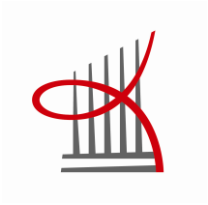


Developing Automatic System Monitoring Solution for Accanto Systems Customer Care

Markku Mikkola

Master's Thesis
April 2015
Information Technology

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Information Technology

AUTHOR 1: Markku Mikkola
Developing Automatic System Monitoring Solution for Accanto Systems Customer Care

Report 31 pages, appendices 68 pages
April 2015

The goal of the development work was to document the requirements, to develop and deploy an automatic system monitoring solution for Accanto Systems Customer Care. This final report describes Icinga Core as the backbone of the monitoring solution and presents the actual use case that was implemented for Accanto Systems.

The client for this work was Accanto Systems Customer Care department which had been suffering a long time with high work load due to increased basic system monitoring tasks and maintenance activities.

The result of this work consisted of several Icinga Core installations in order to monitor the Accanto key customer systems in real time. It included also Icinga alarm integration to the Accanto Systems Customer Care monitoring portal which was done as an in-house development work to create a unified view of all customers' problems.

Key words: Icinga, system monitoring, hosts, services

CONTENTS

GLOSSARY

API	An application programming interface
CentOS	Community Enterprise Operating System
COC	Customer Operations Center
CPU	Central processing unit
cr	credit
fork	Independent development of copied source code
GCC	GNU Compiler Collection
GPL	GNU General Public License
HTTP	Hypertext Transfer Protocol
iCSA	intelligent Customer Service Assurance
iCEM	intelligent Customer Experience Management
IDODB	Icinga Data Out Database
IDOUtils	Icinga Data Output Utils
NNTP	Network News Transfer Protocol
PING	Utility used to test the reachability of a host
POP3	Post Office Protocol version 3
REST	Representational State Transfer
RHEL	Redhat Enterprise Linux
SLA	Service-level agreement
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
TAMK	Tampere University of Applied Sciences
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
VPN	Virtual private network

1 INTRODUCTION

The purpose of this thesis is to evaluate and describe the key features of Icinga and its suitability for Accanto Systems Customer Care as the primary monitoring solution. Icinga is an open source monitoring system software which can be used to monitor networks and any network resources, hosts or services. Other considered and tested monitoring system software's were Nagios and Shinken but ultimately Icinga was selected as it was already well known inside the company and the most compliant with the company requirements.

The report shall focus on the 1.x branch architecture of Icinga which is a "fork" of the well-known monitoring system Nagios. There exists also new parallel development branch of Icinga 2 however that is not in the scope of this thesis because the development of Icinga 2 is still in early stage and Icinga 1.x branch was considered more stable and reliable choice for the core software of the Accanto Systems Customer Care monitoring solution and was chosen by Accanto Systems product management.

This report also aims to identify the requirements and uses cases for Accanto Systems automatic system monitoring solution and to describe the final solution and its benefits and challenges from the Customer Care engineers' perspective. One of the key objective of this solution is to reduce the time spend on basic system maintenance and monitoring tasks which is now done manually by the 1st line customer care engineers. The target is also free resources from support activities to solution delivery projects.

2 BACKGROUND

Few years ago after the organisational changes there was a need to enhance and optimize the daily customer support activities and monitoring tasks due to increased workload on the customer care department. The complex nature of the Accanto Systems supported systems and solutions created a growing need to automate the basic system monitoring activities. These "basic" tasks were taking too much time and resources when executed manually for all the supported customer systems.

For this specific problem Icinga was introduced as a pilot system monitoring solution for one customer only. After this it has been internally developed and "packaged" to be a part of every system deployment and solution that is delivered to the customer and having a support agreement.

2.1. About Accanto Systems Oy

> Accanto Systems provides Customer Experience Management (CEM) and Network Analytics solutions to Service Providers. By analyzing network performance and customer satisfaction, Accanto's iCEM platform calculates the QoE (Quality of Experience) of all customers, identifying the business impact of the revenues that are lost, and costs that are gained through poor service. Accanto then provides recommendations to improve the QoE in order to achieve an optimized ROI for each customer segment. Headquartered in Lahti, Finland, Accanto Systems has 180 customers worldwide. (Accanto Systems Overview. 2015)

2.2. Accanto Systems Customer Care

Accanto Systems has 180 customers world-wide and main customers are telecom operators. Accanto Systems Customer Care provides 1st line support for iCSA and iCEM solutions including its strategic partner Netscout network probe systems.

Accanto Systems customer care department currently operates with four 1st line support engineers who handle all the customer trouble tickets as well as the daily monitoring and maintenance tasks.

3 ICINGA OVERWIEV

As mentioned in the introduction Icinga is an open source monitoring solution which can be used for automated system checks for specified hosts and services as required. It has a simple plugin design which allows users to develop and integrate their own service checks easily and flexible way. Also as being a “fork” of the Nagios monitoring system and backward compatible with it all Nagios configurations, plugins and add-ons can be also used with Icinga.

Currently Accanto Systems Customer Care uses Icinga Core to monitor all its customer systems which are under maintenance agreement. It is used to monitor Accanto Systems intelligent Customer Service Assurance (iCSA) and intelligent Customer Experience Management (iCEM) solutions as well as NetScout network probe systems. The Icinga deployment and development work is still ongoing but currently it includes over 15 Icinga Core instances which are monitoring over ~150 Linux and Windows hosts and over ~2000 system services.

The monitored system services varies from different Linux and Windows processes to data flow monitoring, hardware health checks and database service checks. More detailed descriptions of the monitored systems and the services are available later on this document.

3.1. Icinga features

Icinga has many features but in system monitoring point of view the most important are the capability to monitor and alert the status of network services (like PING, HTTP, SMTP, POP etc.) and host critical resources and processes (memory/CPU/disk usage etc.). The main Icinga features are described below:

- Simple plugin design that allows users to easily develop their own service checks
- Parallelized service checks
- Ability to define network host hierarchy using "parent" hosts, allowing detection of and distinction between hosts that are down and those that are unreachable

- Contact notifications when service or host problems occur and get resolved (via email, pager, or user-defined method)
- Ability to define event handlers to be run during service or host events for proactive problem resolution
- Automatic log file rotation
- Support for implementing redundant monitoring hosts
- Optional classic web interface for viewing current network status, notification and problem history, log file, etc.
- Optional new Icinga web interface based on Icinga Core, IDOUtils, API using a modern and refreshed web 2.0 GUI showing current states, historical information, using cronks and filters, creating reports with multilanguage support (About Icinga. 2014.)

3.2. System requirements and licensing

Icinga runs on multiple Linux or UNIX based variants. These include Linux distributions like Fedora, Ubuntu, openSuSe and Redhat as well as several UNIX platforms like Solaris and HP-UX. In case there is no precompiled version of Icinga that is required by your Linux or UNIX distribution it can be compiled from source using a C compiler like GCC. The systems that Icinga monitors can be nearly anything that is connected to the network. (About Icinga. 2014.).

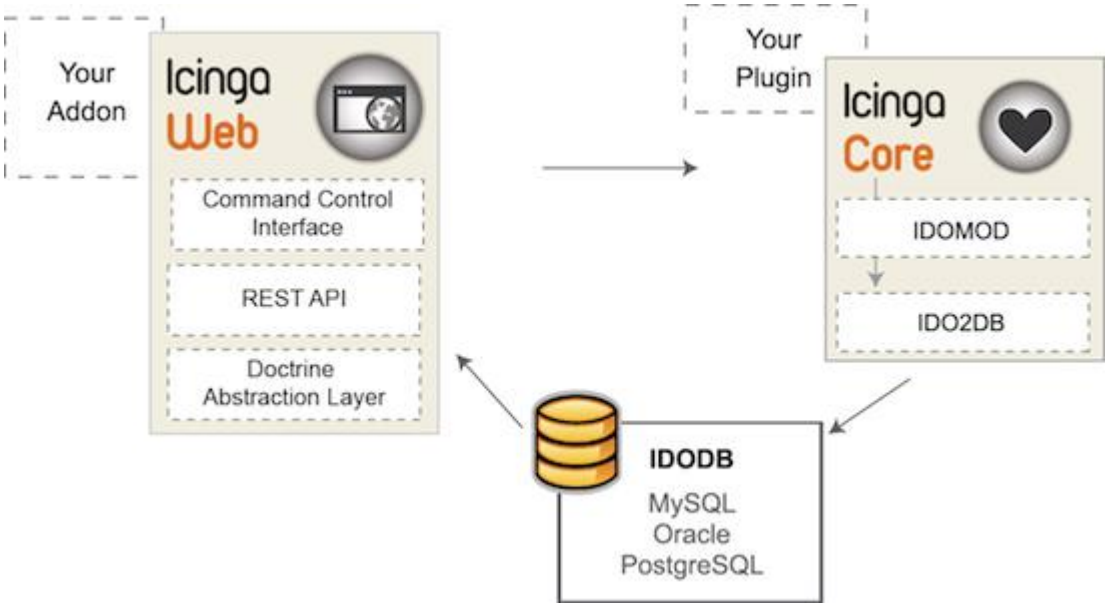
Icinga Core server network interface need to be configured as most of the Icinga checks will require a network access. Also Icinga Web interface requires following additional software:

1. Web Server (Apache preferred)
2. GD Graphics Library version 1.6.3 or higher
3. PHP

Icinga is licensed under the GNU General Public License Version 2. This means that it is 100% free and open source software which can be distributed and modified under the terms described in the license. More detailed information about the GNU General Public License and terms can be found at http://www.gnu.org/licenses/gpl-2.0.html.

3.3. Icinga architecture and components

Icinga consists of 3 separate components: Icinga Core, Icinga Web and Icinga Data Out Database (IDODB). Picture 1 presents the overall Icinga architecture together with the main components and modules.



