Details of Linux Maintenance Service

XF SYSTEMS OÜ / SIIM VAHTRE

2018-03-27

Contents

1 Summary of Works

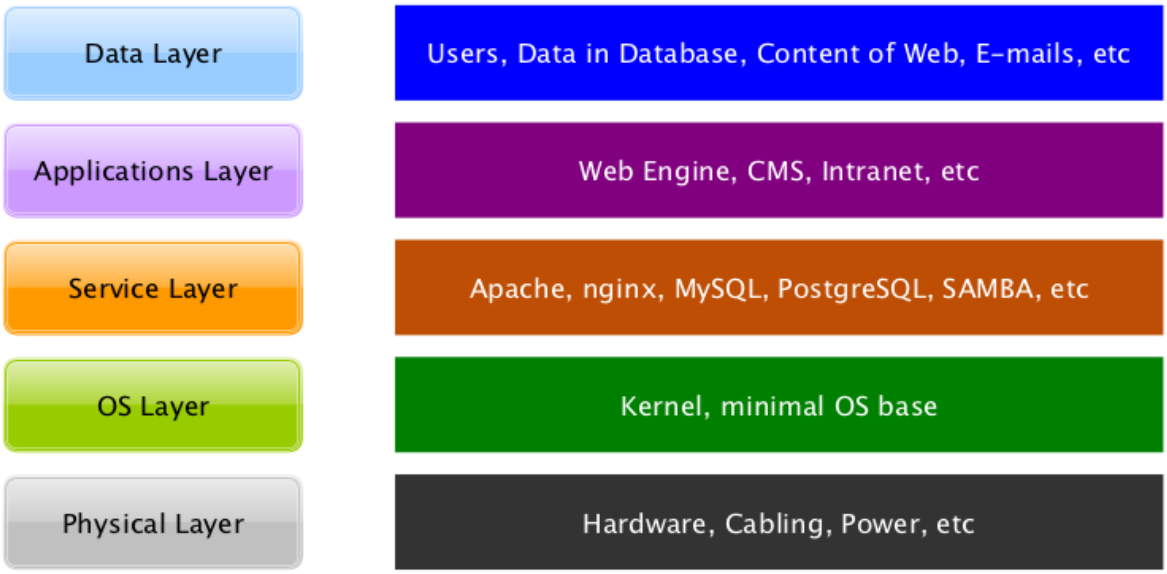
XF maintenance and monitoring service includes the following tasks:

Category	Description
Maintenance works	Tasks that are done continuously and periodically by XF's staff without a specific order from the customer. The purpose of these works is to guarantee a smoothly functioning and stable server.
Automated works	Tasks that are done by XF ServAdmin monitoring system automatically 24/7/365. These works provide constant monitoring and quality control of the server, as well as the necessary background information for increasing the quality of the service and for various other works.
Necessity-based	Tasks that are done at the client's request, a notification from the monitoring system, or when XF's staff notices the necessity in relation to everyday work or a periodic server audit.
Audit	A periodical thorough audit of all aspects of the server. It is carried out when the server is first set up and later at the request of the customer or when necessary.
Additional works	All other works not mentioned above. Additional works are done according to agreements or for an additional fee.

1.1 XF's Responsibilities

XF is responsible for the following service layers of a server:

- **Physical layer** - network connectivity, hardware functioning, the state of hardware components, physical security - XF only takes responsibility for the monitoring of a server's resources and a timely notification of the client in case of problems. XF will use remote management (KVM, power switch), if the possibility exists. If XF is hosting the server, it will also be responsible for that layer.
- **Operating system layer** - XF is responsible for the core (Kernel), distribution and its minimal base.
- **Services layer** - XF's responsibilities are limited to the services and applications specified in the contract, concerning processes running on the server that are outside of the base system (e.g. apache, mysql, postfix, Samba, OpenVPN).
- **Applications layer** - the customer is usually responsible for all systems running on services, e.g. web page engine, CMS, Intranet, information systems. By way of exception, XF will take responsibility limited to the services and applications specified in the contract.
- **Data layer** - data used by applications or services (including users list, data in SQL databases, the content of web pages, emails, etc.) is the responsibility of the customer, with the exception of responsibilities specified in the contract (e.g. adding accounts, changing permissions or other similar tasks).



