP information about the Database Server.<br>Configure this list according to your requirements, your AWS configuration, and your security rules.                                                                               | MySQL. Communication from Administration Portal                                                                                            |
| Custom TCP Rule                                                                                | TCP      | 8008       | If you will always log in from a single IP address, select <i>My IP</i> . If you will log in to the instance from multiple IP addresses, enter those IP addresses, separated by commas, in this field.<br>Configure this list according to your requirements, your AWS configuration, and your security rules. | Administrative Web Interface (PHPMyAdmin) from browser session on user workstation                                                         |

# Administration Portal

## Inbound

| Type                            | Protocol | Port Range | Source                                                                                                                                                                                                                                                                                                         | Description                                                                                                       |
|---------------------------------|----------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| SSH (edit the default SSH rule) | TCP      | 22         | If you will always log in from a single IP address, select <i>My IP</i> . If you will log in to the instance from multiple IP addresses, enter those IP addresses, separated by commas, in this field.<br>Configure this list according to your requirements, your AWS configuration, and your security rules. | SSH. For ssh sessions from user workstation to the appliance. This is necessary to start the installation wizard. |
| HTTP                            | TCP      | 80         | If you will always log in from a single IP address, select <i>My IP</i> . If you will log in to the instance from multiple IP addresses, enter those IP addresses, separated by commas, in this field.<br>Configure this list according to your requirements, your AWS configuration, and your security rules. | HTTP from browser session on user workstation.                                                                    |
| HTTPS                           | TCP      | 443        | If you will always log in from a single IP address, select <i>My IP</i> . If you will log in to the instance from multiple IP addresses, enter those IP addresses, separated by commas, in this field.<br>Configure this list according to your requirements, your AWS configuration, and your security rules. | HTTPS from browser session on user workstation.                                                                   |
| Custom TCP Rule                 | TCP      | 123        | Enter the IP address of the NTP server.<br>Configure this list according to your requirements, your AWS configuration, and your security rules.                                                                                                                                                                | NTP. Communication between the Administration Portal and configured NTP server.                                   |

| Type            | Protocol | Port Range | Source                                                                                                                                                                                                                                                                                                         | Description                                                                                                                                |
|-----------------|----------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Custom TCP Rule | TCP      | 7700       | If you will always log in from a single IP address, select <i>My IP</i> . If you will log in to the instance from multiple IP addresses, enter those IP addresses, separated by commas, in this field.<br>Configure this list according to your requirements, your AWS configuration, and your security rules. | ScienceLogic Web Configurator. Configuration Utility from browser session on user workstation. This is necessary to license the appliance. |
| Custom UDP Rule | UDP      | 161        | Specify an IP address for each Data Collector that you will allow to can collect SNMP information about the Administration Portal. Configure this list according to your requirements, your AWS configuration, and your security rules.                                                                        | SNMP Agent. Allows SNMP information about the Administration Portal to be collected by SL1.                                                |

## Data Collector

### Inbound

| Type                            | Protocol | Port Range | Source                                                                                                                                                                                                                                                                                                         | Description                                                                                                       |
|---------------------------------|----------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| SSH (edit the default SSH rule) | TCP      | 22         | If you will always log in from a single IP address, select <i>My IP</i> . If you will log in to the instance from multiple IP addresses, enter those IP addresses, separated by commas, in this field.<br>Configure this list according to your requirements, your AWS configuration, and your security rules. | SSH. For ssh sessions from user workstation to the appliance. This is necessary to start the installation wizard. |

| Type            | Protocol | Port Range | Source                                                                                                                                                                                                                                                                                                         | Description                                                                                                                                |
|-----------------|----------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Custom TCP Rule | TCP      | 123        | Enter the IP address of the NTP server.<br>Configure this list according to your requirements, your AWS configuration, and your security rules.                                                                                                                                                                | NTP. Communication between the Data Collector and configured NTP server.                                                                   |
| Custom UDP Rule | UDP      | 161        | Specify an IP address for each Data Collector that you will allow to collect SNMP information about this Data Collector.<br>Configure this list according to your requirements, your AWS configuration, and your security rules.                                                                               | SNMP Agent. Allows SNMP information about the Data Collector to be collected by SL1.                                                       |
| Custom UDP Rule | UDP      | 162        | Specify a list of IP addresses for all managed devices from which you want to receive SNMP traps.<br>Configure this list according to your requirements, your AWS configuration, and your security rules.                                                                                                      | SNMP Traps. Necessary to receive SNMP traps from managed devices.                                                                          |
| Custom UDP Rule | UDP      | 514        | Specify a list of IP addresses for all managed devices from which you want to receive Syslog messages.<br>Configure this list according to your requirements, your AWS configuration, and your security rules.                                                                                                 | Syslog messages. Necessary to receive syslog messages from managed devices.                                                                |
| Custom TCP Rule | TCP      | 7700       | If you will always log in from a single IP address, select <i>My IP</i> . If you will log in to the instance from multiple IP addresses, enter those IP addresses, separated by commas, in this field.<br>Configure this list according to your requirements, your AWS configuration, and your security rules. | ScienceLogic Web Configurator. Configuration Utility from browser session on user workstation. This is necessary to license the appliance. |

| Type            | Protocol | Port Range | Source                                                                                                                                                                                                        | Description                                                                    |
|-----------------|----------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Custom TCP Rule | TCP      | 7707       | Specify the IP address of the Database Server that you want to retrieve data from the Data Collector.<br>Configure this list according to your requirements, your AWS configuration, and your security rules. | Data Pull. Allows the Database Server to retrieve data from the Data Collector |

## Message Collector

### Inbound

| Type                            | Protocol | Port Range | Source                                                                                                                                                                                                                                                                                                         | Description                                                                                                       |
|---------------------------------|----------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| SSH (edit the default SSH rule) | TCP      | 22         | If you will always log in from a single IP address, select <i>My IP</i> . If you will log in to the instance from multiple IP addresses, enter those IP addresses, separated by commas, in this field.<br>Configure this list according to your requirements, your AWS configuration, and your security rules. | SSH. For ssh sessions from user workstation to the appliance. This is necessary to start the installation wizard. |
| Custom TCP Rule                 | TCP      | 123        | Enter the IP address of the NTP server.<br>Configure this list according to your requirements, your AWS configuration, and your security rules.                                                                                                                                                                | NTP. Communication between the Message Collector and configured NTP server.                                       |
| Custom UDP Rule                 | UDP      | 161        | Specify an IP address for each Data Collector that you will allow to collect SNMP information about this Message Collector.<br>Configure this list according to your requirements, your AWS configuration, and your security rules.                                                                            | SNMP Agent. Allows SNMP information about the Message Collector to be collected by SL1.                           |