Picture 1 Icinga Architecture (https://www.icinga.org)

3.4. Icinga Core

Icinga Core component manages the monitoring tasks and collects the system health information generated by the various plugins and passes it via the IDOMOD interface and IDO2DB service daemon over SSL encrypted TCP sockets to the Icinga IDODB. Icinga Core can also operate without IDODB by storing the information in flat files.

3.4.1 IDOUtils

Icinga IDOUtils comes packaged with Icinga Core and it includes both IDOMOD interface / Event Broker Module and IDO2DB service daemon. It is designed to store all configuration and event data from Icinga Core to database. IDOUtils are needed in case Icinga is to be used with database or the new Icinga Web interface is planned to be used. Icinga can be deployed with or without IDOUtils when there is no database involved

and in that case all information is stored in flat files. Currently IDOUtils supports MySQL, PostgreSQL and Oracle databases.

IDOMOD event broker module has been designed to export configuration and runtime event data from the Icinga daemon.

LOG2IDO component has been designed to import historical Icinga log files into a database via IDO2DB daemon.

FILE2SOCK component reads input from a standard file and writes it to UNIX domain or TCP socket.

IDO2DB component has been designed to take the output data from the IDOMOD and LOG2IDO components and store it to database.

3.4.2 Classic Web

Icinga Classic Web interface comes together with the Icinga Core and has a traditional look and feel with single window format like in Nagios. The monitored host and service status, history, notifications and status maps are included in the Classic Web interface. It is available at http://localhost/icinga/ or http://yourdomain.com/icinga after the initial installation.

3.5. Icinga New Web

As stated earlier, Icinga offers two web interfaces for users to view the monitoring results and send commands to the Icinga Core. New Icinga Web interface consists of three component layers:

1. Doctrine Abstraction Layer
2. REST API
3. Command Control Interface

3.5.1 Command Control Interface

Icinga Web uses Command Control Interface to communicate with Icinga Core. It performs commands made in Icinga Web by executing binaries and writing to pipe.

3.5.2 REST API

Icinga-web REST API allows querying monitoring information via GET or POST requests. REST API fetches standard HTTP status queries and returns the data in JSON or XML formats.

Currently supported Icinga Web REST API features are listed below:

- Availability of almost all monitoring fields via GET or POST.
- Return data as xml or json
- AND & OR Search filter groups with unlimited nesting levels (AND(OR(AND()))
- You choose which columns you want returned, not the API (less overhead)
- Support of limit, offset, order, group by
- Return an additional total count field
- Authorization via auth_key in request or cookies
- Respects Icinga-web principals (for example, limit to specific host groups)
- Since Icinga v1.6: Retrieve detailed SLA information or enhance a request with SLA information (Icinga-Web REST API. 2012.)

Icinga REST API can be used e.g. by external software like some mobile phone application.

3.5.3 Doctrine Abstraction Layer

Icinga Web's Doctrine Abstraction Layer retrieves the monitoring information from database and provides Doctrine Query Language (DQL) views. These templates/models can be used to develop own "cronk" modules to collect data from external databases and systems. These models also contain all fields and their relations to each other available by ido2db.

3.6. IDODB

Icinga IDODB is the storage for the historical monitoring data and also Icinga web uses it for access. Icinga IDODB supports MySQL, PostgreSQL and Oracle databases.

4 AUTOMATIC MONITORING SOLUTION FOR ACCANTO SYSTEMS CUSTOMER CARE

4.1. Solution requirements

Detailed requirements for Accanto Systems automatic monitoring solution are documented in Appendix 1: Requirement documentation for Accanto Systems automatic system monitoring solution. Requirement documentation is based on Volere Requirements Specification template.

4.2. Solution use cases

Identified use cases for Accanto Systems automatic monitoring solution are documented in Appendix 1: Requirement documentation for Accanto Systems automatic system monitoring solution.

4.3. Monitored systems

Monitored customer deployments consist of Accanto iCSA and/or iCEM systems which both can be integrated with NetScout Pantera network probe systems or with some other network probe vendor. Therefor it is required to have dedicated service checks for all the systems to ensure the end-to-end customer solution usability and health.

Accanto Systems iCSA and iCEM solutions are described below.

iCSA - intelligent Customer Service Assurance

Accanto Systems' intelligent Customer Service Assurance (iCSA) is the latest in Customer Service Assurance solutions, designed to enable service providers to migrate to superior network, service and customer assurance practices in a seamless and cost-effective manner. Accanto Systems' iCSA solution combines a modular and scalable hardware and software architecture with a broad set of problem solving capabilities which makes it the right customer service assurance and monitoring solution for today and tomorrow. The extensive application suite provided by iCSA helps service providers to manage a massive

amount of data and turn it into meaningful information that can be used to make better and faster decisions. Accanto iCSA solution provides data source agnostic solution for Customer Service Assurance. iCSA Application functionality is not dependent on any specific data source but has a flexible way to integrate and model information from various sources to be utilized by iCSA applications. (Accanto Systems iCSA Product Description Release 5.1 Version 1.1. 2012.)

iCEM - intelligent Customer Experience Management

Accanto iCEM is a unique platform which uses customer-centric and network-centric data to enable Quality of Experience (QoE) monitoring and analytics for each individual subscriber. Using a sophisticated analytical algorithm, iCEM processes network and customer data to provide business value to service providers by identifying and prioritizing network problems to ensure the least disruption to customer experience and Operator revenues. Accanto iCEM provides the operator with the ultimate toolkit and iCEM's flexible metadata driven architecture collects and correlates inputs from a wide array of sources, including probes, OSS, CRM and others. Quality of Experience (QoE) calculations performed for each service and individual subscriber, together with multi-dimensional analysis capabilities, provide deep insights into customer behavior, preferences, location and experience, far surpassing the capabilities of traditional monitoring systems. Combined with its power and flexibility in reporting, alarming and analysis, iCEM provides value to business and technical operations. (Accanto Systems iCEM Overview. 2014.)

NetScout Pantera network probe system is described below.

Pantera - All-in-one Probe and Protocol Analyzer Family

Today's converged telecom market calls for new solutions that can simultaneously troubleshoot and monitor Mobile, High-speed IP and Legacy traffic. Pantera, a vital component of Accanto's adaptive CSA solution, is a real-time all-in-one probe and protocol analyzer family designed to meet the complex needs of operators trying to migrate to high-performance, converged IP networks. Pantera builds on the success of Accanto's acclaimed 3GMaster and NeTracker families, improving on several important elements and making it ideal for mixed-technology environments:

- A more flexible GUI that allows test setup of virtually unlimited protocol/interface combinations
- Improved IP filtering capabilities for core networks
- Modular software capable of leveraging multi-core and advanced processor technologies
- Much more powerful hardware for fast, in-depth analysis and xDR generation

With all-over-IP convergence, the distinction between legacy and NGN is blurring. Now, it is not uncommon to see operator networks composed of a wide

variety of mobile, NGN, and legacy protocols, nodes and interfaces. Pantera's IP analysis capabilities, coupled with its ability to support both wireless and wireline network domains, makes it a standout in terms of value and flexibility. As a probe, Pantera has the ability to collect inputs from a wide array of sources to create true customer-aware xDRs for input into the monitoring system. As an analyzer, Pantera allows fast correlation and drill down to the frame level to give the operator exactly the information they need to resolve complicated issues. (Netscout Pantera Data Sheet. 2014.)

4.4. Monitored services and objects

Common service and object checks for Accanto legacy iCSA and for the iCEM systems are described below. All system checks described below are configurable and have specific thresholds limits to identify the service statuses. The service statuses can be critical, warning, ok or unknown.

1. NRPE Version
    - This checks and shows the version of the NRPE agent running on the remote monitored host.

2. CPU Load
    - This checks and shows the server CPU load averages over the last minute, the last 5 minutes and the last 15 minutes.

3. Root partition
    - This checks and shows the free space (in MB and %) of the Linux root "/" partition.

4. Disk Partition
    - This checks and shows the free space (in MB and %) of the configured Linux file system partitions.

5. Zombie Processes
    - This checks and shows number of Zombie processes in the system.

6. Swap Usage
    - This checks and shows the free swap space (in MB and %) of the system.

Specific monitored services and objects descriptions for Accanto iCSA system are listed below:

1. SDF Loader Queue
    - This checks and shows the number of files in the Oracle loader input directory e.g. /home/oracle/cdr

2. SDF Correlator Queue
    - This checks and shows the number of files in DCS_Correlator input directory e.g. /opt/srti/DataCollector/data

3. iCSA Log
    - This checks and shows the amount of error and warning messages from the iCSA web server content log.

4. Oracle Database
    - This checks and shows the Oracle database “tnsping” response time.

5. Oracle Database CDRPROT Tablespace
    - This checks and shows the usage percentage of the “CDRPROT” table space.

6. Oracle Database TREND Tablespace
    - This checks and shows the usage percentage of the “TREND” table space.

7. Oracle Database DCS Tablespace
    - This checks and shows the usage percentage of the “DCS” table space.

8. Oracle Database ALARM Tablespace
    - This checks and shows the usage percentage of the “ALARM” table space.

9. Oracle DB Processes
    - This checks and shows the number of Oracle database Linux processes.

10. Tomcat
    - This checks and shows the status of the Tomcat Web server Linux process.

11. Oracle BI
    - This checks and shows the status of the Oracle BI server Linux process.

12. DCS_Admin
    - This checks and shows the status of the DCS_Admin Linux process.

13. DataCollector
    - This checks and shows the status of the DataCollector Linux process.

14. DCS_Correlator
    - This checks and shows the status of the DCS_Correlator Linux process.

15. DCS_Proxy
    - This checks and shows the status of the DCS_Proxy Linux process.

16. FileMover
    - This checks and shows the status of the FileMover Linux process.

17. NamingService
    - This checks and shows the status of the NamingService Linux process.

18. BI Scheduler
    - This checks and shows the status of the Oracle BI Scheduler Linux process.

19. RAID check
    - This checks and shows the status of the HP Smart Array Controller(s).

20. HP Hardware Status
    - This checks and shows the system hardware model, serial number and health status.

21. Max Partition
    - This checks and shows the max date of all the protocol table partitions.

22. SDF Received
    - This checks and shows the delay of SDF generation on the integrated data sources.

23. CDR Load Count
    - This checks and shows the sum of loaded CDR rows over all protocols.

Specific monitored services and objects descriptions for Accanto iCEM system are listed below:

1. EngineAdapter
    - This checks and shows the status of the EngineAdapter Linux process.

2. EngineLoader
    - This checks and shows the status of the EngineLoader Linux process.

3. QueryTool General Log
    - This checks and shows the amount of error and warning messages from the general iCEM QueryTool log.
    -

4. QueryTool Error Log
    - This checks and shows the amount of error and warning messages from the iCEM QueryTool Error log.

