



URBAN SOFTWARE

Dedicated to serve our customers

CACTI HEALTH CHECK REPORT

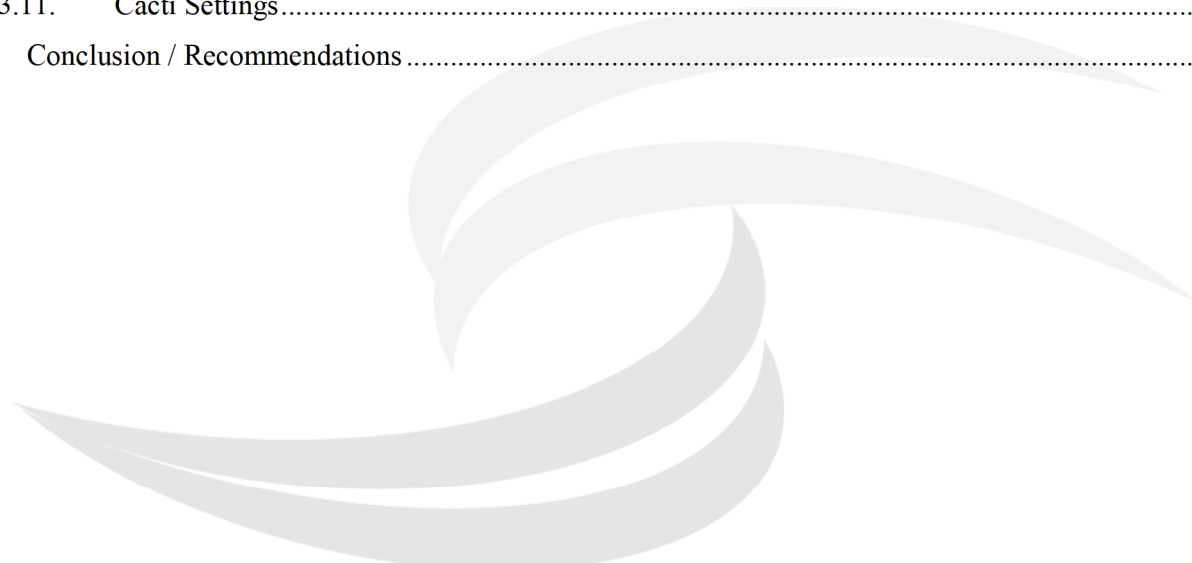
PREPARED FOR: **<CUSTOMER>**





Contents

CACTI HEALTH CHECK REPORT	1
PREPARED FOR: <CUSTOMER>.....	1
1. PREFACE.....	3
1.1. Confidentiality, Copyright, and Disclaimer.....	3
1.2. About This Document	3
1.3. Audience.....	3
1.4. Terms.....	3
2. PREPARATION.....	3
2.1. Health Check Approach.....	3
3. HEALTHCHECK DETAILS	4
3.1. Server Hardware.....	4
3.2. Installed Software.....	5
3.3. Access.....	6
3.4. Storage Configuration.....	7
3.5. Network Configuration.....	7
3.6. Network Services.....	7
3.7. Kernel Parameters	8
3.8. Security.....	9
3.9. Backup.....	9
3.10. Performance Analysis.....	10
3.11. Cacti Settings.....	11
4. Conclusion / Recommendations	13





1. PREFACE

1.1. Confidentiality, Copyright, and Disclaimer

This is a confidential document between Urban-Software.com. and **<CUSTOMER>** (“Client”). Copyright© 2017 Urban-Software.com. All Rights Reserved. No part of the work covered by the copyright herein may be reproduced or used in any form or by any means- graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems without permission in writing from Urban-Software.com

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	<p>Assist Client in a prioritized review and health check of Client's existing Linux environment running Cacti on Ubuntu.</p> <ul style="list-style-type: none">• 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. <p>Assist Client and client partners in troubleshooting Cacti on Linux performance</p>



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: Network speed and duplex modes should be selected optimal. When using distributed polling and distributed Check systems, the speed between both should be checked and configured with the best speed settings available.



Issues on the network card can show hardware issues and should be investigated.

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: High I/O load on the disk drives will cause the polling times to go up and responsiveness of the Cloud system will go down.
Issues in syslog can show performance issues for network based storage devices.

3.1.4. Memory

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

Observation: n/a

Guidance: ECC should be installed and configured for checking in order to monitor the hardware devices and identify possible issues with memory modules or other components

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 of Operating System is installed?

Observation: Ubuntu Linux 16.04 – 64bit

Guidance: Ubuntu Software.com recommends that the host be patched to the latest Update as part of a regular patch management. For Ubuntu the LTS version is recommended for long term support and patch availability.

Investigation: When was the last kernel update applied?

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

Guidance: Applying the latest updates ensures that patches bugs are fixed and relevant files changed.

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: Applying the latest package updates ensures that previous bugs are fixed and vulnerabilities closed.
Considering a tool like unattended-upgrade to keep the time of window for vulnerable packages as low as possible. It can be configured to automatically install security updates, while leaving manual updates for intervention of deployment.