| Type            | Protocol | Port Range | Source                                                                                                                                                                                                                                                                                                      | Description                                                                                                                                |
|-----------------|----------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Custom UDP Rule | UDP      | 162        | Specify a list of IP addresses for all managed devices from which you want to receive SNMP traps. Configure this list according to your requirements, your AWS configuration, and your security rules.                                                                                                      | SNMP Traps. Necessary to receive SNMP traps from managed devices.                                                                          |
| Custom UDP Rule | UDP      | 514        | Specify a list of IP addresses for all managed devices from which you want to receive Syslog messages. Configure this list according to your requirements, your AWS configuration, and your security rules.                                                                                                 | Syslog messages. Necessary to receive syslog messages from managed devices.                                                                |
| Custom TCP Rule | TCP      | 7700       | If you will always log in from a single IP address, select <i>My IP</i> . If you will log in to the instance from multiple IP addresses, enter those IP addresses, separated by commas, in this field. Configure this list according to your requirements, your AWS configuration, and your security rules. | ScienceLogic Web Configurator. Configuration Utility from browser session on user workstation. This is necessary to license the appliance. |
| Custom TCP Rule | TCP      | 7707       | Specify the IP address of the Database Server that you want to retrieve data from the Message Collector. Configure this list according to your requirements, your AWS configuration, and your security rules.                                                                                               | Data Pull. Allows the Database Server to retrieve data from the Message Collector.                                                         |

---

## Additional Configuration Steps

After the instance is successfully launched, perform these additional steps to complete configuration:

- For instances of the **Database Server** or **All-In-One Appliance**:

- [Assigning an EIP to the instance](#) (optional step)
- [Accessing the Appliance Using SSH](#)
- [Licensing the instance in the Web Configuration Tool](#)
- For instances of the **Administration Portal**:
  - [Assigning an EIP to the instance](#) (optional step)
  - [Accessing the Appliance Using SSH](#)
  - [Configuring the instance in the Web Configuration Tool](#)
- For instances of the **Data Collector and Message Collector**:
  - [Assigning an EIP to the instance](#) (optional step)
  - [Accessing the Appliance Using SSH](#)
  - [Configuring the instance in the Web Configuration Tool](#)
  - [Rebooting Data Collectors and Message Collectors](#)

---

## Assigning an EIP to the New Instance

This chapter assumes you have already [received the ScienceLogic AMI](#) and [created an EC2 instance](#) based on the ScienceLogic AMI.

AWS can assign a public-facing IP address to your new instance. However, the IP address will change each time the instance is stopped or terminated. If you will be accessing an All-In-One Appliance or an Administration Portal appliance from the internet, ScienceLogic recommends you use an Elastic IP address (EIP).

An EIP is a permanent static address that belongs to an account (not an instance) and can be reused. An EIP address is required only if you want the public IP address to remain constant. When you assign an EIP to an instance, the instance still retains its private IP address in its VPC.

If you use an AWS VPN to access the All-In-One Appliance or Administration Portal appliance, that is you can access the All-In-One Appliance or Administration Portal appliance only through your corporate network, you do not have to assign an EIP to the All-In-One Appliance or Administration Portal appliance .

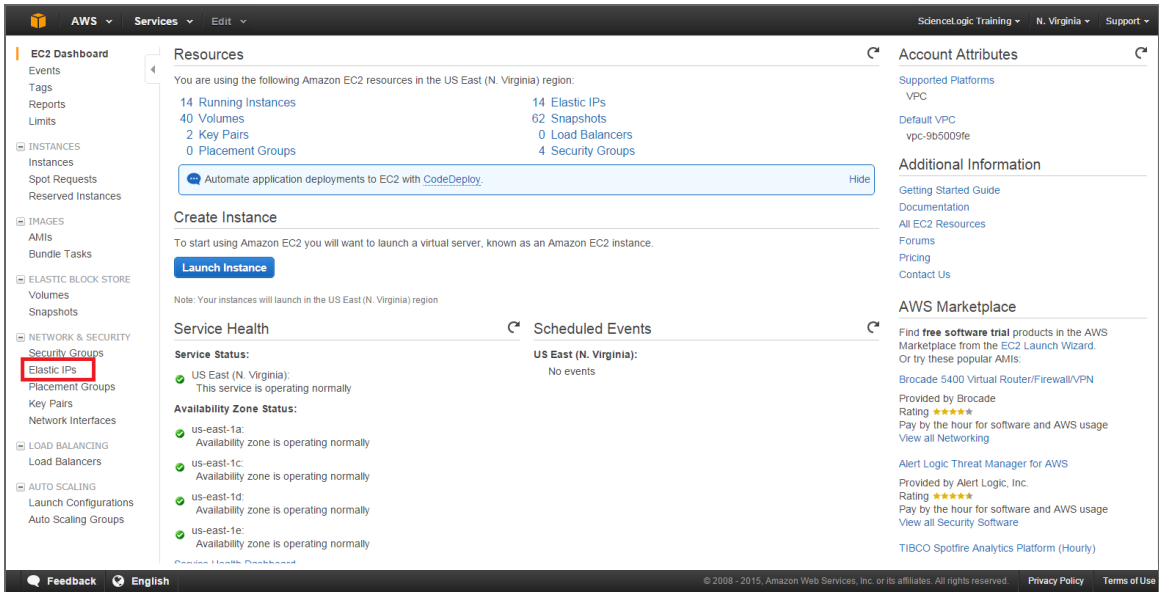
**NOTE:** For more information on Elastic IP, see <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html>

**NOTE:** AWS accounts are limited five Elastic IP addresses.

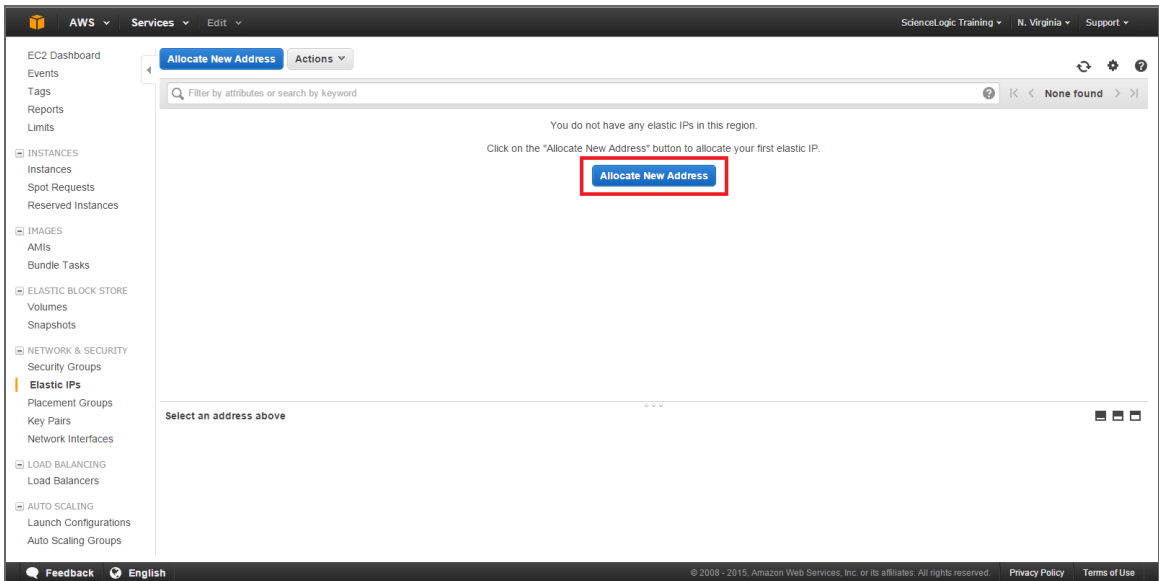


To assign an EIP to your new instance:

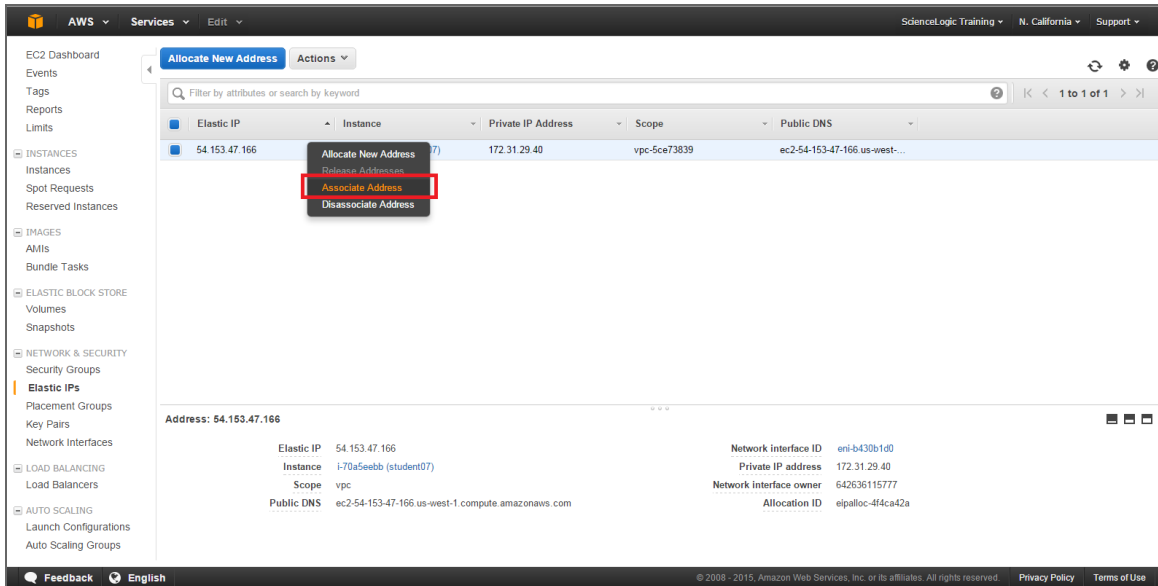
1. Go to the [EC2 Dashboard](#).
2. In the left navigation pane, under the **Network & Security** heading, click **[Elastic IPs]**.



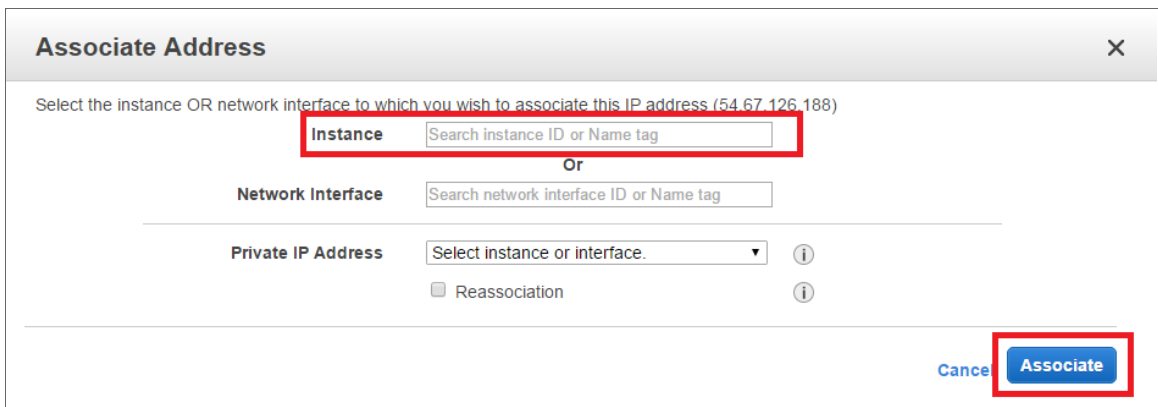
3. In the **Allocate New Address** page, click the **[Allocate New Address]** button and then click the **[Yes, Allocate]** button.



4. Right-click the new address and select **Associate Address** from the drop-down menu.



5. In the **Associate Address** modal page, select the new SL1 appliance instance in the **Instance** field, then click the **[Associate]** button. The SL1 appliance instance is now associated with the new EIP.



## Accessing the Appliance Using SSH

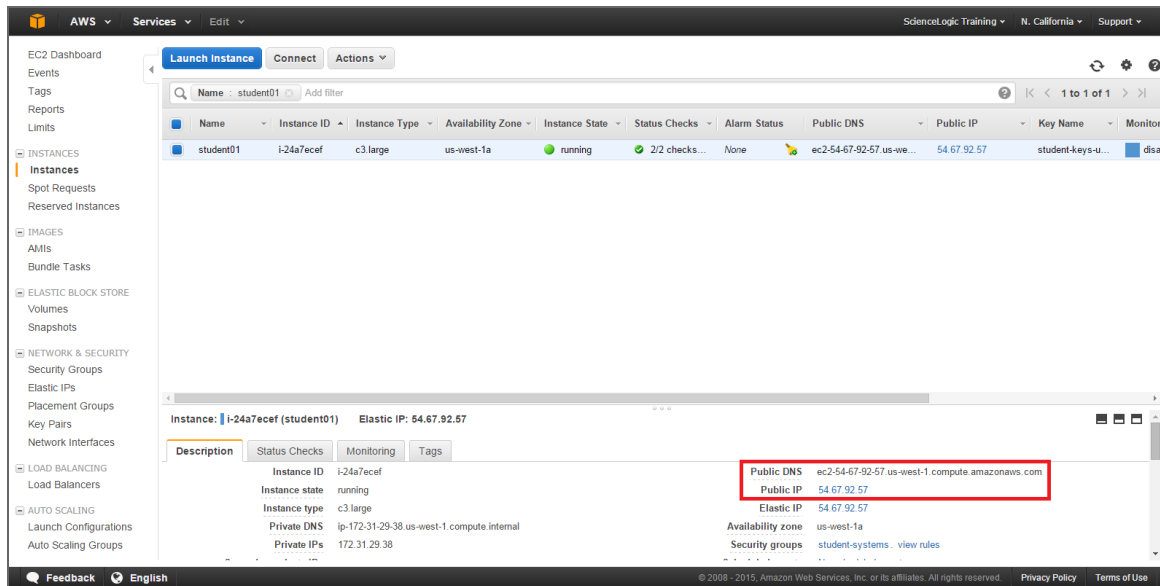
This chapter assumes you have already [received the ScienceLogic AMIs](#) and [created an EC2 instance](#) based on the ScienceLogic AMI.