5. VectorWise
    - This checks and shows the status of the Vectorwise VW DBMS server and recovery server Linux processes.

6. VectorWise Uptime
    - This checks and shows the VectorWice database instance uptime.

7. VectorWise Sessions
    - This checks and shows the number of VectorWice open database sessions.

8. Protocol Table Partitions
    - This checks and shows the max date of all the protocol table partitions.

9. SSD Writes
    - This checks and shows the amount of successful writes on the SSD disk.

10. Disk Partition
    - This checks and shows the free space (in MB and %) of the configured Linux file system partitions.

11. NS_PT_*protocol_name* Load Queue [camel]
    - This checks and shows the number of files in EngineAdapter service input directory for each protocol.

12. NS_PT_*protocol_name* Load Queue [db]
    - This checks and shows the number of files in EngineLoader service input directory for each protocol.

13. NS_PT_*protocol_name* Loaded
    - This checks and shows the number of rows loaded for each protocol.
    -

14. NS_PT_*protocol_name* Rejected [db]
    - This checks and shows the number of rejected rows by the database during loading process.

15. NS_PT_*protocol_name* Rejected [folder]
    - This checks and shows the size of the “rejected files” folder.

16. NS_PT_*protocol_name* Group Calculations for All
    - This checks and shows the percentage of groups for which KPI's are calculated.

17. Source Content Delay NS_PT_*protocol_name*
    - This checks and shows the source content delay for each integrated data source.

Monitored services for Netscout network probe system are listed below:

1. NSClient++ Version
    - This checks and shows the version of the NSClient agent running on the remote monitored host.

2. Uptime
    - This checks and shows the server uptime.

3. CPU Load
    - This checks and shows the server CPU load average for last 5 minutes.

4. Memory Usage
    - This checks and shows the server memory capacity and usage (total, used and free percentages).

5. C:\ Drive Space
    - This checks and shows the system C:\ drive capacity and usage percentages (total, used and free).

6. D:\ Drive Space
    - This checks and shows the system D:\ drive capacity and usage percentages (total, used and free).

7. Explorer
    - This checks and shows the status of system Windows Explorer process.

8. APE service
    - This checks and shows the status of the Application Protocol Engine process.

9. FileZilla Server
    - This checks and shows the status of the FileZilla server process.

10. RAID
    - This checks and shows the status of the system storage RAID controller.

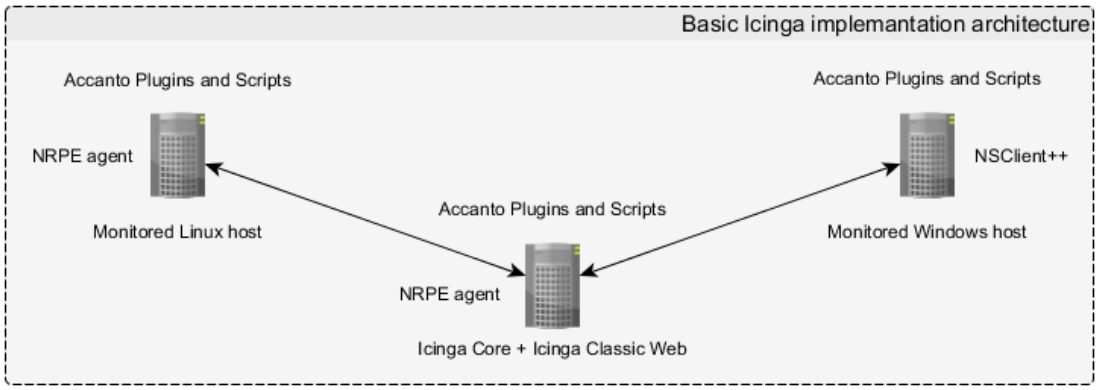
4.5. Customer backend setup for system monitoring

Accanto Systems has chosen to use Icinga Core version 1.7.2 and Icinga Classic Web as the backend for customer system monitoring software. This provides all required functionality to monitor all critical services and hosts on the customer network and capability to export required monitoring information to the Accanto Systems Customer Care monitoring portal.

4.5.1 Customer Icinga Core setup

Icinga is deployed on Redhat Enterprise Linux (RHEL) 4 or RHEL 6 server which is also hosting the Accanto iCSA or iCEM web services. There is no need to have a dedicated Icinga Core server as it has been proven to work together with the iCSA or iCEM web server. Also the cost of a new dedicated hardware for Icinga Core server is too high in this stage when it is not a real “sales item” in Accanto’s product portfolio.

All customer Icinga setups are deployed without IDOUtils and IDO database. All monitoring data is stored on “flat files” and saved on local file system. The basic setup consists of Icinga Core with Classic UI and required monitoring agents NRPE and NSClient++. Addition to that all required Accanto specific service plugins and scripts are integrated with the Icinga Core setup. Picture 2 below presents the basic Icinga implementation architecture:



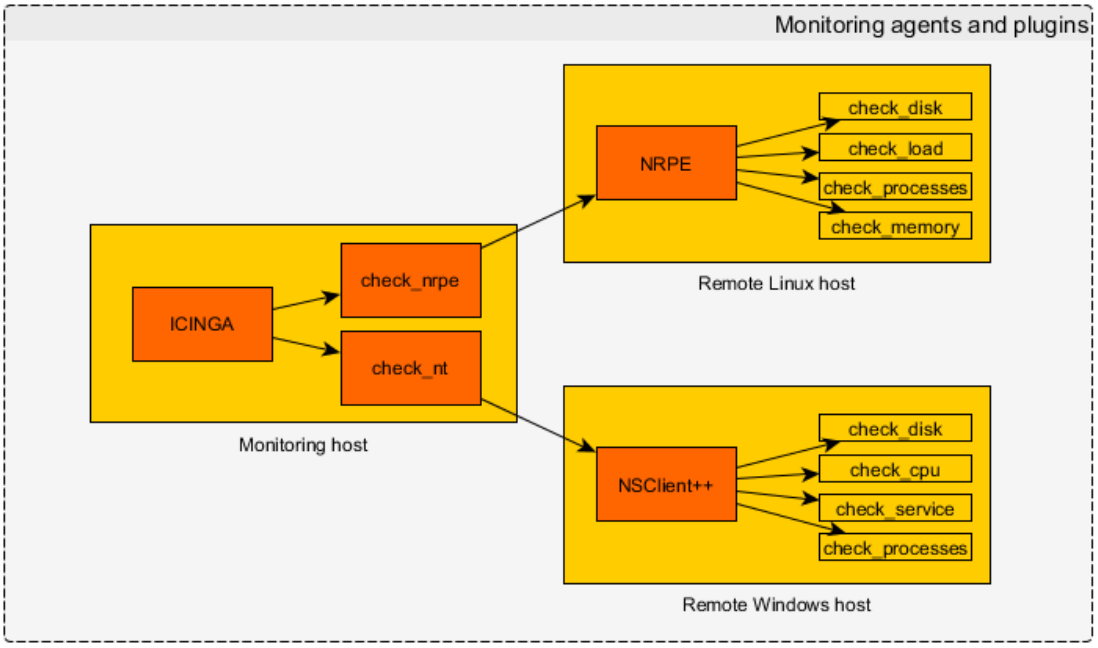
Picture 2 Icinga implementation architecture

The Icinga Classic Web interface provides an easy-to-use GUI for customer local System Administrator to monitor their iCSA, iCEM and Probe systems and report any issues to Accanto Systems global support. It is also used by the Accanto support engineers to get a quick glance of the customers' systems health when investigating some customer reported issue on the system.

4.5.2 Monitoring Agents and plugins

The customer Icinga setup utilizes monitoring agents NRPE and NSClient++, which are installed on the monitored remote hosts. The Icinga Core server is getting all service check results via these add-on agents. These remote monitoring add-ons allows the monitoring host (Icinga server) to request commands, plugins or scripts to be executed on the remote monitored server and send back the check results to monitoring host. In Accanto customer Icinga setup NRPE agents are deployed on the iCSA and iCEM servers which are running upon RHEL operating system. In case of Netscout probe systems the NSClient++ is used to collect and execute the checks on Windows OS based network probes.

Below picture 3 presents the used add-ons NRPE and NSClient++ together with the required plugins check_nrpe and check_nt.



Picture 3 Monitoring agents and plugins

On monitoring host, the Icinga process will control the check_nrpe and check_nt plugins to check configured services or resources on remote monitored host. The plugins connects to the appropriate agent on monitored hosts which executes the checks and passes the results back to the Icinga via the plugins.

