Alert Logic Enterprise Shared Services

Unified Agent Deployment Guide

Contents

ALERT LOGIC UNIFIED AGENT

- Agents are required to be deployed within your environment to feed important data to our Alert Logic ActiveAnalytics platform for correlation and review.
- Alert Logic provides a single unified agent for supported Linux and Windows platforms to capture network traffic towards Cloud Defender appliances, and captures local system logs directly towards Alert Logic (encrypted and compressed).
- Alert Logic provides a single unified agent for the Cloud Defender Suite for supported Linux and Windows platforms
- Threat Manager utilizes network packets replicated and forwarded, within the local VPC, by the Agent "Protected Host" to the Cloud Defender appliance for network detection.
- Log Manager will collect local system logs captured by the Agent via syslog or identified windows event streams and send to the Alert Logic cloud infrastructure.
- All data collected by the agent is compressed and sent to Alert Logic via HTTPS (TLS Standard (SSL) 2048bit key encryption, 256bit AES bulk encryption).
- **NOTE:** In order to fully benefit from the automatic agent assignment (i.e. to avoid manual assignment) please install agents only after provisioning the appliance.

You must access the Alert Logic user interface (UI) to download and install the agent for Windows or Linux.

- At the top of the Alert Logic user interface (UI), from the drop-down menu, select **Threat Manager**.
- In the left navigation, click **Support**. From the menu bar, click **Downloads**.
- Download the appropriate agent and follow the on-screen instructions.
- For Windows users, click **Windows Agents**, and then select the desired agent.
- For Linux users, click **Linux Agents**. Linux users can select either Debian-based agent installers or RPM-based agent installers. Both installers are available in a 32-bit or 64bit format.
- Locate the **Unique Registration Key** from the **Downloads** screen. Copy your unique registration key. You will need this key to register the agent with Alert Logic Data Center.

Please refer to the updated online instructions for agent installation details, including access to registration key.
Replace **<registrationKey>** with your own registration key in the provided example scripts.

Install the Alert Logic agent for Linux
Install the Alert Logic agent for Windows

AGENT INSTALL IN LINUX (RHEL/CENTOS)

```
#!/bin/sh
yum -y install https://scc.alertlogic.net/software/al-agent-LATEST-
1.x86_64.rpm
/etc/init.d/al-agent provision --key <registrationKey> --inst-type host
echo "*.* @@127.0.0.1:1514;RSYSLOG_FileFormat" >> /etc/rsyslog.conf
service rsyslog restart
/etc/init.d/al-agent start
```

If you run SELinux, you must first run the following command:

```
semanage port -a -t syslogd_port_t -p tcp 1514
```

AGENT INSTALL IN WINDOWS

```
msiexec.exe /i [path]al_agent-LATEST.msi /quiet PROV_ONLY=host
SENSOR_HOST=vaporator.alertlogic.com SENSOR_PORT=443 REBOOT=ReallySuppress
PROV_KEY=<registrationKey>
```

SINGLE POINT OF EGRESS CONFIGURATION

- Typically, Alert Logic agents capture network traffic towards Cloud Defender appliances, and captures local system logs directly towards Alert Logic (encrypted and compressed).
- For scenarios where provisioned agents cannot provide logs to Alert Logic directly (e.g. nodes with no Internet access) you can configure the agents to use a designated NAT node or the Cloud Defender appliance as a NAT node. Both network IDS-relevant traffic and compressed/encrypted log data will be routed via the Cloud Defender appliance.
- This strategy allows the enforcement of dedicated nodes for egress traffic, but transmission of log data becomes dependent on the availability of the configured NAT device or Cloud Defender appliance.
- To speed up log collection troubleshooting we recommend not to mix log collection strategies, or at least leverage Protected Hosts tagging to document the expected behavior.