This chapter assumes that you have access to SSH on the command line (for UNIX users) or have installed PuTTY (for Windows users).

# Gathering Information Required for Accessing the Appliance Using SSH

To gather the required information:

1. Go to the [EC2 Dashboard](#).
2. In the left navigation pane, under the **Instances** heading, select **Instances**.



3. Click in the row that contains the SL1 appliance instance.
4. The lower pane contains information about the instance. Write down the **Public DNS** and **Public IP**.
5. If you are using AWS instances to create a distributed SL1 system, perform this step for each AWS instance you want to include in the distributed system.

## Configuring SSH

Before you can use SSH with the SL1 appliance instance, you must ensure that SSH can use the .pem file downloaded earlier during the configuration. For details on downloading the .pem file, see the last few steps in the section on [Launching the EC2 Instance](#).

## UNIX and LINUX Users

You can connect to your SL1 appliance instance using the SSH command.

**NOTE:** You should store the .pem file in a secure location. ScienceLogic recommends you store the .pem file in \$HOME/.ssh. ScienceLogic also recommends you change the permissions on the .pem file to allow only read-only access by the owner of the .pem file.

To connect using the .pem file generated by AWS, enter the following at the shell prompt:

```
ssh -i ~/.ssh/my-aws-key.pem em7admin@[hostname or IP address]
```

where:

- **~/.ssh/my-aws-key.pem.** Replace with the name and full path to your .pem file.
- **hostname or IP address.** Replace with the hostname or public-facing IP address of the SL1 appliance instance.

You can also configure your SSH client to automatically select the correct key file when accessing the SL1 appliance instance. For details, see the man page for ssh\_config for your flavor of UNIX.

## Windows Users

You can connect with your SL1 appliance instance using PuTTY and SSH as the em7admin user. However, you must first convert the private key for your instance into a format that PuTTY can use. See the following for detailed instructions on using PuTTY SSH and converting your private key:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html>

---

## Web Configuration Tool

- For instances of the **Database Server** or **All-In-One Appliance**, see the section on [Licensing the instance in the Web Configuration Tool](#)
- For instances of the **Administration Portal**, see the section on [Configuring the instance in the Web Configuration Tool](#)
- For instances of the **Data Collector and Message Collector**, see the section on [Configuring the instance in the Web Configuration Tool](#)

---

## Rebooting Data Collectors and Message Collectors

After installing an SL1 appliance as an AWS instance, you must reboot the instance.

To reboot the AWS instance:

1. Connect to the command-line interface of the appliance as the em7admin user using SSH. See the [Accessing the Appliance Using SSH](#) section for more information.
2. Execute the following command:

```
sudo reboot
```

---

# Chapter

# 11

## Installing SL1 in Azure

---

### Overview

This chapter describes how to deploy a ScienceLogic virtual machine in Azure from a VHD image file.



**NOTE:** If you are looking for resources and support for Azure, see the Microsoft Azure Marketplace: <https://azuremarketplace.microsoft.com/>.

**NOTE:** If you are configuring a Database, ScienceLogic recommends allocating four times the memory for the Database as compared to the memory for the Data Collectors.

**TIP:** A single Azure image file can be used to create multiple virtual machines. For example, you can use the same Azure VHD file for the Database Server to create multiple Database Servers.

**IMPORTANT:** High Availability for Azure deployments is supported for installations of 12.1.x that are running on Oracle Linux 8 (OL8). ScienceLogic recommends that all customers running SL1 versions prior to 12.1.x upgrade and then complete the High Availability setup and configuration.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (.
- To view a page containing all of the menu options, click the Advanced menu icon (.

This chapter covers the following topics:

|                                                                      |     |
|----------------------------------------------------------------------|-----|
| <i>Prerequisites for Installing SL1 in Azure</i> .....               | 168 |
| <i>System Requirements</i> .....                                     | 168 |
| <i>Deploying an SL1 System in Azure</i> .....                        | 168 |
| <i>Creating an Azure Virtual Machine</i> .....                       | 174 |
| <i>Setting the Virtual Machine Allocation Method to Static</i> ..... | 176 |
| <i>Configuring Ports on SL1 Appliances</i> .....                     | 178 |
| <i>Configuring the Virtual Machine</i> .....                         | 180 |
| <i>Troubleshooting</i> .....                                         | 180 |

---

## Prerequisites for Installing SL1 in Azure

To deploy an SL1 appliance in Azure, you need the following components:

- Windows PowerShell version 5 or later. (See [Microsoft's documentation for instructions on installing PowerShell on Windows](#).)
- PowerShellGet. (See [Microsoft's documentation on PowerShellGet](#) for more information.)
- Azure PowerShell module. (See [Microsoft's documentation for instructions on installing the Azure PowerShell module](#).)
- *Azure CLI tool*
- *An Azure Resource group*
- *An Azure storage account that includes at least one blob container*
- An Azure Network Security Group (NSG). (See [Microsoft's documentation on Network Security Groups](#) for more information.)

In addition, before attempting to deploy SL1 in Azure, you should confirm that the following prerequisites are all true:

- Your Azure policies allow you to create a new virtual machine from the ScienceLogic VHD.
- Your virtual machine naming convention does not conflict with any existing policies in Azure.
- You are using virtual networks and subnets that allow access and the creation of new virtual machines.
- Your resource group allows you to create new virtual networks.

---

## System Requirements

For details about supported hypervisors and the requirements and specifications for each SL1 appliance, see the ScienceLogic Support Site: <https://support.sciencelogic.com/s/system-requirements>

---

## Deploying an SL1 System in Azure

This section provides the information you need to deploy SL1 in Azure and includes procedures for each step.

### SL1 Appliance Deployment Order for Distributed Systems

To deploy a distributed SL1 system on Azure instances, create appliances in this order:

1. Database Server
2. Administration Portal (if applicable)



3. Data Collectors
4. Message Collectors (if applicable)

## Installing and Configuring the Azure CLI

Azure CLI is a tool that lets you manage resources in Azure. To complete the SL1 installation on Azure using the procedures in this section, you must have the Azure CLI tool installed.