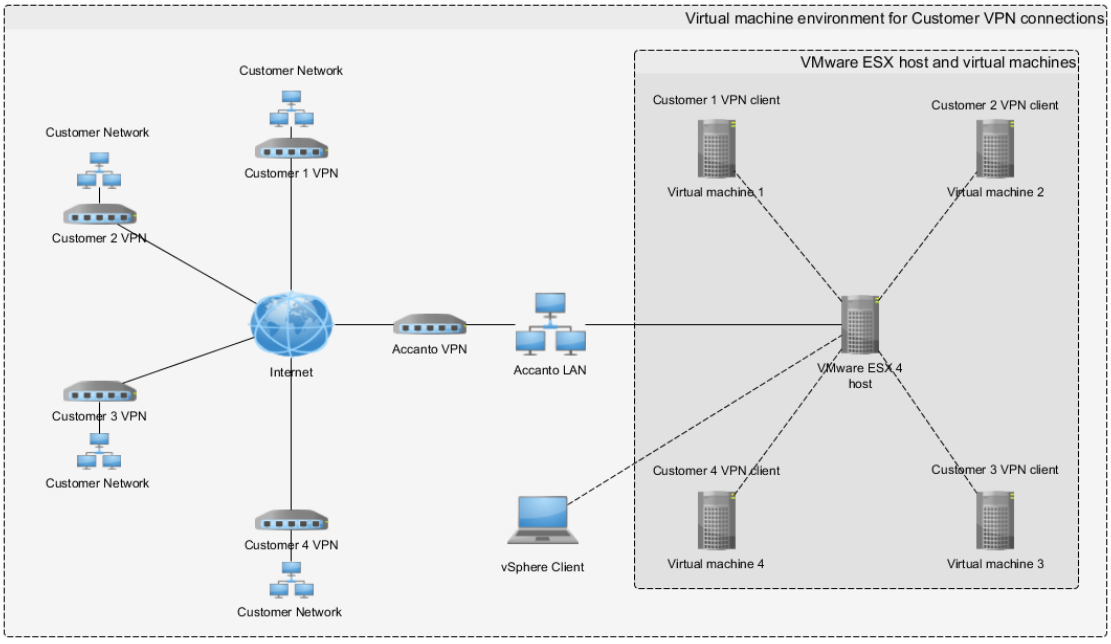
4.6. Frontend setup for Accanto Customer Care

The customer Icinga frontend setup requires a shell script that generates the “Service Problems” as a HTML file on the Icinga Core server and stores it locally on the file system. The shell script is scheduled as a linux cronjob to be executed on specific time intervals. The “Service Problems” HTML file includes all the Critical, Warning and Unknown service alerts from the customer systems. This “alerts” file is then downloaded from customer system to Accanto Systems monitoring portal server through VPN tunnel via customer specific virtual machine. From this file all required information is finally parsed in to the unified view of all customer systems alerts.

4.6.1 Customer specific VPN tunnels and virtual machine setup

Each remote connection to customer network and systems requires a secure VPN connection. VPN procedures varies a lot between the different customer connection but the common and problematic thing is that creating a VPN connection usually disables the local network interface on the VPN client machine where the VPN client is installed and running. Therefore it is required to install VPN clients to each customer specific virtual machines. This way the customer specific virtual machines still remain connectable via the console from VMware ESX host server even if the virtual machines main network interfaces are “disabled” by the VPN client.

Below picture 4 presents an example virtual machine setup for customers VPN connections.



Picture 4 VMware virtual machine setup

4.6.2 Virtual machines with clustered file system

All virtual machines are hosted on VMware ESX Hypervisor which also provides a shared virtual storage disk for all virtual machines in the cluster. This shared disk is used as a common storage for all customers Icinga monitoring data and alarms. These stored alarms are then forwarded to the Accanto Systems monitoring portal.

The virtual machines are running upon CentOS 6.5 operating systems with Red Hat cluster suite software and global file system (GFS2) add-on. Cluster software is used to provide clustered shared storage to all nodes in the cluster. This allows all nodes in the cluster to access the shared disk simultaneously.

Below are listed the used software for clustered file system:

- gfs2-utils
- lvm2-cluster
- cman
- modcluster
- rgmanager
- openais

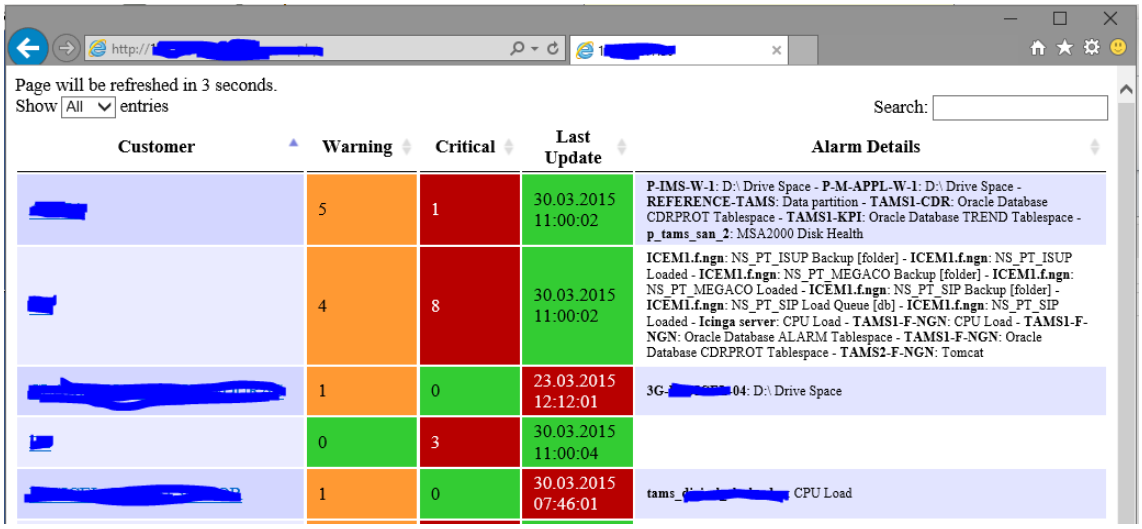
On the VMware virtual machine setup it is also required to disable the simultaneous write protection by specifying the “multi-writer” flag on each virtual machine configuration file, e.g. “virtual_machine1.vmx” file which defines the virtual machine. Below are the added configuration properties:

```
scsi1:0.sharing = "multi-writer"
disk.locking = "false"
```

More information about the enabling or disabling simultaneous write protection can be found on VMware knowledge base article KB: 1034165.

4.6.3 Accanto Systems monitoring portal

Accanto Systems monitoring portal is an in-house development work that was created as part of this monitoring solution for Accanto Systems. Its purpose is to provide unified and simple view of the entire key customer’s systems health to Customer Care support engineers. Below picture 5 presents the sample view of Accanto Systems monitoring portal from which support engineers can quickly review all the customer system statuses.

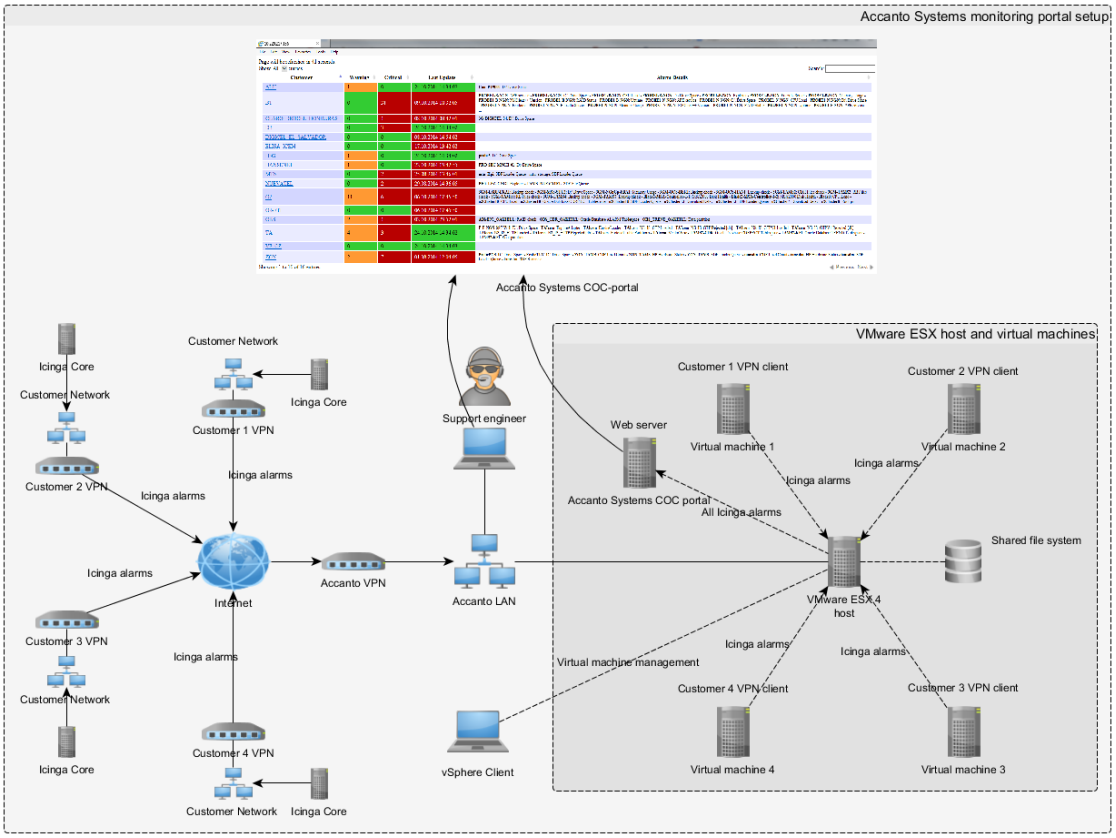


Page will be refreshed in 3 seconds.
Show All entries
Search:

Customer	Warning	Critical	Last Update	Alarm Details
[redacted]	5	1	30.03.2015 11:00:02	**P-IMS-W-1**: D:\ Drive Space - **P-M-APPL-W-1**: D:\ Drive Space - **REFERENCE-TAMS**: Data partition - **TAMS1-CDR**: Oracle Database CDRPROT Tablespace - **TAMS1-KPI**: Oracle Database TREND Tablespace - **p_tams_san_2**: MSA2000 Disk Health
[redacted]	4	8	30.03.2015 11:00:02	**ICEM1.f.ngn**: NS_PT_ISUP Backup [folder] - **ICEM1.f.ngn**: NS_PT_ISUP Loaded - **ICEM1.f.ngn**: NS_PT_MEGACO Backup [folder] - **ICEM1.f.ngn**: NS_PT_MEGACO Loaded - **ICEM1.f.ngn**: NS_PT_SIP Backup [folder] - **ICEM1.f.ngn**: NS_PT_SIP Load Queue [db] - **ICEM1.f.ngn**: NS_PT_SIP Loaded - **Icinga server**: CPU Load - **TAMS1-F-NGN**: CPU Load - **TAMS1-F-NGN**: Oracle Database ALARM Tablespace - **TAMS1-F-NGN**: Oracle Database CDRPROT Tablespace - **TAMS2-F-NGN**: Tomcat
[redacted]	1	0	23.03.2015 12:12:01	**3G-[redacted]04**: D:\ Drive Space
[redacted]	0	3	30.03.2015 11:00:04	
[redacted]	1	0	30.03.2015 07:46:01	**tams_[redacted]** CPU Load

Picture 5 Accanto Systems Monitoring Portal

Detailed requirements of the COC portal are included in Appendix 1. Picture 6 below presents the complete front-end setup for customer care monitoring portal.



