You cannot virtualize a Threat Manager if it does uses network spanning (port mapping is only available for physical appliance)

Virtual vs physical decision tree image and a Threat Manager - VMware - Deployment and User Guide.

<https://docs.alertlogic.com/install/log-manager-virtual-appliance.htm>

Alert Logic does not have a Vendor specific virtualization method, the virtualization experience has best suited a VMware environment.

Certified Virtual Vendor - N/A

Alert Logic does offer .ova images through the portal for Threat, Log and WSM appliances and these can be used to create Virtual Machines on most common platforms.

You can find the download images here:

<https://console.clouddefender.alertlogic.com/tm/support/downloads>

<https://console.clouddefender.alertlogic.com/lm/support/downloads>

Minimum Vendor Virtual Versions - the disk images are of the latest build for the products.
Recommend Guest OS requirements –

Regarding the specification for the Virtual Threat Manager, the minimum recommended requirements are:

| **Components** | **System Requirements** |
| --- | --- |
| CPU | 4 virtual CPUs |
| RAM | 8 GB |
| Disk space | 40 GB minimum |
| Supported virtual environment | VMware only |
| Log collection support | N/A |
| Encryption | TLS Standard (SSL): 1024–2048bit key encryption, 256bit AES bulk encryption |

[https://docs.alertlogic.com/requirements/system-requirements.htm?#tmVirtualAppliance](https://docs.alertlogic.com/requirements/system-requirements.htm#tmVirtualAppliance)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Technology | Eligible for virtualization | Certified Virtual Vendor | Minimum Vendor Virtual Versions | Recommend Guest OS requirements | Additional Comments |
| Threat Manager | Yes | VMWare | V5.1 | Guest OS provided by Alert Logic | We cannot virtualize a Threat Manager if it does uses network spanning (port mapping is only available for physical appliance) |
| Log Manager | Yes |  VMWare |  V5.1 |  Guest OS provided by Alert Logic |  N / A |
| WAF | Yes |  VMWare |   |  Guest OS provided by Alert Logic |   N / A |
| WSM | Yes |  VMWare |   |  Guest OS provided by Alert Logic |   N / A |

Best practices for upgrading or migrating generally follow a parallel process, where the replacement Threat Manager is first created, configured and confirmed to be receiving traffic. Once this is completed the original Threat Manager that is due to be replaced is then decommissioned. This ensures that there is minimal disruption to the inspection of traffic.

A Virtual appliance can be deployed into an existing virtual environment and would allow you to assign specific resources to meet the demand for of your Threat Manager and/or Log Manager.

The benefits would be that if you currently have a virtual environment, it may be easier to deploy Virtual Threat or Log managers into this and "tune" these virtual machines to your requirements

The physical appliance has a set specification, for example, the Next Generation Threat Manager Tier 1 contains a 4 Core CPU and 16GB of memory. The advantage of this physical device allows you to rack the sensor into an existing physical network. The other advantage of a physical device is generally they provide more processing power and this can be aligned with a network that requires a large amount of traffic or Log messages to be processed.

**Overall, Virtual Threat / Log Manager configuration:**
Pros: Better scalability, can be cheaper to run with room for reducing / increasing resources more effectively.

Cons: Generally lower performance compared to physical.

**Physical Threat / Log Manager**
From a performance standpoint, it is difficult to specify a number of the utilization for a virtual threat or log manager. It would depend on a number of factors, including underlying hardware, type of traffic and type of log messages.
The Physical Tier 1 NGTM Threat manager would generally provide greater processing power and is able to provide around 1.2 Gb/s of traffic analysis.

Agent traffic can be switched over to the new appliance by adjusting the Assignment Policy on the Alert Logic UI. If there are configurations on the Agent itself involving a single point of egress, these would need to be updated also.

The appliances will need to be claimed once they have been spun up, which can be accomplished by visiting the private IP address of the appliance in a web browser and entering your Unique Registration Key.

The instructions on how to claim the appliances are here:
<https://docs.alertlogic.com/install/threat-manager-virtual-appliance.htm>
<https://docs.alertlogic.com/install/log-manager-virtual-appliance.htm>

You can find your Unique Registration Key in the portal on the same page as the virtual appliance images.

Please let us know in advance that you will be terminating or migrating appliances, so that we can suppress monitoring and alerting.

**Amending the agents**​
If you are able to use the same internal IP address for the new appliance, then this would be preferable, as it would avoid any need to change the agent's configuration. You will still need to amend the Assignment Policies in the portal to point the agents at the new appliance. However, any egress 443 traffic would flow as before.