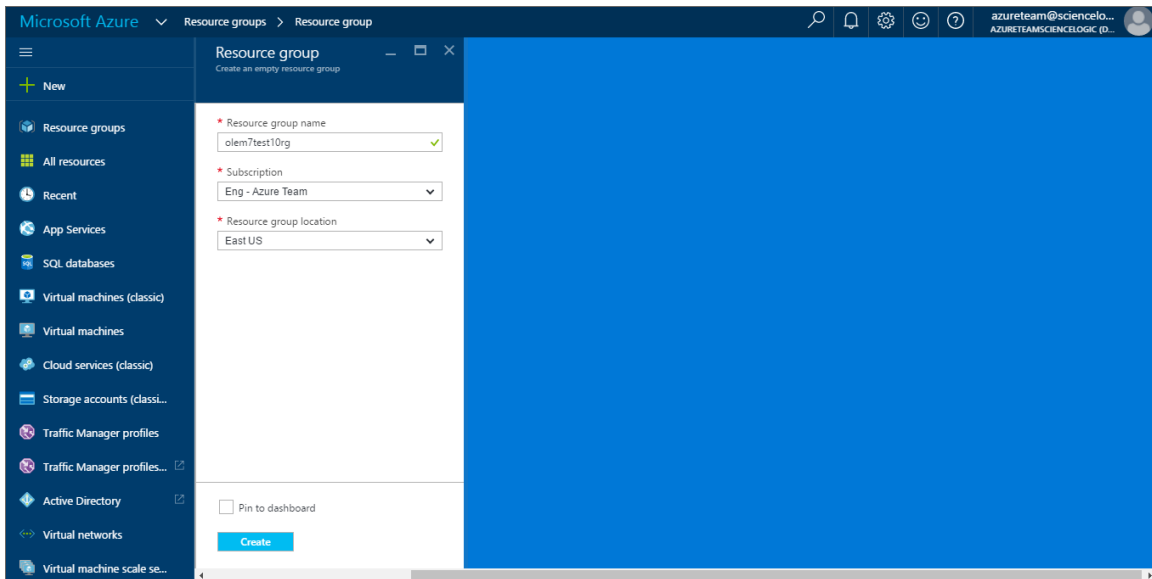
To install and configure the Azure CLI tool:

1. Download and install the Azure CLI tool from the Microsoft website:  
<https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-windows?view=azure-cli-latest>
2. After installation completes, search for and click on "PowerShell" in Windows to start the program.
3. In PowerShell, type "az login". You will be prompted to sign into your Microsoft Azure account. After you log in, you will see information about your Azure subscription within the PowerShell window.

## Configuring an Azure Resource Group and Storage Account

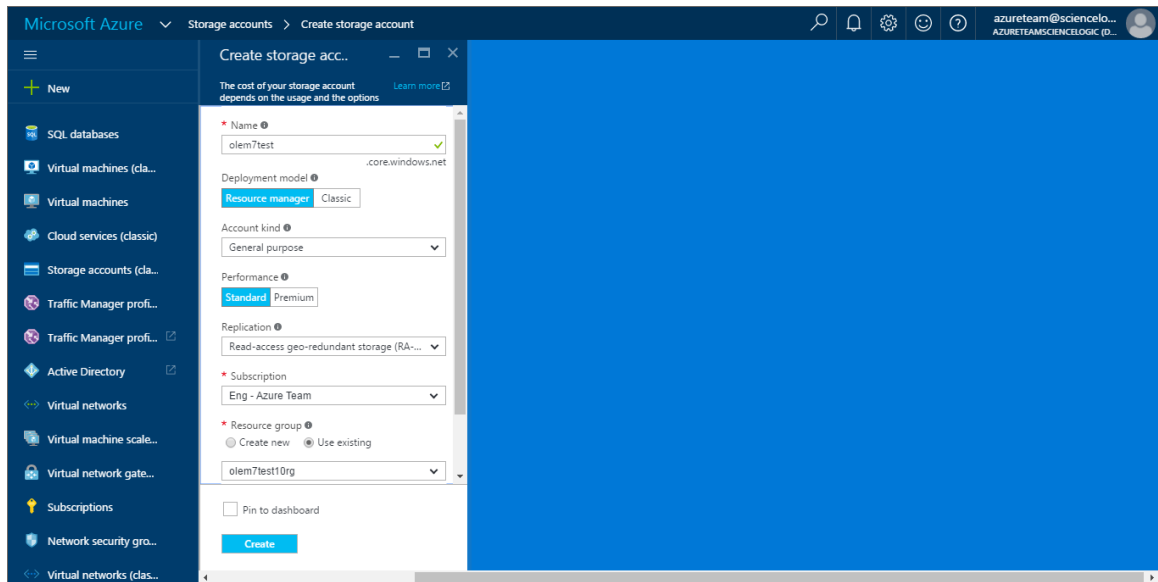
To create and configure an Azure storage account:

1. Log in to the Azure Portal, and then click **Resource groups** on the left menu.



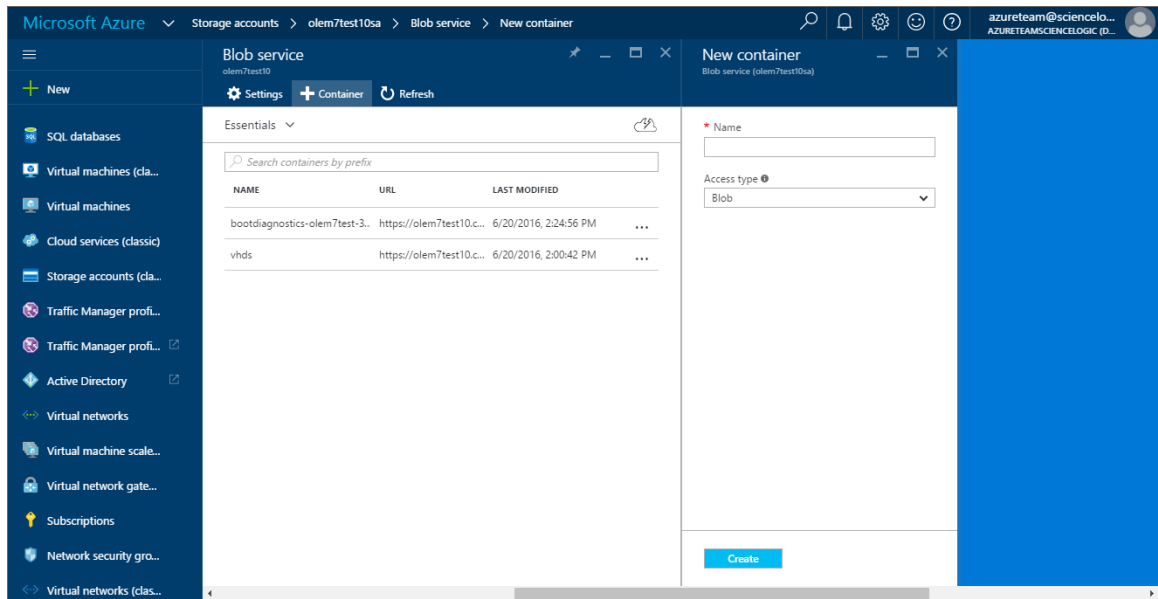
2. Click the **[Add]** button and add information for a new Resource group. Click the **[Create resource group]** button to create the Resource group.
3. After creating the Resource group, click **Storage accounts** on the left menu.

4. Click the **[Add]** button, and then click the **[Create Storage accounts]** button to create a new Storage account. When creating the Storage account, complete the following fields:



- **Deployment model.** Select *Resource manager*.
  - **Account kind.** Select *General purpose*.
  - **Resource group.** Select *Use existing*, and then select the Resource group you created in step 2.
5. After creating the Storage account, click **Storage accounts** on the left menu, and then select the newly created Storage account.
  6. Under the Services section of the Storage account pane, click **Blobs**. The Blob service blade information appears.