Picture 6 Customer Care monitoring portal setup

4.7. Improvement ideas

There is a natural improvement ongoing constantly as new system checks are identified through the system problems all the time. Current solution is intended for Customer Care use but new use cases for Sales department have been identified. These uses cases for Sales could be for example to monitor the customer system capacity and estimate the current and future load in order to "push" sales of the new system installations and upgrades for the customer.

4.8. Benefits

Icinga allows the Accanto Customer Care to proactively identify problems in customer iCSA, iCEM and Probe systems before they become a severe issue. For example if a disk has failed on the server and the disk controller RAID setup is not fault tolerant anymore, Icinga will raise an alarm and send notification to Accanto Customer Care monitoring portal. This enables the 1st line support engineer to make any necessary actions to get the failed disk replaced before the disk RAID fails and data is permanently lost.

Other major benefit is that this kind of automatic system monitoring saves a lot of time and resources compared to manual system health checks. It also enables support engineer to acknowledge the service problems and plan for maintenance tasks. This also helps to identify new issue from old ones that are already acknowledged and taken care of.

In the future Accanto automatic monitoring solution could become a real sales item or extension to the existing Accanto Systems support services.

4.9. Challenges

One of the challenges at the beginning was to get all customers systems monitoring data and alerts into one place where it could be analysed and presented in a unified and simple format. There were few open source free web interfaces on the market that were tested for this purpose but those were found too "complex" or just not fit for our needs

and environment due to the limitation that multiple VPN connections creates for customer connections. Because of these problems and limitations the Accanto monitoring portal, the "COC-portal" was created as in-house development work. It is not pretty but it provides all required functionality and it is clear and simple view of all the alarms in customer systems.

Also one challenge in the beginning of the development work was that there were no "real" support for Icinga usage and configuration available except of Icinga Communities and Google. Of course there are some companies that provide Icinga consulting services but there were no budget for that kind of services to be used.
Currently the main challenge is to maintain the customer specific VPN tunnels as these connections are often "cut off" from time to time by the VPN server or the security tokens needs to be manually renewed in order to maintain the connection active.

4.10. Other Icinga use cases

Other Icinga users and use cases are presented on official Icinga web page at Icinga in action. Below are presented some large companies and organizations that use Icinga:

Picture 7 Icinga users (https://www.icinga.org/users/)

5 CONCLUSION

Nowadays the different kind of IT systems requires a highly complex system environments and solutions in order to provide the services to the consumers and profit for the service providers. The large scale and complexity of the current IT systems creates a new kind of challenge to maintain them and to provide a first class support services.

This challenge has been faced also in Accanto Systems were growing customer base is putting pressure on the service delivery projects and to the maintenance activities as the work load has increased rapidly. In order to manage the growing work load and to guarantee the quality support for all customers Accanto has chosen Icinga monitoring software to manage basic systems monitoring activities automatically and in real-time. Addition to Icinga monitoring the Accanto monitoring portal was developed to unify all customers Icinga alerts into one place in which support engineers can proactively monitor all system statuses.

This automatic monitoring solution has been in active use for several months now and it has proven to be very valuable and time consuming help for Accanto Systems customer care department. In best cases the Customer Care can identify and fix the customer issues even before those are noticed by the customers themselves.

This solution has now been included in all new system deliveries as a basic integration task and it has become a required milestone in handover process from delivery to maintenance. It is still worth to realize that Icinga itself won’t fix any problems, it just helps to notice them on time so that the engineers can take necessary actions to fix them.

REFERENCES

Accanto Systems Overview. 2014. LinkedIn. Read 13.11.2014. http://www.linkedin.com/company/accanto-systems?trk=company_name

About Icinga. 2014. Read 10.12.2014. http://docs.icinga.org/latest/en/about.html

Icinga-Web REST API. 2012. Read 13.11.2014. https://wiki.icinga.org/display/Dev/Icinga-Web+REST+API

Accanto Systems, iCSA Product Description Release 5.1 Version 1.1. Jul 2012. Read 19.12.2014. s.6.

Accanto Systems iCEM Overview. 2014. Read 10.12.2014. http://www.accantosystems.com/web/index.php?id=79

Netscout Pantera Data Sheet. 2014. Read 10.12.2014. http://www.syrus.ru/files/pdf/PanteraDatasheetV3-Jan10.pdf

APPENDICES

Appendix 1. Requirements documentation for Accanto Systems automatic monitoring solution

1 THE PURPOSE OF THE PROJECT

1.1. The User Business or Background of the Project Effort

The purpose of this project is to reduce the time spend on Accanto Systems customer care 1st level support on basic system maintenance tasks which is now done manually to obtain the system operation and health. The purpose is also to free resources for Accanto Systems professional services department. This project will produce a new product for Accanto Systems Customer Care department for proactive and automated system health monitoring purposes.

1.2. Goals of the Project

Purpose:
We want to free resources to other/professional services activities and reduce the number of registered product trouble tickets as well as the 1st line engineer time spend on solving the issues related on basic maintenance tasks.

Advantage:
To have more resources available for professional services delivery projects and to gain new revenue.

Measure:
20% reduce of registered customer trouble tickets.
5% increase of new revenue within 1 year of product release.

2 STAKEHOLDERS

2.1. The Client

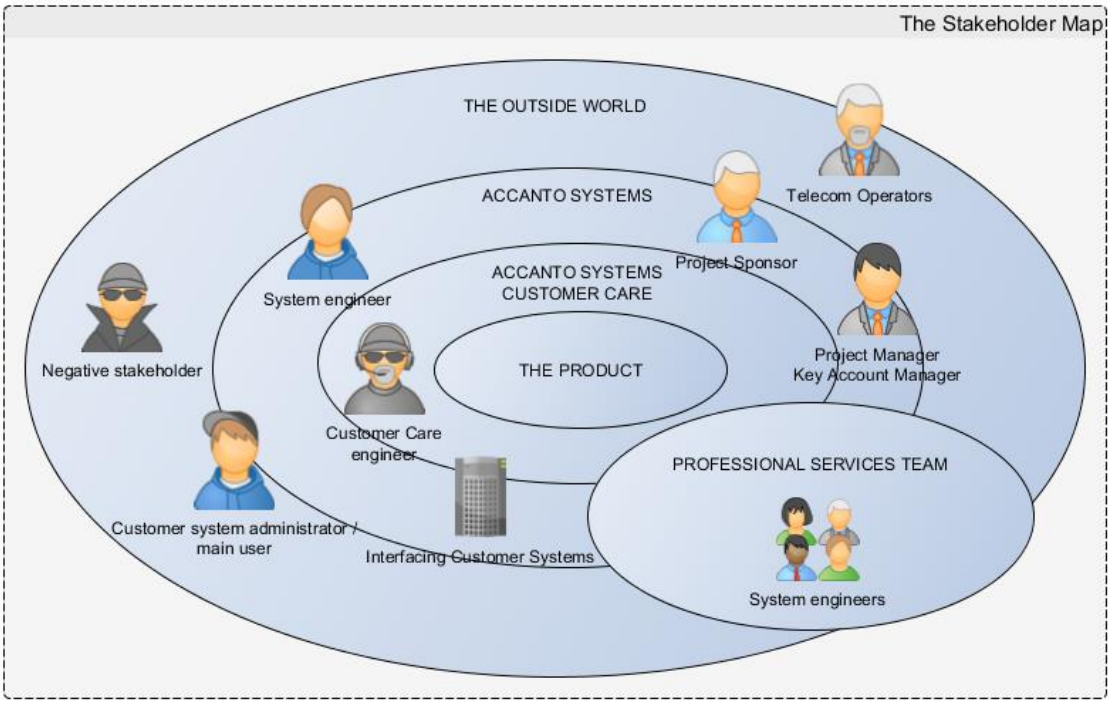
The client and the product sponsor is Accanto Systems Professional Services VP Ismo Nurmi.

2.2. The Customer

The customer of this in-house development work is Accanto Systems Professional Services VP Ismo Nurmi.

2.3. Other Stakeholders

The product stakeholder map is presented in picture1.



Picture 1 Stakeholder map

2.4. The Hands-On Users of the Product

User Categories:

- Customer Care engineers
- Profession Services engineers
- Technical Lead engineers
- Customer Care Managers
- Project Managers
- R&D engineers
- Key Account Managers

2.5. Personas

-

2.6. Priorities Assigned to Users

User Categories:

- Key users: Customer Care engineers and Professional Services engineers
- Secondary users: Customer Care Managers, Project Managers, Key Account Managers, Technical Lead engineers and R&D engineers
- Unimportant users: N/A

2.7. User Participation

Following user categories have important role to contribute knowledge of their area of expertise in this project.