If you want to specify a single point of egress for agents to use, run the following command for Linux hosts:

```
/etc/init.d/al-agent configure --host <LOGMANAGERAPPLIANCEIP>
```

If you have set up a proxy, and you want to specify the proxy as a single point of egress for agents to use, then run the following command (A TCP or HTTP proxy may be used in this configuration):

```
/etc/init.d/al-agent configure --proxy <PROXYIP/PROXYHOST>
```

INSTALLATION FOR IMAGE CAPTURE (EC2 AMI)

- There are instances when it is necessary to install the agent but defer the provisioning and registration of the agent. If the agent is installed on a system that will be imaged and cloned in the future, the agent should not be registered or provisioned before the system is imaged. Doing so would result in multiple systems having the same identity and cause collection to fail.
- The agent can be installed in a *"install only"* mode (Bake-in Method) before an image is made. An agent in this mode is not provisioned. That is, the agent does not get its unique identity, certificate and key files. It is also not registered as an active source. The agent service is not started and is configured to have a manual start type in Windows machine but can be set to auto start before creating the base image. In Linux, the agent service starts automatically when the machine is boot-up for the first time. When the agent is starts, it will acquire its unique identity and get provisioned and registered.

At a high level, the bake-in method involves:

- Create a new image from the existing or base system image where the Alert Logic agent is not currently installed/registered
- Modify the image by downloading and installing the appropriate agent for that machine (based on OS and architecture)
- Provision the agent but do **not** start the agent
- Bake the new image

The following steps are required for one-time provisioning per base image:

- Create an image from the existing or base image to be modified (Must not include Alert Logic agent)
- Download and install the appropriate Agent package on the instance with your unique Registration Key
- NOTE: Agent packages and unique Registration Key are also available via the Threat Manager or Log Manager UI Support Page.

Linux RPM	32-bit: https://scc.alertlogic.net/software/al-agent-LATEST-1.i386.rpm 64-bit: https://scc.alertlogic.net/software/al-agent-LATEST-1.x86_64.rpm	`rpm -ivh al-agent-<version>.rpm`
Linux DEB	32-bit: https://scc.alertlogic.net/software/al-agent_LATEST_i386.deb 64-bit: https://scc.alertlogic.net/software/al-agent_LATEST_amd64.deb	`dpkg -ivh al-agent-<version>.deb`

Windows	MSI: https://scc.alertlogic.net/software/al_agent-LATEST.msi
	ZIP: https://scc.alertlogic.net/software/al_agent-LATEST.zip
		`Interactive: msiexec /i [path]al_agent-LATEST.msi PROV_ONLY=host INSTALL_ONLY=1`
		
		`Unattended: msiexec /i [path]al_agent-LATEST.msi /q PROV_ONLY=host INSTALL_ONLY=1 PROV_KEY=<uniqueRegistrationKey>`

Next steps (Linux)

Provision the agent	`/etc/init.d/al-agent provision --key <UNIQUEREGISTRATIONKEY> --inst-type host`

Configure the agent service	Reconfigure local syslog daemon (rsyslog or syslog-ng) to forward logs to 127.0.0.1 port 1514 (TCP)
	
	`rsyslog.conf:`
	`*.* @@127.0.0.1:1514;RSYSLOG_FileFormat`
	
	`syslog-ng.conf:`
	`destination d_alertlogic {tcp("localhost" port(1514));};`
	
	`log {source(s_src); destination(d_alertlogic);};`

Restart the syslog daemon.	**NOTE:** These configurations will direct your local syslog to the agent on TCP port 1514.

Next steps (Windows)

- By default the agent is configured to have a manual start in “INSTALL_ONLY” mode.
- To change this to an automatic startup type use the services.msc GUI or the following command before creating the base image:

```
sc config al_agent start= auto
```

Last steps (Windows and Linux)

- Stop the machine and bake a new base image
- At this point, the new image is ready to be used
- Each instance will start the Alert Logic agent automatically when booted, and each agent will be registered individually.