1.2 Maintenance Works

1. Responding to errors reported by the monitoring system.
2. Notifying the customer of the problems that have been discovered or might arise.
3. Responding to automated notification mechanisms (e.g. email root user) of the operating system or services running on it.
4. Implementing critical security updates **ASAP**.
5. Implementing all security updates (including non-critical) at least 1-2 times a month.
6. Keeping the server standardized.
7. Maintaining the documentation of the server. Documentation is kept for the server's hardware, services, applications. Information about integrations with other systems, as well as other information XF possesses and deems necessary to be kept is also documented.

1.3 *Necessity-based* Works

1. Making changes in the configuration of services.
2. Optimizing services.
3. Analyzing and checking log files.
4. Conducting speed-, load- and other tests.
5. Analyzing load graphs.
6. Restoring data from backups.
7. Finding solutions to technical operating system-specific problems.
8. Changing the configuration of the operating system and core (Kernel).
9. Optimizing the operating system and core (Kernel).
10. Making suggestions about adding, updating, replacing hardware or software.
11. Answering information requests regarding the server or its documentation.
12. Consulting on related matters.
13. Fixing all problems that are directly caused by XF's activity in its area of responsibility.

1.4 Extra Works

Additional works require previous arrangement and are done for the hourly fee of additional works or an agreed project fee. Additional works are all works that were not previously mentioned, or works outside of XF's area of responsibility specified in the contract. Examples of additional works:

1. Works done outside of working hours or that require quick response time (quicker than specified in the contract).
2. Implementing or configuring services or applications not specified in the contract.
3. Installing or re-installing a server.
4. Larger updates (e.g. a major distribution version update).
5. Moving data from one service provider to another or from one service/solution to another.
6. Works regarding backups that are not related to a concrete one-time recovery task (i.e. a one-time recovery of a concrete folder as of a given date is not additional work. Additional work is, for example, searching for vaguely described data from archives, or testing different versions).
7. Training and consultation that are unrelated to a concrete provided service.
8. Configuration and maintenance of special solutions or non-standard software.
9. Development-, programming- and scripting works.
10. Any major change in the *status-quo*.
11. Any task that can be considered unreasonable or that interferes with guaranteeing seamless work.

XF might categorize regular works as additional works for one of the following reasons:

1. The customer has granted administrator access to the server to third parties and there are reasons to believe that their activity or carelessness created the necessity for the given works.
2. The necessity for the given works arises from the customer's activity in a service layer that should be XF's responsibility (except when this activity is previously coordinated with XF).
3. The necessity for the given works arises from the customer's inactivity when XF has previously notified the customer and given sufficient reasons why the activity is needed.

1.5 Audit Details

An audit is a methodical, thorough inspection of a server. It consists of concrete tasks that are described in detail in the internal documentation of the company. In short, it comprises the following:

1. A thorough analysis of the information gathered by the XF monitoring system (see *Automated works*).
2. An analysis of the server's load graphs.
3. Checking disks, the age of hardware, versions of BIOS, firmware, etc.
4. Checking if the server's software is updated and mapping possible solutions.
5. Checking if the server is standardized.
6. Checking the current status of the server (processes, open ports, quality of network connectivity, speed of hard drive).
7. Checking the functioning of automated scripts (cron).
8. An analysis of logins and the history, frequency and other aspects of service use.
9. Checking the server's ability to log and a thorough analysis of log files.
10. Checking the data on file systems (to detect rootkits, worms, viruses and other fiends).
11. An audit of the firewall.
12. A remote security scan.
13. A security check of the configuration of services and applications (postfix, apache, php, dns, etc.).
14. Checking backups.
15. A physical check of the server if necessary (a secure location, surveillance, access check, etc.).
16. If XF is hosting the server - validating, restructuring and improving the server's documentation.