User Categories:

- Key users: Customer Care engineers, Professional Services engineers and R&D engineers

Customer Care engineers have the best experience of the system problems that often triggers customer trouble tickets. Professional Services and R&D engineers are expected to provide a complete list of critical system services and objects that needs to be monitored.

2.8. Maintenance Users and Service Technicians

The product maintenance activities shall be in responsibility of following user categories.

User Categories:

- Professional Services engineers
- Customer Care engineers

3 MANDATED CONSTRAINTS

3.1. Solution Constraints

Description: The product shall run upon Red Hat Enterprise Linux Server 6.4 64-bit operating system.
Rationale: This is the chosen OS by the product line management.
Fit criterion: The product shall be approved for RHEL 6.4 compliance by product design unit testing group.

Description: The product shall run upon Red Hat Enterprise Linux Server 4.9 64-bit operating system.
Rationale: This is the chosen OS by the product line management.
Fit criterion: The product shall be approved for RHEL 4.9 compliance by product design unit testing group.

Description: The server hardware shall be HP Proliant DL380 G7.
Rationale: This is the selected server hardware by the product line management.
Fit criterion: The product shall be approved for HP server hardware compliance by product design unit testing group.

Description: The server shall run on x86 processor architecture.
Rationale: The server hardware uses x86 architecture.
Fit criterion: The product shall be approved for x86 compliance.

Description: The Icinga Core server shall run on same hardware than the product web server.
Rationale: This is the selected server hardware by the product line management.
Fit criterion: The product shall be approved for HP server hardware compliance by product design unit testing group

Description: The Icinga monitoring software shall be installed on iCSA or iCEM web server.
Rationale: This is the selected option by the product line management.

Fit criterion: The Icinga software shall be approved for iCSA / iCEM web server compliance by product design unit testing group.

Description: Each Customer shall have dedicated virtual machine for remote VPN connection.
Rationale: This is required due to VPN connection restrictions.
Fit criterion: VPN clients shall be tested for Virtual CentOS 6.5 compliance by Professional Services team.

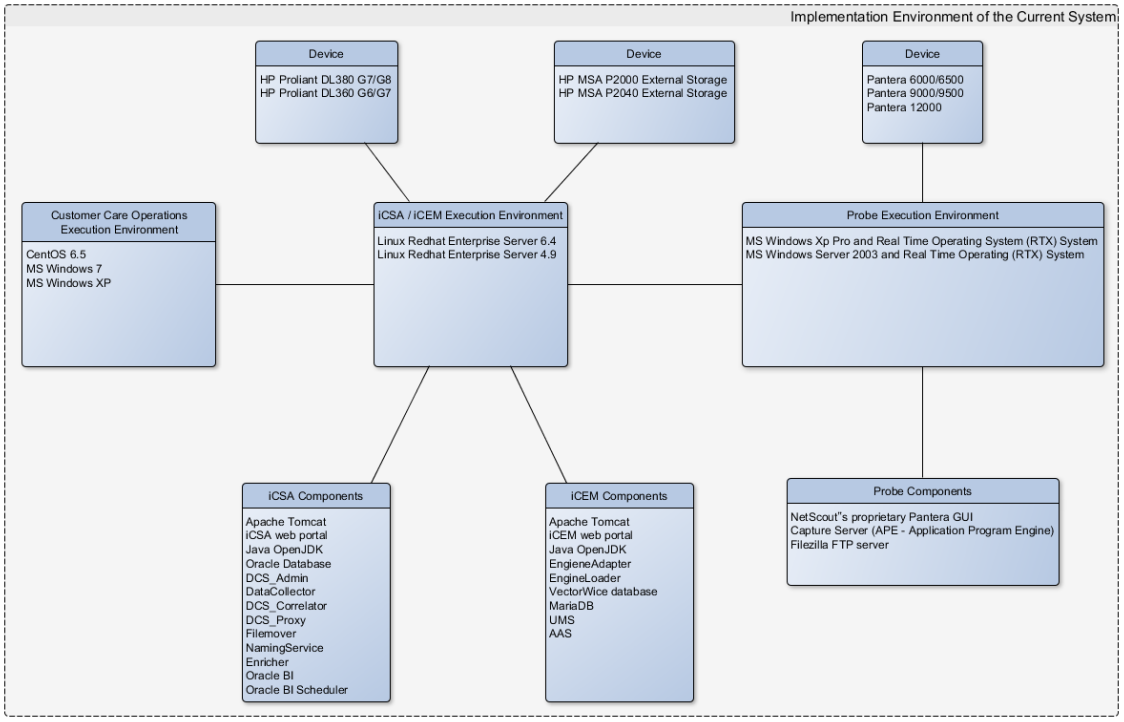
Description: The Customer virtual remote connection / VPN servers shall run upon CentOS 6.5.
Rationale: This is the chosen OS by the product line management.
Fit criterion: The product shall be approved for CentOS 6.5 compliance by Professional Services team.

Description: The Accanto COC web server shall run upon CentOS 6.5 64-bit operating system.
Rationale: This is the chosen OS by the product line management.
Fit criterion: The product shall be approved for CentOS 6.5 compliance by Professional Services team.

Description: Icinga version 1.7.2 shall be used as a core monitoring software.
Rationale: This is the chosen 3rd party monitoring software and version by the product line management.
Fit criterion: Icinga version 1.7.2 shall be tested for RHEL 6 compliance by product design unit testing group.

3.2. Implementation Environment of the Current System

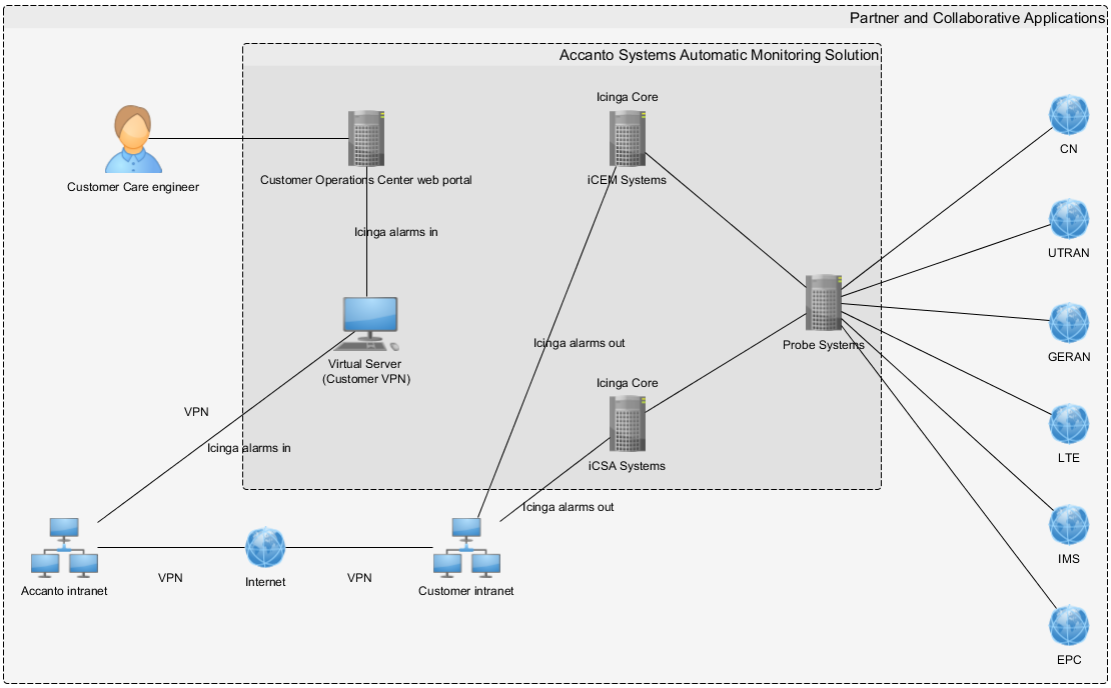
Below picture 2 presents the current environment and components in which the product shall be integrated.



Picture 2 Implementation Environment of the Current System

3.3. Partner or Collaborative Applications

Below picture 3 presents the external interfaces and partner systems and applications that will communicate with the product system.



Picture 3 Partner applications

3.4. Off-the-Shelf Software

The following off-the-shelf (OTS) software and hardware shall be used to implement the product system.

OTS hardware:
HP Proliant DL380 and DL360 server family

OTS commercial software:
Operating Systems: Red Hat Enterprise Linux Server, releases 4.9 and 6.4

OTS open source software (free):
Operating System: CentOS release 6.5
3rd party SW: Icinga Core 1.7.2 monitoring software, NRPE and NSClient++ monitoring agents and Nagios plugins

3.5. Anticipated Workplace Environment

The user work place is a standard open office environment where user's sits in front of the monitor and keyboard. Work areas are usually separated only by thin walls. Some privacy is needed due to nature of the work. Work place includes large monitoring screens which are located on the office walls.

3.6. Schedule Constraints

The product shall be ready for Accanto Customer Care internal review by end of year 2014. However this deadline is not critical and does not include any penalties as being in-house development work. This is done when required resources have free time from their other tasks.

3.7. Budget Constraints

The budget for this project comes from Accanto Systems Professional Services annual budget but there is no exact amount of money or resources allocated to this in-house development work. This is done when required resources have free time from their other tasks.

