URBAN SOFTWARE

Dedicated to serve our customers

CACTI HEALTH CHECK REPORT

PREPARED FOR: <CUSTOMER>

URBAN SOFTWARE
Dedicated to serve our customers

Contents

1. PREFACE

1.1. Confidentiality, Copyright, and Disclaimer

1.2. About This Document

This document provides the reader with a detailed description of the results of the Urban-Software.com Cacti Health Check performed by Urban-Software.com for Client.

1.3. Audience

This document is intended for Client technical staff responsible for the following functions:

- Developing and maintaining a Linux based Cacti System
- Optimizing and maintaining Cacti configurations within the Client environment

1.4. Terms

The table below provides a glossary of the terms and acronyms used within this document.

ACRONYM	DESCRIPTION

2. PREPARATION

2.1. Health Check Approach

The following table outlines the focus of each phase.

PURPOSE	DETAILS
Health Check	Assist Client in a prioritized review and health check of Client's existing Linux environment running Cacti on Ubuntu. • Review configurations and hardware platforms. • Review installed and started services. • Review level of installed updates. • Review partitioning and filesystem layout. • Review kernel parameters. • Review network architecture for physical and/or virtual systems, including network interfaces, drivers, and applicable options, interface bonding, and routing and bridging configuration. Assist Client and client partners in troubleshooting Cacti on Linux performance

3. HEALTHCHECK DETAILS

3.1. Server Hardware

In this chapter, we examine the area of server hardware and present the results of the investigation along with recommendations for improvement.

3.1.1. Hardware Configuration

The Cacti systems is a physical 1U Intel Single-CPU RI1102H Server (V3.0) system with the following specs:

1HE Intel Single-CPU RI1102H Server (V3.0)	1
1HE Supermicro Chassis CSE-511/512L	1
1HE Kühler für Supermicro (X8SIL+X9SCM+X10SLH-F)	1
Optimized for Linux	1
Supermicro Mainboard X11SSH-F	1
8x SATA-3 (6 Gb/s) SW-Raid Controller on Board C236 (0,1,5,10)	1
Full Remote Management (KVM over LAN, IPMI 2.0) inkl. Management software, DHCP configuration	1
Intel Xeon E3-1240 v5 4-Core 3,5GHz 8MB 8GT/s	1
16 GB (2x 8GB) ECC DDR4 2133 RAM 2 Rank ATP (Premium)	1
240 GB SATA III Samsung SSD 2,5" (PM863)	2
2x 2,5" HDD Kit	1
260 Watt Power Supply	1

3.1.2. Network Cards

Investigation: Are there any errors or dropped packets on the network cards?

Observation:

```
eno1   Link encap:Ethernet  HWaddr 18:66:da:xx:xx:xx
       inet addr:172.x.x.x  Bcast:172.xx.xx.xx  Mask:255.255.255.0
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:110463181 errors:0 dropped:4833 overruns:0 frame:0
       TX packets:113531346 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:32441297728 (32.4 GB)  TX bytes:20783916637 (20.7 GB)
       Interrupt:63
```

eno1 is configured to use 1000Mb/s
Dropped packages have been identified on eno1 and should be investigated.

Guidance: [illegible]

[redacted]

3.1.3. Disk Drives

Investigation: Are I/O wait issues occurring on the disk drives?
Are any errors occurring in the syslog?

Observation: No error messages show up in syslog or dmesg.

Guidance: [redacted]

3.1.4. Memory

Investigation: Is there any indication of a failing memory module?

Observation: n/a

Guidance: [redacted]

3.2. Installed Software

In this section we examine the area of installed software and present the results of the investigation along with recommendations for improvement.

3.2.1. Operating System

Investigation: What version and update or Operating System is installed?

Observation: Ubuntu Linux 16.04 – 64bit

Guidance: [redacted]

Investigation: When was the last kernel update applied?

Observation: The kernel version does not differ between the systems:
4.4.0-98-generic

Guidance: [redacted]

Investigation: When was the last package updates applied?

Observation: The system has vulnerable packages, packages with known security flaws and which already have an update available. It also requires a reboot (see /var/run/reboot-required.pkgs)

Guidance: [illegible]

3.3. Access

Investigation: How Is user authentication managed?

Observation: User authentication is not centralized. They were using local username and password for all accounts. This may cause security issues due to the high operating cost of managing and changing account access.

Guidance: [illegible]

3.3.1. Root Access

Investigation: Is root access allowed remotely?

Observation: The server does allow remote root access using public-key authentication: **PermitRootLogin** was set to **without-password** in the **sshd_config**

Guidance: [illegible]

3.3.2. Password Policy

Investigation: What are the password policies on the system?

Observation: PAM module for password strength testing like pam_cracklib was not used
Minimum and Maximum password age was not set in /etc/login.defs
Default umask in /etc/login.defs could be more strict like 027

Guidance: [illegible]

3.4. Storage Configuration

3.4.1. File system layout

Investigation: Are /tmp and /var on separate partitions?

Observation: The /tmp and /var directories are not separate partitions.

Guidance: [illegible]

3.4.2. NFS Mount Options

N/A

3.5. Network Configuration

3.5.1. Speed and Duplex

Investigation: The Network interfaces should be running with full speed

Observation: The network interface is configured to use auto negotiation for speed and duplex mode

Guidance: [illegible]

3.5.2. DNS Settings

Investigation: Is DNS resolution working and setup properly?