7. In the Blob service pane, click the **Plus** icon to add a new container. Type a name for the container and select *Blob* as the **Access Type**. When you are finished, click the **[Create]** button to create the Blob container.



## Creating the BLOB\_URI

Before you can upload the VHD image file, you must:

- Determine the URL value of the Azure storage account
- Define the BLOB\_URI

To create the BLOB\_URI, you must determine the container URL and then append the name of the VHD file. You will use the BLOB\_URI value when you upload the VHD file. This BLOB\_URI tells Azure where to put the VHD file and what to call it.

To determine the container URL:

1. Log in to the Azure portal.
2. Select **Storage Accounts**.
3. Select the **Containers** section.
4. Click the ellipsis (...) button to the right of the container name to open the pop-up menu.
5. Click **Container Properties** in the pop-up menu. You will see a URL displayed in the Properties.
6. Click the blue Copy icon on the Properties page to copy the URL for the container.

To create the BLOB\_URI value, append the destination to the container URL. For example, if the container URL is:

```
https://azuretest.blob.core.windows.net
```

Your BLOB\_URI value might be:

```
https://azuretest.blob.core.windows.net/vhds/em7inazure.vhd
```

Where "/vhds" is the directory on the container, and "em7inazure.vhd" is the name of the VHD image file you will be uploading.

## Uploading a VHD Image File to an Azure Storage Account

After creating the Resource group, Storage account, and Blob container, you must upload the ScienceLogic VHD image file to the Blob container. To do so, you will need the following information:

- The ScienceLogic VHD file
- Resource Group name
- Blob container URI
- Local file path to the VHD file

## Downloading the ScienceLogic VHD File

To download the ScienceLogic VHD file:

1. Open a browser session and go to [support.sciencelogic.com](http://support.sciencelogic.com).
2. Go to the **Product Downloads** menu and choose **Platform**.
3. Find the platform version that you want to download. Click on its name.
4. Expand the **Release Files** list and find an entry of Record Type *Product Image*.
5. In the **Release File Downloads** pane to the right, download the .vhd files for each SL1 appliance.

## Converting a VHD Image File from Dynamic to Fixed

After downloading the ScienceLogic VHD file to a Windows server, you must convert it from Dynamic to Fixed.

To do this:

1. Open a PowerShell session as an administrator.
2. At the PowerShell prompt, navigate to the directory to which you downloaded the .vhd file.
3. For each .vhd file, run the following command:

```
Convert-VHD -Path <vhd_file_path> -DestinationPath <destination_file_path> -VHDType Fixed
```

where:

- **vhd\_file\_path** specifies the full path of the downloaded .vhd file, including the file name.
- **destination\_file\_path** specifies the full path to where you want to store the converted file, including the file name

4. If you see the following error, proceed to step 5. Otherwise, proceed to the next section.  

```
convert-vhd: The term 'convert-vhd' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
```
5. To install the Hyper-V Module for Windows PowerShell, run the following command:  

```
Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V-Management-PowerShell
```
6. To install Hyper-V Services, run the following command:  

```
Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V-all
```
7. Reboot the server when prompted.

## Uploading the VHD File to an Azure Container

To upload the ScienceLogic VHD file to your Blob container, perform the following steps:

1. Open Microsoft Azure PowerShell and log in to your Azure account:  

```
Login-AzAccount
```
2. You created a resource group and storage container blob to which you will upload your VHD image file in [Configuring an Azure Resource Group and Storage Account](#). You identified the BLOB\_URI in [Obtaining the Container URL for an Azure Storage Account](#). Now you are ready to upload your VHD image file.

**NOTE:** The virtual machine that you create in [Creating an Azure Virtual Machine](#) must be in the same resource group as the storage account.

3. Add your VHD file to the storage account with the following cmdlet:

```
Add-AzVhd -Destination '<BLOB_URI>' -LocalFilePath '<VHD_LOCAL_FILE_PATH>' -ResourceGroupName '<RESOURCE_GROUP>'
```

where:

- **BLOB\_URI** specifies the BLOB\_URI you created in the section [Creating the BLOB\\_URI](#) where you will upload your VHD file. When entering the BLOB\_URI, you must include the .vhd file name. For example: `https://azuretest.blob.core.windows.net/vhds/em7inazure.vhd`
- **VHD\_LOCAL\_FILE\_PATH** specifies the file path on your machine for the VHD file you want to upload.
- **RESOURCE\_GROUP** specifies the resource group you created and that will be used when you create the Azure VM.

4. Repeat step 3 for each VHD file.

## Creating the Image

**NOTE:** The following steps require that you have an Azure resource group and storage account with the VHD file uploaded.

To create the image:

1. Open Microsoft Azure PowerShell and log in to your Azure account:

```
Login-AzureRmAccount
```

2. Run the following command:

```
az image create --name <image-name> -g <resource-group-name> --os-disk-caching ReadWrite --os-type Linux --source <BLOB_URI>
```

where:

- **resource-group-name** specifies the resource group you created in Azure.
- **image-name** specifies what you want to call the image (such as "dbimage123").
- **BLOB\_URI** specifies the destination value you provided when you uploaded the VHD file. This is also the BLOB\_URI you created in the section [Creating the BLOB\\_URI](#). When entering the BLOB\_URI, you must include the .vhd file name. For example: `https://azuretest.blob.core.windows.net/vhds/em7inazure.vhd`

**NOTE:** This command might return a large amount of JSON output. This is normal.

3. Repeat these steps for each SL1 appliance you want to build.

---

## Creating an Azure Virtual Machine

**NOTE:** The following steps require that you have an Azure resource group and storage account with the VHD file uploaded.

To create an Azure virtual machine:

1. Open Microsoft Azure PowerShell and log in to your Azure account:

```
Login-AzureRmAccount
```

2. Run the following command:

**NOTE:** The virtual machine that you create must be in the same resource group as the storage account.

```
az vm create -g <resource_group_name> -n <vm_name> --image
<image_name> --public-ip-sku Standard --admin-username em7admin --
authentication-type ssh --ssh-key-name <ssh_key_name> --os-disk-
size-gb <disk_size> --storage-sku StandardSSD_LRS --vnet-name
<virtual_network_name> --subnet <subnet_name>
```

where:

- **resource\_group\_name** specifies the resource group you created in Azure.
- **VM\_name** specifies what you want to call your virtual machine.
- **image\_name** specifies the name you gave to the image when you created it in the section [Creating the Image](#).
- **ssh\_key\_name** specifies the SSH key that you want to use within Azure. You will need this to SSH into the virtual machine. For more information, see <https://learn.microsoft.com/en-us/azure/virtual-machines/ssh-keys-portal>.
- **disk\_size** specifies the virtual machine disk size you want to use.
- **virtual\_network\_name** specifies the virtual network name you want to use within Azure.
- **subnet\_name** specifies the subnet name you want to use within Azure.