An audit results in a report covering the detected issues and suggestions for the future.

1.6 Automated works / monitoring

XF is constantly conducting various tests on servers using its specialized software. The results of these tests are saved. All events and changes are registered and specialists are notified when necessary. In addition, the system generates various statistical information and charts that provide important background information for various problems and help predict future issues.

The following list is illustrative. In reality, the number of tests is more accurate and, depending on the server, some parameters might not be possible to monitor at all.

The list was last reviewed: 2018-02-23

1.6.1 Service Quality Checks

1. Checking the performance of concrete services and applications on a server
2. Is the web page operational?
3. Checking the content of the web page (e.g. check if the number of products displayed on the page is correct)
4. Testing email traffic

1.6.2 Server's Main Resources Usage Checks

1. Free disk space and file count
2. Processor usage
3. RAM and swap usage
4. Network functioning and latency (ICMP echo / ping, number of connections, current speed and volume of network usage, the number of ARP entries)
5. The number of processes

1.6.3 Hardware Performance Checks

1. The state of storage media (SMART, disk faults, Write Cache, file system tests)
2. The status of hardware RAID or software RAID
3. General check of hardware (e.g. DRAC information)
4. Temperature
5. Errors registered at the level of server core
6. Age of hardware

1.6.4 Backup Functioning Check

1. The functioning of BackupPC, Bacula, RDiffBackup, RSync and other backup software
2. Checking the functioning of MySQL / PostgreSQL database backups (sql dump)
3. Checking backing up of various specialized solutions (e.g. Hansa text copies, Zimbra backups)
4. Checking the functioning of a simple file-based backup (e.g. tar, cp)

1.6.5 Security Checks

1. Checking that the server's operating system is up to date, checking the need for software updates
2. Checking the permissions of important folders
3. Checking the private data on web pages
4. Checking user and access information (shell-users, SSH keys, etc.)
5. Various firewall and access rights tests (continuous remote access check)
6. Recursive DNS check
7. The number of emails in queue, detection of possible local viruses/spam outbreaks
8. Check of various concrete security issues and hacks
9. DoS attacks notification

1.6.6 Other Checks

1. Check that the clock is synchronized and time zone is correct
2. Server hostname check
3. Functioning of the local name server service
4. Automated check of the correctness of name server zone files
5. Various standardization checks

1.6.7 Special Solutions

1. Application- or service specific checks
2. Checks specific to a concrete client's needs
3. High Availability check (Linux-HA, DRBD, cluster-software)
4. Check if a certain file or attribute exists

1.6.8 Automated Information Saving

1. Core and operating system version
2. Brand and serial number of the server
3. Current uptime, time of startup
4. Network configuration
5. Time of server installation

1.6.9 Saving Configuration Changes

1. Registering changes in the server's system configuration (once a day)
2. Registering changes in additional devices (e.g. switches, routers) (once a day)

1.6.10 Monitoring Resource Graphs

XFServAdmin software downloads data from the server, processes them and renders them graphically over time. These data help, for example, to find possible bottlenecks in the server or predict future problems.

1. Processor usage and the type of usage (user processes, core, IO, virtualization)
2. Load average and the correlation of it with the number of processors and IO usage
3. Memory and swap usage
4. Uptime
5. Disk space and file count usage
6. Detailed usage of disks and other block devices (writing, reading, IO latency, IO-merge 1. effectiveness)
7. Latency of network connections (“PING”), not including overhead
8. The number of neighboring devices
9. The number of active connections
10. Network usage (upload and download speed), volume
11. Temperature, speed of ventilators, power usage
12. The number of users
13. The number of processes
14. The number of unsent emails
15. The response time of a web page or other web service in different layers
16. Monitoring (temperature, network traffic, etc.) of additional devices (e.g. switches, routers, UPS, etc.)