4 NAMING CONVENTIONS AND TERMINOLOGY

4.1. Definitions of All Terms, Including Acronyms, Used in the Project

COC: Customer Operation Center

OTS: Off-The-Self

VPN: Virtual Private Network

OS: Operating System

RHEL: Red Hat Enterprise Linux

CentOS: Community Enterprise Operating System

NRPE: Nagios Remote Plugin Executor

CN: Core Network

UTRAN: Universal Terrestrial Radio Access Network

GERAN: GSM EDGE Radio Access Network

LTE: Long Term Evolution

IMS: IP Multimedia Core Network Subsystem

EPC: Evolved Packet Core

iCEM: intelligent Customer Experience Management

iCSA: intelligent Customer Services Assurance

Probe: System that “probes” the network protocol signalling data

5 RELEVANT FACTS AND ASSUMPTIONS

5.1. Relevant Facts

All the virtual servers shall be hosted on Oracle VM VirtualBox or VMWare ESXi. Opening of the customer specific VPN tunnels cannot be fully automated as these require a various manual VPN token or passcode generation methods. The Customer Care engineer has to manually open the connections on each virtual server.

5.2. Business Rules

The allowed working week for Customer Care engineer is from Monday to Friday and there is no on-call duties agreement. The normal work day is 7.5 hours, from 8 am to 16 pm.

5.3. Assumptions

It is assumed that virtual servers are available for all the customer remote VPN connections as well as dedicated virtual web server for Accanto Systems Customer Care COC-portal.

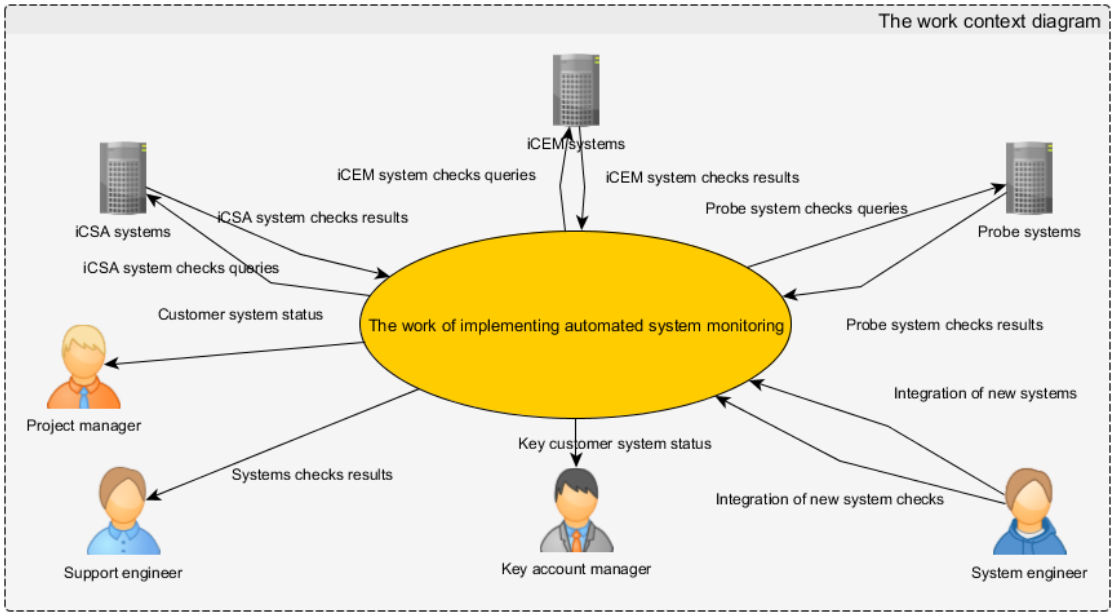
6 THE SCOPE OF THE WORK

6.1. The Current Situation

Currently it is very time consuming work for 1st line support engineer to proactively monitor the customer systems health. It requires opening multiple VPN connections to different customer systems and executing various commands in command line or using some external tool to verify that the system is operational and in good health.

6.2. The Context of the Work

Below picture 4 shows the input/output flows between the work and the outside adjacent systems. It also identifies the boundaries of the investigated work. Refer to the Data Dictionary in Section 7 for more information about the input/output interfaces.



Picture 4 Work context diagram

6.3. Work Partitioning

Below is the list of all business events which shall be included in this work. These business events form the basis of detailed system requirements. The inputs and outputs are traceable to the work context diagram.

Business Event List

Event Name	Input and Output	Summary of BUC
1. Time to monitor all customer systems status.	All systems checks results (out).	To verify that customer systems are operational and there are no issues.
2. System engineer installs new customer system.	Integration of new systems (in).	To monitor newly installed customer systems.
3. System engineer implements new system checks.	Integration of new system checks (in).	To monitor new system services and checks.
4. Time to check iCSA system services.	iCSA system checks queries (out). iCSA system checks results (in).	To verify that customer iCSA systems are operational and there are no issues.
5. Time to check iCEM system services.	iCEM system checks queries (out). iCEM system checks results (in).	To verify that customer iCEM systems are operational and there are no issues.
6. Time to check probe system services.	Probe system checks queries (out). Probe system checks results (in).	To verify that customer probe systems are operational and there are no issues.
7. Time to monitor customer system status during ongo-	Customer system status (in).	To monitor that customer systems are operational and there

ing project.		are no issues during the project.
8. Time to review key customer system overall health and service quality.	Key customer system status (in).	To review the overall customer solution status and quality provided to the customer.

6.4. Specifying a Business Use Case (BUC)

Below are presented BUC scenarios for each identified business event in the business event list ref. section 6c.

BUC Scenario for Business Event 1

Business Event 1: Time to monitor all customer systems status.

Business Use Case: To verify that customer systems are operational and there are no issues.

Trigger: All systems checks results.

Preconditions: Monitoring agents are installed on the target system.

Interested Stakeholders: Support engineer.

Active Stakeholders: iCSA systems, iCEM systems, Probe systems, monitoring system and Support engineer.

- Support engineer decides to check customer systems status.
- Monitoring system (Icinga) queries service check results from the monitored systems (iCSA, iCEM and Probe).
- Monitored systems (iCSA, iCEM and Probe) send system check results to monitoring system.
- Monitoring system (Icinga) stores the monitoring information and makes it available for further processing.
- All customer services problems are downloaded periodically as HTML format and parsed to Customer Care monitoring portal.

Outcome: All systems problems for all customers are shown in Customer Care monitoring portal.

BUC Scenario for Business Event 2

Business Event 2: System engineer installs new customer system.

Business Use Case: To monitor newly installed customer systems.

Trigger: Integration of new systems.

Preconditions: New customer system is installed.

Interested Stakeholders: System engineer and Support engineer.

Active Stakeholders: System engineer.

- System engineer installs a new system (iCSA. iCEM or Probe) in new or existing customer environment.
- System engineer integrates new system into Icinga monitoring system.
- System engineer integrates new system into Customer Care monitoring portal.

Outcome: New customer system is under Customer Care monitoring.

BUC Scenario for Business Event 3

Business Event 3: System engineer implements new system checks.

Business Use Case: To monitor new system services and checks.

Trigger: Integration of new system checks.

Preconditions: New critical system services are installed or identified. Icinga monitoring software and required monitoring agents (NRPE or NSCLient++) are installed.

Interested Stakeholders: System engineer and Support engineer.

Active Stakeholders: System engineer and Support engineer.

- New service checks are needed on customer system
- System engineer configures new service checks on the monitoring system (Icinga) and on the monitoring agents (NRPE or NSClient++) running on monitored host.

Outcome: New critical service checks are enabled for monitoring.

BUC Scenario for Business Event 4

Business Event 4: Time to check iCSA system services.

Business Use Case: To verify that customer iCSA systems are operational and there are no issues.

Trigger: iCSA system checks queries. iCSA system checks results.

Preconditions: Customer has iCSA system installed and valid maintenance agreement.

Interested Stakeholders: Support engineer.

Active Stakeholders: Support engineer.

- Support engineer decides to check customer systems status (from Customer Care monitoring portal).
- If problems are found those are investigated and if necessary escalated 2nd and 3rd line support.
- Customer is informed about any critical issues and trouble ticket is created for tracking the issue with customer.

Outcome: All critical iCSA system services are automatically monitored and problems are reported in Customer Care monitoring portal.

BUC Scenario for Business Event 5

Business Event 5: Time to check iCEM system services.

Business Use Case: To verify that customer iCEM systems are operational and there are no issues.

Trigger: iCEM system checks queries. iCEM system checks results.

Preconditions: Customer has iCEM system installed and valid maintenance agreement.

Interested Stakeholders: Support engineer.

Active Stakeholders: Support engineer.

- Support engineer decides to check customer systems status (from Customer Care monitoring portal).
- If problems are found those are investigated and if necessary escalated 2nd and 3rd line support.
- Customer is informed about any critical issues and trouble ticket is created for tracking the issue with customer.

Outcome: All critical iCEM system services are automatically monitored and problems are reported in Customer Care monitoring portal.

BUC Scenario for Business Event 6

Business Event 6: Time to check probe system services.

Business Use Case: To verify that customer probe systems are operational and there are no issues.

Trigger: Probe system checks queries. Probe system checks results.

Preconditions: Customer has Probe system installed and valid maintenance agreement.

Interested Stakeholders: Support engineer.

Active Stakeholders: Support engineer.

- Support engineer decides to check customer systems status (from Customer Care monitoring portal).
- If problems are found those are investigated and if necessary escalated 2nd and 3rd line support.
- Customer is informed about any critical issues and trouble ticket is created for tracking the issue with customer.

Outcome: All critical Probe system services are automatically monitored and problems are reported in Customer Care monitoring portal.

BUC Scenario for Business Event 7

Business Event 7: Time to monitor customer system status during ongoing project.
Business Use Case: To monitor that customer systems are operational and there are no issues during the project.
Trigger: Customer system status.
Preconditions: Customer has iCSA, iCEM or Probe systems installed.
Interested Stakeholders: Project manager.
Active Stakeholders: Project manager and System engineer.
- Project manager decides to check customer systems status (from Customer Care monitoring portal).
- If problems are found those are escalated to the project System engineer.
- Customer is informed about any critical project issues.
Outcome: Customer systems status can be reviewed and monitored during project phase.