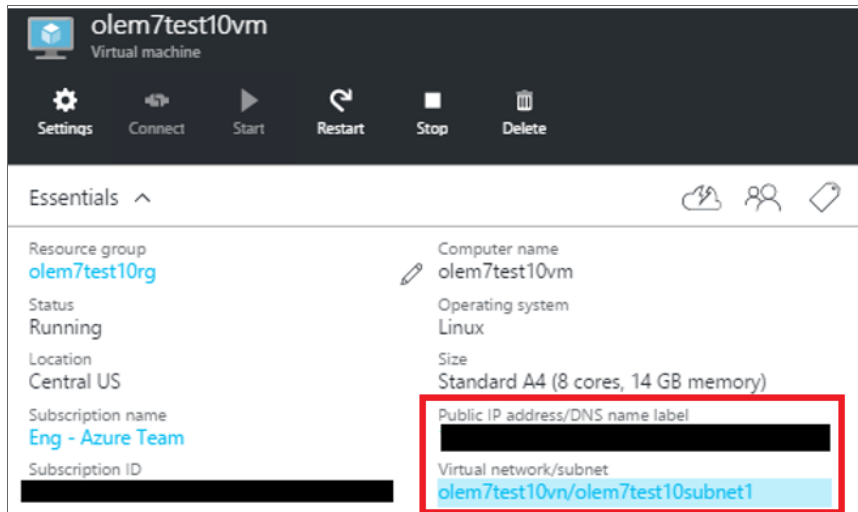
**NOTE:** If the public IP address is not available, ignore `--public-ip-sku Standard` in the command above.

3. Repeat these steps for each SL1 appliance you want to build.

## Setting the Virtual Machine Allocation Method to Static

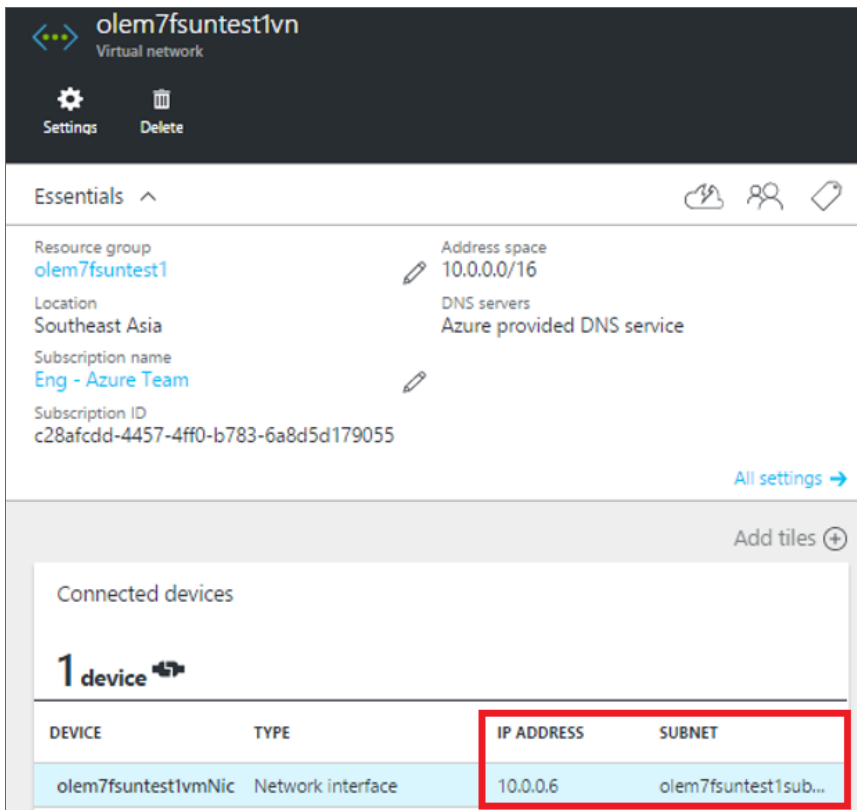
To ensure the IP address for the virtual machine remains the same after reboot, you must set the allocation method to **static**. To do so:

1. In the Azure Portal, navigate to the Virtual machine pane and verify that the virtual machine has a public IP address and a virtual network/subnet set.

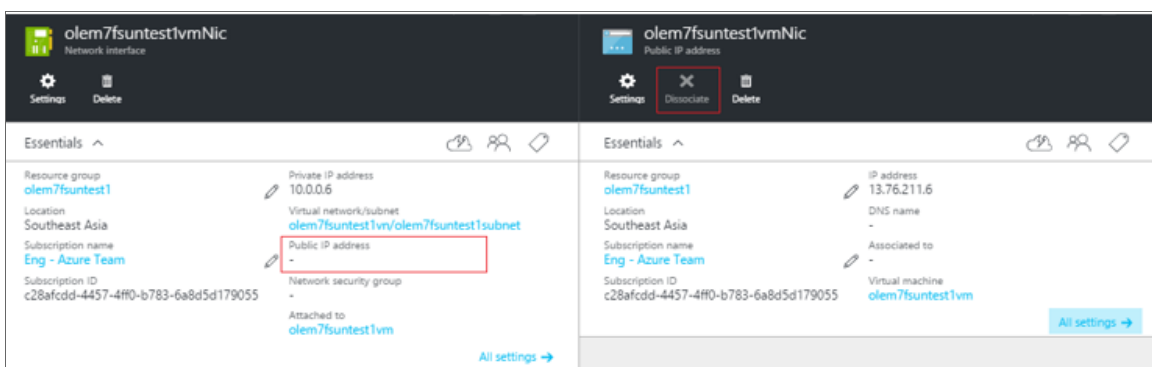




- Click the name of the Virtual network/subnet. The Virtual network pane appears.



- In the "Connected devices" section of the Virtual network pane, click the Network interface. The Network interface pane appears.
- Click the Public IP address value, and then click the **[Dissociate]** button.



- In the Network interface pane, click on **Settings > IP addresses**. Then, do one of the following:
  - If you **are not** using a VPN, complete steps 6 through 9. Ignore step 10.
  - If you **are** using a VPN, skip ahead to step 10.

6. If you **are not** using a VPN, then in the IP addresses pane, select *Enabled* in the **Public IP address** field and then click on the **IP address** field.
7. Click the **[Create new]** button.
8. In the Create public IP address pane, type a name for your IP address in the **Name** field and select *Static* in the **Assignment** field.
9. Click **[OK]** and then click **[Save]**.
10. If you **are** using a VPN, then in the IP addresses pane, select *Disabled* in the **Public IP address** field and then select a **Subnet**. You can use the default values for all other fields.