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: A centralized solution like LDAP or ActiveDirectory should be used for managing access to the system. This centralized approach ensures better identity, policy and audit.

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: Proper locking of your SSH configuration can reduce human weaknesses. A common city should be selected. Since SSH has an important function on the system, proper locking of the server is needed.

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: Using the right tool helps with finding who can access control files.



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: To decrease the impact of a full /tmp or /var file system, place /tmp and /var on their own separate partitions. A full /tmp or /var directory will render the system unresponsive and may cause malfunctions on other system components like the database.

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: Network cards should be set to auto negotiation in order to determine the best available speed and duplex mode

3.5.2. DNS Settings

Investigation: Is DNS resolution working and setup properly?

Observation: Only one dns server has been defined

Guidance: A fullstack system should be configured for DNS resolution. A malfunctioning DNS resolution can cause a serious performance impact due to the DNS resolution timeout causing.

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: Network time protocol sync should be used to keep the systems in time sync. Especially for the real database the time should be kept in sync on all systems.

3.6.2. Syslog Daemon

Investigation: Central log server should be enabled



Observation:

Guidance:

A central log server enables troubleshooting as well as the logging of security related events.

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:

The following modules should be enabled

Apache mod_headers to guard webserver against Denial of Service

Apache mod_reqtimeout/mod_qos Module to protect against Slow-look attack

Apache mod_security to guard webserver against web application

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:

Check the permissions of /etc/squid/squid.conf to limit access

Configure Squid option reply_body_psize_psize to limit the upper size of response

Configure Squid option http_response_headers_size (0) to suppress the value

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:

The kernel parameters should be reviewed. The following provides a list of the parameters which differ

kernel.dmesg_restrict - Expected: 0

kernel.core_pattern - Expected: 1

kernel.dmesg_restrict - Expected: 1



kernel.yes - Reported 2
kernel.yes - Reported 0
net.ipv4.conf.all.accept_redirects - Reported 0
net.ipv4.conf.all.log_martians - Reported 1
net.ipv4.conf.all.rp_filter - Reported 0
net.ipv4.conf.default.accept_redirects - Reported 0
net.ipv4.conf.default.accept_source_route - Reported 0
net.ipv4.conf.default.log_martians - Reported 1
net.ipv4.conf.default.rp_filter - Reported 0
net.ipv4.conf.lo.conflict_srcaddr - Reported 0
net.ipv4.conf.lo.conflict_srcaddr - Reported 0

3.8. Security

3.8.1. SELinux/AppArmor

Investigation: Is SELinux/AppArmor enabled on the system?

Observation: AppArmor is installed and enabled

Guidance: AppArmor defines what running processes can do and access. The allowed activities are stored in policy files.

Investigation: Is IPTables/FirewallD enabled on the system?

Observation: IPTables is disabled on both system

Guidance: Configure a firewall to filter incoming and outgoing traffic.

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: A daily backup should be generated which stores the email files including the mail data as well as the complete MySQL database. In addition, any system related configuration files should be backed up as well (e.g. Apache, MySQL, configuration)



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: Confirm that the last cover sheet was part of a maintenance. Unreported system outages can be caused by hardware issues or misconfigurations.

3.10.2. Disk space utilization

Investigation: Is there enough free space?

Observation: The system has enough free space left

Guidance: A full file system can cause severe performance issues as well as data corruption on database systems. Make sure there's appropriate monitoring in place

3.10.3. Disk I/O Performance

Investigation: Is the disk performance adequate?

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

Guidance: Install the sysstat package to collect meaningful information for the I/O and load averages.

3.10.4. NFS Performance

Investigation: Is the NFS performance adequate?

Observation: No 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: The I/O Wait time is within the normal range with 2.3 for the 15 minute average

Guidance: The system should operate in a normal load average value (1-3). Elevated load averages and high I/O wait times indicate an underlying problem



3.11. Cacti Settings

3.11.1. Cacti / Spine Version

Investigation: Is the current Cacti and Spine version installed?

Observation:

Guidance:

Check the current version of Cacti and Spine installed. Verify the version of the installed plugins. Check the version of the installed plugins. Check the version of the installed plugins. Check the version of the installed plugins.

3.11.2. Cacti Plugin Setup / Configuration

Investigation: Are current Plugins installed and configured?

Observation:

Guidance:

Check the current version of the installed plugins. Verify the version of the installed plugins. Check the version of the installed plugins. Check the version of the installed plugins.

3.11.3. Database Parameters

Investigation: Are the database parameters using the recommended settings?

Observation:

Guidance:

Check the current version of the database parameters. Verify the version of the database parameters. Check the version of the database parameters. Check the version of the database parameters.

3.11.4. RRD Storage Path I/O Performance

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

Observation:

Guidance:

Check the current version of the RRD storage path. Verify the version of the RRD storage path. Check the version of the RRD storage path. Check the version of the RRD storage path.

3.11.5. Poller Mode

Investigation: Is the correct poller being used?

Observation:



URBAN SOFTWARE

Dedicated to serve our customers

Guidance:

On the subject of the digital product, the company has made a significant contribution. It is a very good example of a company that is committed to its customers.

4. CONCLUSION / RECOMMENDATIONS

