Logmanager

Logmanager – Proof of Concept test guide

An integral part of any Logmanager sales engagement is installation and testing of the solution at customer environment in the form of PoC (Proof of Concept test). To be precise - what is meant by Proof of Concept test - Logmanager PoC is a realization of methods or ideas in order to demonstrate Logmanager feasibility in a customer environment. It should demonstrate in principle, with the aim of verifying, that the concept of deploying Logmanager has practical potential for a given customer. Remember: PoC is by design small and covers only a selected customer use-cases (usually up to five) – it does not replace implementation service and full Logmanager deployment.

PoC is delivered by a certified partner of the Logmanager solution. A registered partner carries out this service usually with the support of a dedicated vendor Sales Engineer. This guide defines individual steps which need to be taken to run a successful PoC, responsibilities of each interested party, schedules and installation check-list.

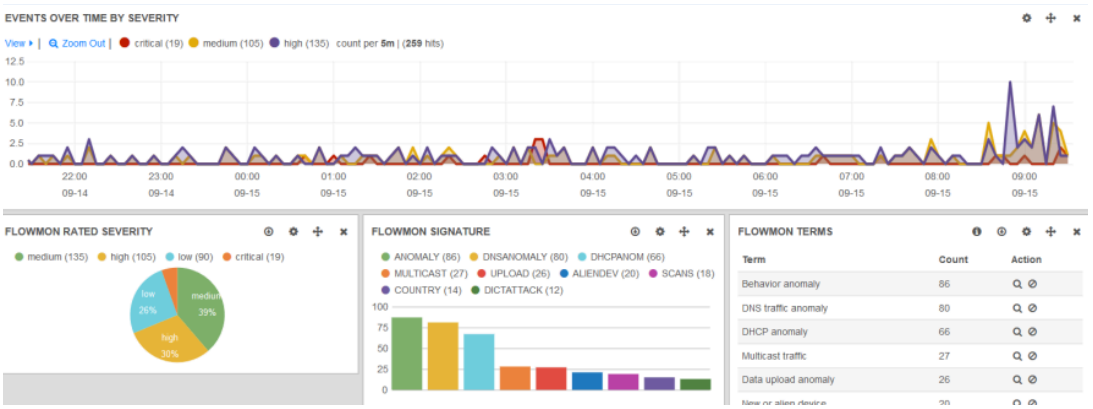
Logmanager POC Technical Discovery

As the name suggests, the goal of the PoC is to prove a concept. In this case, the general concept is the ability of the tested system to perform and provide log management functionality. As this is a complex subject which can be divided into many parts different for each client. Understanding the main tasks which the solution should fulfill has to be known and agreed by all involved parties before PoC. Approaching PoC without establishing such an agreement will lead to a chaotic and meaningless process.

Below are some questions which should be asked to help understand log management needs:

1. **Goal/Objectives** – at the end of the day, what are you trying to accomplish? What's the main goal of considering log management / SEM /SIEM in your company?
2. **Burning issue** - is the issue at hand pressing, in a sense that lack of solution costs you revenue?
3. **Success** – how will you measure success of the PoC? Did you consider/know that?
4. **Requirements** – do you have any specific requirements which solution needs to fulfil? Specific constraints you need to work with such as laws, regulations, policies?
5. Capabilities – are there any specific capabilities you are most interested in? For example - reporting, alerting, correlations, rapid data search, data visualizations?
6. **Competition** – do you have any prior experience with log management solutions? Did you try other products but decided they were not for you? Are you planning on testing anything else?

Logmanager



POC Schedule:

Logmanager PoC usually takes a minimum two weeks. Each PoC is a bit different, so it's hard to provide exact steps, but below schedule - is what usually works best based on our experience:

PoC Preparation:

1. **Discovery session** – 30min max – finding out the main issue's client is facing and the need for a log management solution. The goal is to help Sales Engineers prepare for the demo.
2. **Logmanager presentation/demo** – 1 to 2h - overview of main functionalities, how we do things, product demo with focus on client needs.
3. **Sizing document and Offer** – creation of offer based on sizing document received from the client to make sure there is enough budget in place for Logmanager purchase in case of successful PoC results.
4. **PoC preparation meeting** – 30min – goal of the meeting is to clearly define success criteria for the PoC.

PoC Test process:

1. **PoC Installation** – 2 to 3h – installation of Logmanager demo box in client environment and configuration of basic sources.
2. **PoC Installation Follow up** – 1 to 2h – configuration of additional sources. Setting up other functionalities requested by the client (such as alerts, custom dashboards, reports).
3. **Additional meetings** as needed. Ongoing review of the PoC progress.
4. **PoC Summary** – 1 to 2h – overview of the gathered data, presentation of main goals requested by the client.

