Scout Deployment Planning

The number of Scouts appropriate for your deployment depends on the number of IP devices you have in your discovery universe and the kinds of discovery you plan to do. When the Scout's purpose is passive listening, however, the calculation becomes simple: Deploy one Scout in Area 0 (i.e., the network backbone) for OSPF Discovery (aka passive listening). Whenplacing Scouts in hybrid areas, virtual environments, or in different remote locations, your primary objective is to ensure that the Scouts are connected to the Command Center. Only connected Scouts can do their job.

- A standard installation of Lumeta comes with unlimited virtual Scouts.
- Lumeta recommends that you place a Scout in every Area 0, the OSPF backbone.
- Lumeta recommends that you place a Scout in remote, insulated areas of the network.
- If two autonomous systems areas are BGP peers, use one Scout for both areas.

The physical deployment of Scouts is based on the end goal of providing pervasive monitoring across the network infrastructure. To this end, Scouts are placed using two general guidelines. First, deploy them around the periphery of an enclave to ensure adequate monitoring of attacks being launched from outside. Second, deploy Scouts throughout the center of the enclave to ensure complete detection of attacks launched from within.

Scouts can respond to requests from multiple collectors, communicating the responses elicited through the combination of active and passive collection methods. They work in tandem and recursively, generating authoritative indexing.

Scouts do not store data, but instead transmit it back to the Command Center where it is stored and analyzed. Scouts operate bi-directionally and are proxy-aware, meaning their session traffic goes through an HTTP proxy so addressing information is not exchanged between the Internet and Lumeta.

The primary job of Scouts is to collect information on the state of the network and exchange information with Collectors. Scouts are available as virtual machines and are installed in the same manner as Command Centers. Your licensing agreement with Lumeta determines whether the component operates as a Command Center or a Scout.

Scout Density Recommendations

Scouts need to be positioned places where they will have visibility into a network. This means that they need to be placed where they will have a perspective on and access into a network, and can report back to the Command Center. Scouts can't do their job if their reach is blocked by firewalls or ACLS. Conversely, they also can't do their job when deployed in the same subnet. In this arrangement, the Scouts in too close proximity end up exchanging data with each other and duplicating their findings up to the Command Center, which provides no new information or benefit.

Scout FAQs

What does it mean to correctly position Scouts for OSPF?
It means that each Scout must be connected to a router that "speaks" OSPF and you must know the OSPF area in which each router participates. You also need to know whether your OSPF configuration uses passwords or MD5 encryption, and if so, the credentials for those authentication methods. Althou gh very large enterprises often have multiple Area 0s, each of these is considered a different network from the Lumeta perspective.

Is there always a backbone area that knows about OSPF?

Yes. No OSPF benefit comes from having Scouts in multitudes of OSPF areas because the only information Lumeta takes in via OSPF is the list of routes. As long as your Scout is positioned on the network backbone, it'll pick up all of the necessary route information. Note that OSPF networks linked via other routing protocols (like BGP) would only learn routes as long as they are propagated over the other protocol's network, otherwise an additional OSPF Scout should be used.

Of what value is OSPF discovery?
OSPF seeds the Zone Networks list in advance of Host Discovery and Path Discovery. It makes discover happen faster.

Is timing a factor in the dissemination and collection of OSPF data?
No. Data propagation takes essentially no time at all. OSPF is the most immediate function Lumeta can perform.

How should Lumeta be set up to perform OSPF discovery?
Designate one collector per zone for OSPF discovery.

How does a Zone Network's Eligible list affect OSPF results?
The Eligible list defines what OSPF-discovered routes get targeted for additional Lumeta discovery in that zone (e.g., Path and Host Discovery).

Are Link State Advertisements (LSAs) encrypted?
No. OSPF does not encrypt LSAs, however MD5 encrypted passwords are supported by Lumeta when used in your OSPF network, in addition to plain-text password authentication, or no authentication.

How may interfaces, physical or virtual, should be used on a Scout?
All interfaces are on and available when Lumeta is delivered as an appliance. On a virtual server, choose to configure however many interfaces you need. A single Scout can supply data to multiple network zones. Even a single Scout interface can supply data to multiple zones. However, data is not shared between zones.

What happens when you delete a Scout?
Deleting a Scout disables it within its zone, along with any and all collectors that may have been using that Scout.