Observation: Only one dns server has been defined

Guidance: [illegible]

3.5.3. Ethernet Bonding

N/A

3.6. Network Services

3.6.1. Time and Clock Configuration

Investigation: Is NTP configured on the server?

Observation: The **timesyncd** was found on the system and running

Guidance: [illegible]

3.6.2. Syslog Daemon

Investigation: Central log server should be enabled

Observation:

Guidance:

3.6.3. Apache

Investigation: Are security/Anti-DoS/Bruteforce modules installed?

Observation: The Following modules have been installed
mod_reqtimeout/mod_qos
ModSecurity: web application firewall

Guidance:

3.6.4. Squid Proxy

Investigation: Is a proxy system running and configured properly?

Observation: The Squid proxy was running on the system
The file permissions of /etc/squid/squid.conf should be optimized.

Guidance:

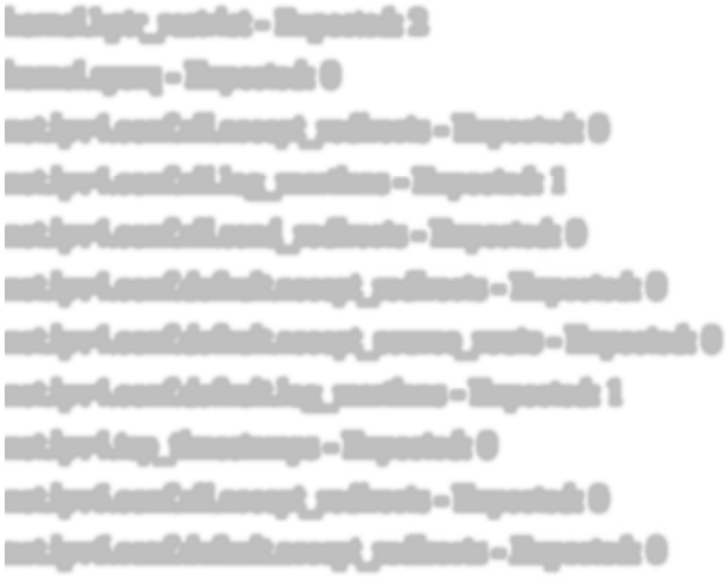
3.7. Kernel Parameters

3.7.1. Target Security Policy

Investigation: The Linux kernel can be tuned with the sysctl command. It uses a list of kernel parameters, which alter how the kernel should behave within the areas of storage, network, memory management, and more.

Observation: The kernel parameters differ from the list of best practices parameters

Guidance:



3.8. Security

3.8.1. SELinux/AppArmor

Investigation: Is SELinux/AppArmor enabled on the system?

Observation: AppArmor is installed and enabled

Guidance:

Investigation: Is IPTables/FirewallD enabled on the system?

Observation: IPTables is disabled on both system

Guidance:

3.9. Backup

3.9.1. Backup and Restore

Investigation: Is a backup/restore process in place?

Observation: No backup software was identified. No cronjobs for backups have been found.

Guidance:

3.10. Performance Analysis

3.10.1. Availability

Investigation: What is the uptime of the system?

Observation: The system has been up for the past 16days:
01:44:40 up 16 days, 20:47

Guidance: [illegible]

3.10.2. Disk space utilization

Investigation: Is there enough free space?

Observation: The system has enough free space left

Guidance: [illegible]

3.10.3. Disk I/O Performance

Investigation: Is the disk performance adequate?

Observation: The system does not have the sysstat package installed.

Guidance: [illegible]

3.10.4. NFS Performance

Investigation: Is the NFS performance adequate?

Observation: Nof NFS shares have been used

Guidance: The NFS performance should be fast and responsive. On virtualized systems, the nfsiostat package may not show the true NFS performance.

3.10.5. System Load Average

Investigation: Is the Load Average in normal range?

Observation: Thc I/O Wait timc is within thc normal rangc with 2.3 for thc 15 minutc average

Guidance: [illegible]

3.11. Cacti Settings

3.11.1. Cacti / Spine Version

Investigation: Is the current Cacti and Spine version installed?

Observation:

Guidance: [illegible]

3.11.2. Cacti Plugin Setup / Configuration

Investigation: Are current Plugins installed and configured?

Observation:

Guidance: [illegible]

3.11.3. Database Parameters

Investigation: Are the database parameters using the recommended settings?

Observation:

Guidance: [illegible]

3.11.4. RRD Storage Path I/O Performance

Investigation: Is the I/O performance of the RRD storage path adequate?

Observation:

Guidance: [illegible]

3.11.5. Poller Mode

Investigation: Is the correct poller being used?

Observation:

Guidance: [redacted]

3.11.6. Poller Settings

Investigation: Is the poller being configured according to recommended settings?

Observation:

Guidance: [redacted]

3.11.7. Boost Status

Investigation: Is Boost being used and configured?

Observation:

Guidance: [redacted]

3.11.8. Boost Configuration

Investigation: Is Boost being configured according to recommended settings?

Observation:

Guidance: [redacted]

3.11.9. Polling Times

Investigation: Are the polling times consistent and within the configured range?

Observation:

Guidance: [redacted]

3.11.10. Cacti Log

Investigation: Are errors/warnings showing up in the Cacti log?

Observation:

Guidance: [illegible]

4. CONCLUSION / RECOMMENDATIONS