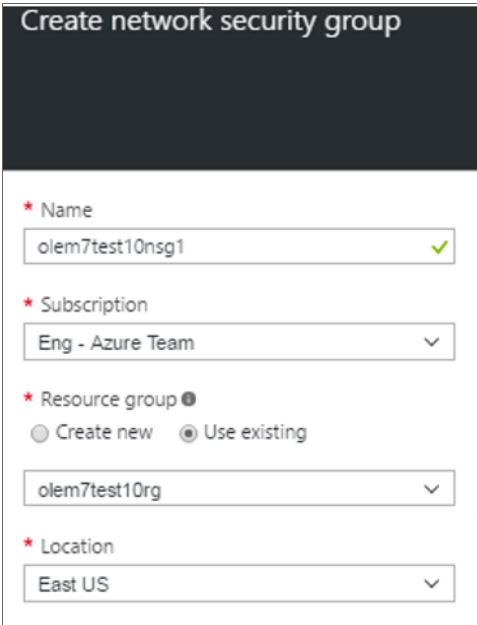
---

## Configuring Ports on SL1 Appliances

You must next create a Network security group that will specify the ports required for communication between the SL1 appliances and that will specify the ports required for communication between the SL1 appliances and the monitored devices in your network.

To configure the ports for communication:

1. In the Azure Portal, navigate to the Network security groups pane, and then click the **[Add]** button. The Create network security group pane appears.

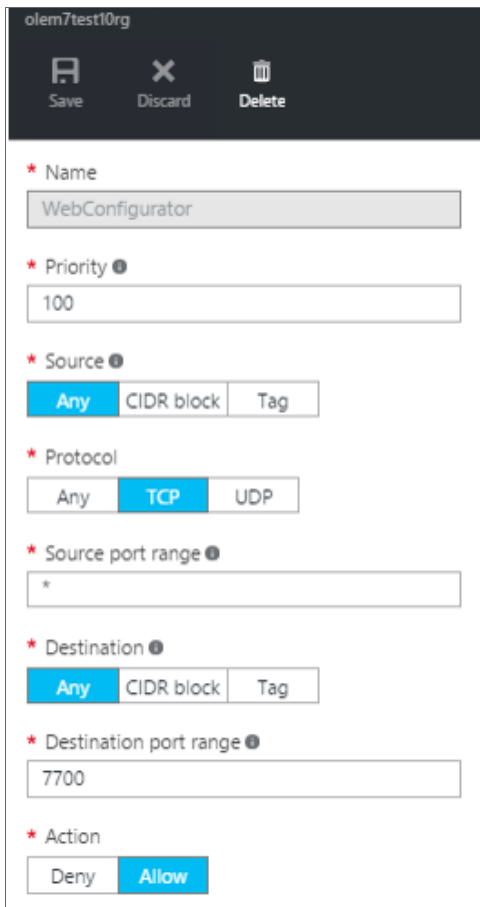


The screenshot shows the 'Create network security group' pane in the Azure Portal. The pane is titled 'Create network security group' and contains several fields:

- Name:** olem7test10nsg1 (with a green checkmark)
- Subscription:** Eng - Azure Team
- Resource group:** olem7test10rg (with radio buttons for 'Create new' and 'Use existing', where 'Use existing' is selected)
- Location:** East US

2. Type the information for the Network security group (name, subscription, resource group, and location), then click **[Create]**.
3. In the Network security groups pane, click the newly created Network security group, and then click the **[Settings]** button.
4. In the Settings pane, click **Inbound security rules**.

- In the Inbound security rules pane, click the **[Add]** button. The Add inbound security rule pane appears.



- Use the table below to create security rules.
- Repeat steps 5 and 6 to create an inbound security rule for each of the ports listed in the table below.
- After creating all of the inbound security rules, navigate to the Virtual machine pane and click the **[Settings]** button.
- In the Settings pane, click **Network interfaces** and then click on the name of the Network interface.
- In the Network interface pane, click the **[Settings]** button and then click **Network security group**.
- Select the newly created network security group to associate it with the Network interface.
- Perform steps 9-11 for each network interface in your SL1 system.

**NOTE:** ScienceLogic recommends that you limit the Source port range for security reasons.

| Type | Protocol | Port | Description                                                                  |
|------|----------|------|------------------------------------------------------------------------------|
| SSH  | TCP      | 22   | SSH. This is necessary to start the installation wizard.                     |
| SMTP | TCP      | 25   | Necessary to receive inbound email for tickets, events, and email round-trip |

| Type            | Protocol | Port | Description                                                                                                                                |
|-----------------|----------|------|--------------------------------------------------------------------------------------------------------------------------------------------|
|                 |          |      | monitoring.                                                                                                                                |
| HTTP            | TCP      | 80   | HTTP from browser session or user workstation.                                                                                             |
| Custom TCP Rule | TCP      | 123  | NTP. Communication between the All-In-One Appliance and configured NTP server.                                                             |
| Custom UDP Rule | UDP      | 161  | SNMP Agent. Allows SNMP information about the SL1 appliance to be collected by SL1.                                                        |
| Custom UDP Rule | UDP      | 162  | SNMP Traps. Necessary to receive SNMP traps from managed devices.                                                                          |
| HTTPS           | TCP      | 443  | HTTPS from browser session or user workstation.                                                                                            |
| Custom UDP Rule | UDP      | 514  | Syslog messages. Necessary to receive syslog messages from managed devices.                                                                |
| Custom TCP Rule | TCP      | 7700 | ScienceLogic Web Configurator. Configuration Utility from browser session or user workstation. This is necessary to license the appliance. |
| Custom TCP Rule | TCP      | 7705 | ScienceLogic PhoneHome. See <a href="#">Configuring SL1 for PhoneHome Communications</a> .                                                 |
| Custom TCP Rule | TCP      | 7706 | MySQL. Communication from Administration Portal.                                                                                           |
| Custom TCP Rule | TCP      | 7707 | Data Pull. Allows the Database Server to retrieve data from the SL1 appliance.                                                             |
| Custom TCP Rule | TCP      | 8008 | Administrative Web Interface (PHPMYAdmin) from browser session on user workstation.                                                        |

---

## Configuring the Virtual Machine

To configure each virtual machine, perform the following steps:

1. Use SSH to access the virtual machine using its public IP address, username, and the SSH key defined in step 2 of the section [Creating an Azure Virtual Machine](#).

```
ssh -i <private key path> em7admin@<vm-ip-address>
```

2. Using vi or another text editor, edit the /etc/silo.conf file:

```
sudo visilo
```

3. Set the db password.

---

## Troubleshooting

If the Data Collector continuously displays a message saying the collector is working when running a Dynamic Application, **DO NOT** restart the Azure virtual machine, as doing so could cause you to lose SSH access to the machine.

Instead, do the following:

1. Using the command line interface, verify whether you can run the Dynamic Application in debug mode by typing the following command:

```
sudo /usr/local/silo/proc/dynamic_single.py <did> <app_id>
```

2. Restart the data pull processes (em7\_hfpulld, em7\_lfpulld, em7\_mfpulld) by typing the following command:

```
sudo service <service_name> restart
```

---

# Chapter

# 12

## Updating SL1

---

### Overview

For information on updating an existing SL1 system, see the *Updating SL1* chapter of the *System Administration* manual, which describes how to update the software on your SL1 appliances.

© 2003 - 2023, ScienceLogic, Inc.

All rights reserved.

#### LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

#### Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

#### Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: [legal@sciencelogic.com](mailto:legal@sciencelogic.com). For more information, see <https://sciencelogic.com/company/legal>.

ScienceLogic

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010