POC Responsibilities

Each party involved in the PoC has certain responsibilities to fulfill in order for PoC to be successful. Below are requirements for each interested party:

Logmanager

Customer:

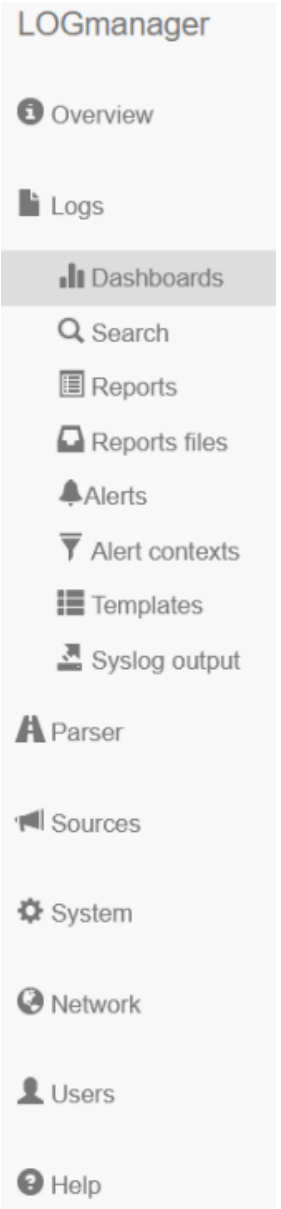
- Defining main goals of the PoC (together with vendor technician).
- Providing clearly defined success criteria for the PoC.
- Actively participating in technical discovery sessions.
- Assigning engineers to oversee the PoC according to the previously agreed goals.
- Filling list of installation prerequisites.
- Filling the sizing document, ensuring budget is available based on received offer.
- In case of PoC being run on-site, reservation of separate rooms for each PoC meeting.

Partner Account Manager:

- Helping clients with defining challenges and needs for the solution.
- Assigning engineers to run the PoC according to the previously agreed goals.
- Sending documents and preparing the offer.
- Coordinating meetings and communication with clients.

Logmanager technician (partner or vendor):

- Continuous configuration of other sources requested by customers and checking correct classification, parsing and processing of customer data.
- Alerts proposal and definition at customer request.
- Training of the assigned customer engineer, repeating the demonstration of basic functions and explaining system advanced features.
- Remote support and consultations via virtual meeting system at customer request.
- Configuration debugging and diagnostics of correct activity of the system.
- Questions and answers to technical queries, help with designing dashboards, alerts, reports, just everything for customer satisfaction.
- Creation of written PoC conclusion and wiping all customer data from PoC demo unit.



Logmanager

Installation Prerequisites

Below is a list of prerequisites needed for installation. It should be provided by the Customer to the responsible Logmanager technician before the installation to allow for smooth deployment. Attached to this document is an excel sheet, which should be filled according to the below list.

1. **List of log sources to be collected by Logmanager, containing:** Source type (vendor name, system function, software version); Source IP; Designated destination port; Expected log volume (if known).
2. **Information necessary for deploying Logmanager to the network:** IP Addressing for Logmanager, including: IP Address; Subnet mask; Default gateway; Primary DNS IP address; Secondary DNS IP address; NTP servers.
3. **SMTP relay configuration (for sending security and system alerts):** SMTP Addressing for Logmanager, including: SMTP IP address/Hostname; Port; Source email address (email address which will be shown as a sender); Username/ password if SMTP Authentication is required; Admin email (email address to which Logmanager will be sending alerts about internal issues, such as low buffer size).
4. **If integration with LDAP for user authentication is required:** IP address of the LDAP server; IP address of the sec. LDAP server; LDAP service port; The base directory structure (e.g.: DC=test,DC=example,DC=com); Suffix directory structure (e.g.: @test.example.com); Username/password for access to the information in Active Directory; List of LDAP groups which should have access to the Logmanager.

Physical requirements

1. Logmanager PoC is usually run on a demo box, which is a small Intel NUC unit (115mm x 111mm x 48.7mm). It needs a little space on a flat surface and single power connection, preferably one which is backed up by an UPS.
2. Ethernet connectivity for Logmanager – 100/1000Base-T to admin VLAN (or VLAN designed to transfer the log data). Doesn't require access to the internet during the PoC, optional VPN connectivity for remote access of Logmanager technician.

PoC Installation Check List

Installation means the initial deployment and putting Logmanager into operation in the customer's environment. Familiarizing with operating rules, configuration of the sources of logs, events and machine data and checking the function of all the components. Time needed for the installation depends on the environment complexity, usually it does not exceed 3 working hours.

1. Initial configuration:
    - Connect Demo Box to the network by setting a provided network config on a primary interface (IP Address, Netmask, Gateway, DNS, NTP).
    - Test GUI availability.
    - Test access to Logmanager update server.
    - Make sure Demo Box has the latest code version. If not, perform an update.

- Disable automatic Telemetry sending to vendors.
- Configure SMTP settings and test email notification sending.
- Optionally:
    - Create user groups and rights for Logmanager (Local or centralized via AD/LDAP).

2. Add supported sources of logs and events:
    - Make sure classification and parser is available for given sources. Create proper data classification.
    - Assist customer engineer to configure source devices for sending logs to Logmanager.
    - After connecting each source make sure logs are being collected and parsed properly (make use of native dashboards for given source type – if they are being populated properly).
    - In case of Windows Systems:
        - Make sure Logmanager is accessible from the station/server over the network to ports 443/20514/20515.
        - Make sure the SRV record is properly resolved on the workstation.
        - After installation, check if the station was added to the Windows Agents List.
        - Configure either global or per-station event collection settings and filters.
        - Make sure logs are being pulled from Windows Station.

3. In case of unsupported sources of logs and events:
    - Create a proper classification based on chosen source attribute (source IP, destination port, syslog program name). Set classification action as TAG (as currently there is no parser).
    - Assist customer engineer to configure source device for sending logs to Logmanager.
    - Make sure logs are being properly gathered and tagged based on created classification.
    - Export logs to CSV file in RAW format.
    - Send exported CSV file to assigned Logmanager System Engineer for parser creation.