BUC Scenario for Business Event 8

Business Event 8: Time to review key customer system overall health and service quality.
Business Use Case: To review the overall customer solution status and quality provided to the customer.
Trigger: Key customer system status.
Preconditions: Customer has iCSA, iCEM or Probe systems installed.
Interested Stakeholders: Key account manager.
Active Stakeholders: Key account manager.

- Key account manager decides to check customer systems status (from Customer Care monitoring portal).
- If problems are found those are escalated to 1st line support.
- Customer is informed about any critical issues and trouble ticket is created for tracking the issue with customer.

Outcome: Key account manager can review the key customer systems health and services quality.

7 BUSINESS DATA MODEL AND DATA DICTIONARY

7.1. Data Model

-

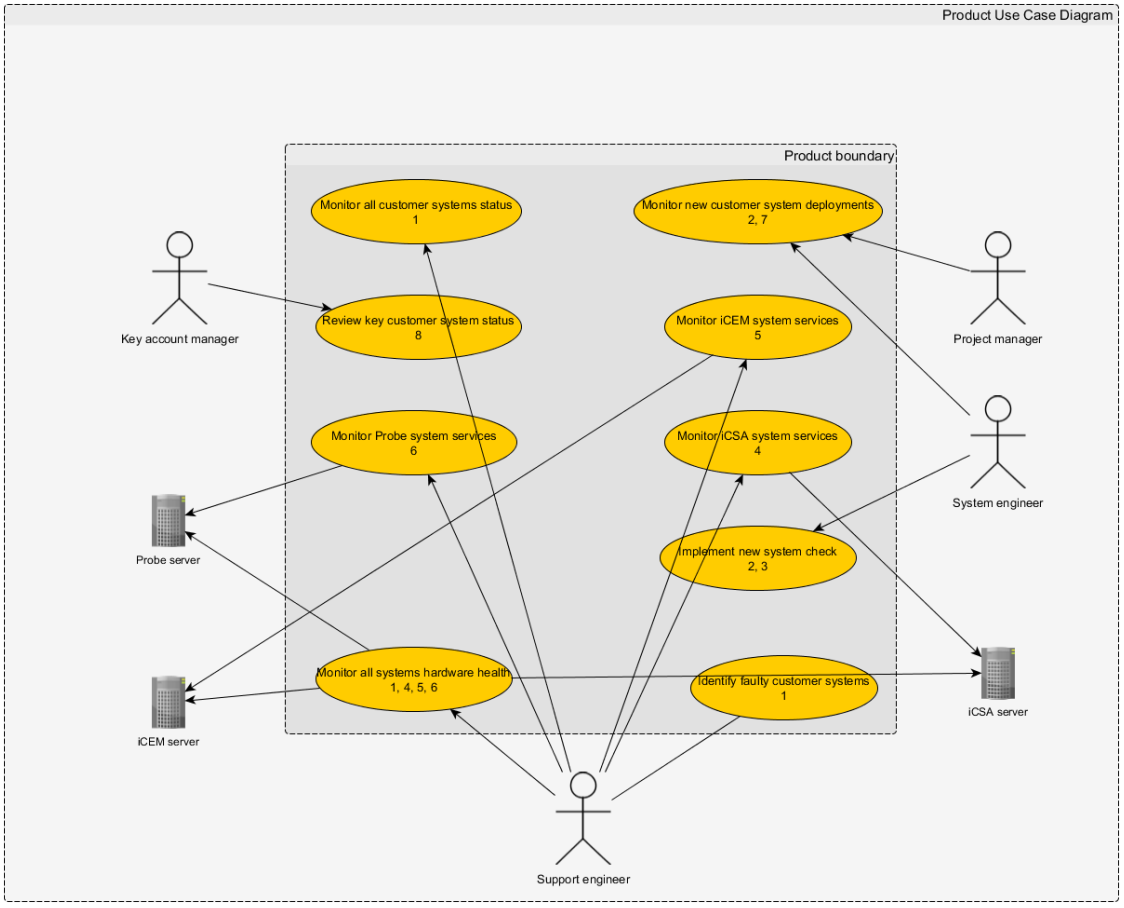
7.2. Data Dictionary

-

8 THE SCOPE OF THE PRODUCT

8.1. Product Boundary

The product use case diagram presented in picture 6 identifies the boundaries between the users (actors) and the product. The product use case diagram shows the actors/users outside the product boundary (the rectangle). The product use cases (PUCs) are the ellipses inside the boundary. The numbers link each PUC back to the BUC that it came from (see section 7). The lines denote usage.



Picture 5 PUC diagram

8.2. Product Use Case Table

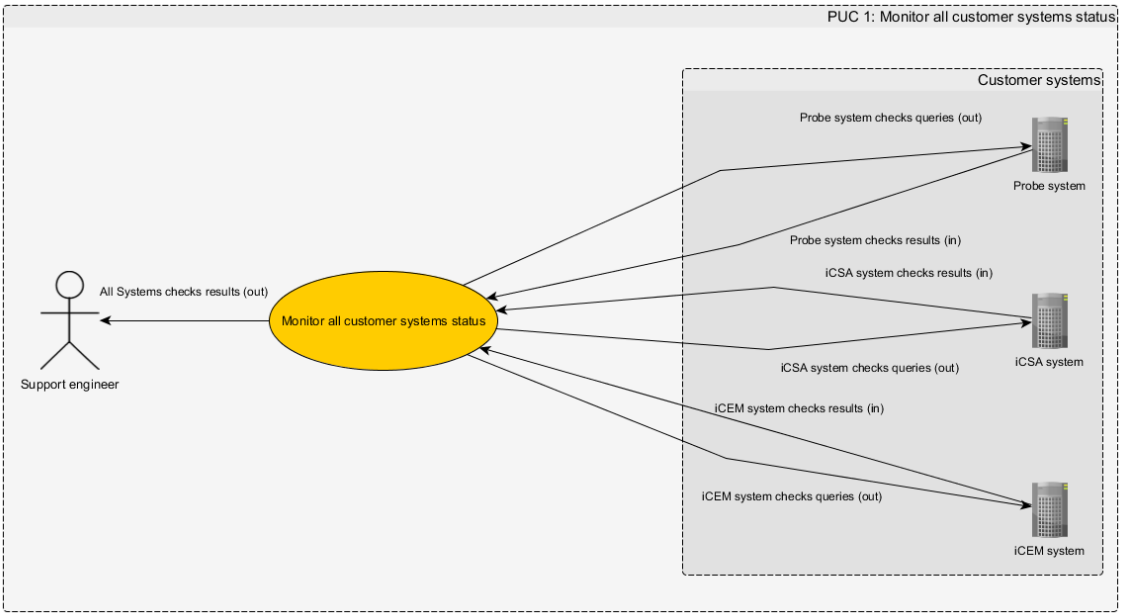
Below is the Product Use Case summary table.

Table 1 Product use case summary table

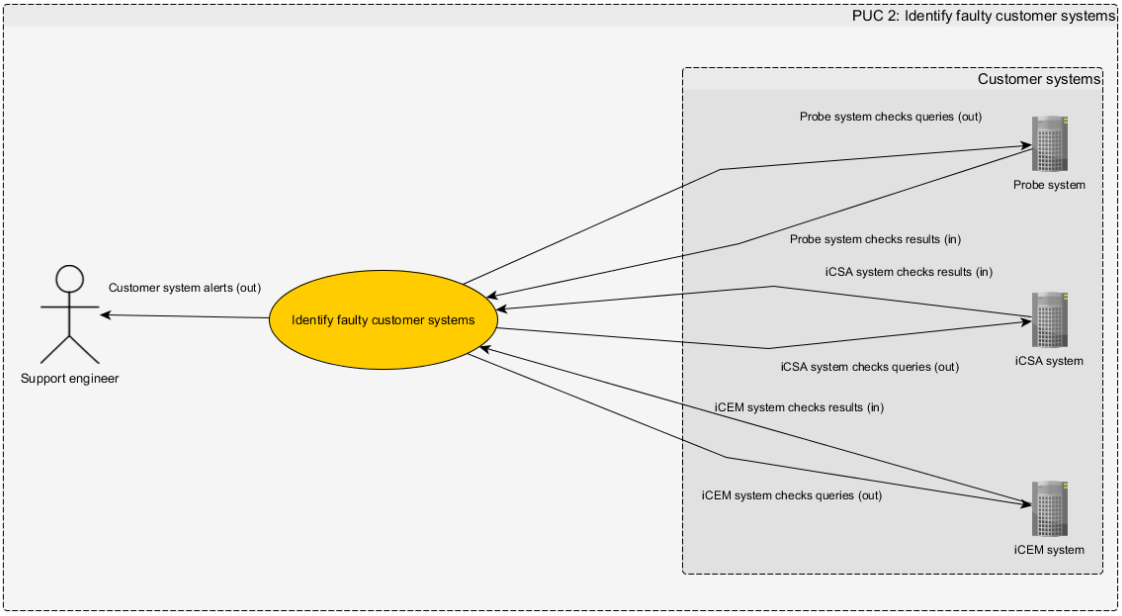
PUC No	PUC Name	Actor/s	Input & Output
1	Monitor all customer systems status	Support engineer	All Systems checks results (out)
2	Identify faulty customer systems	Support engineer	Customer system alerts (out)
3	Review key customer system status	Key account manager	Key customer system status (out)
4	Monitor Probe system services	Support engineer, Probe systems	Probe system checks queries (out), Probe system checks results (in)
5	Monitor iCEM system services	Support engineer, iCEM systems	iCEM system checks queries (out), iCEM system checks results (in)
6	Monitor iCSA system services	Support engineer, iCSA systems	iCSA system checks queries (out), iCSA system checks results (in)
7	Monitor all systems hardware health	Support engineer	
8	Monitor new customer system deployments	System engineer, Project manager	Customer system status (out), Integration of new systems (in)
9	Implement new system check	System engineer	Integration of new system checks (in)

8.3. Individual Product Use Cases

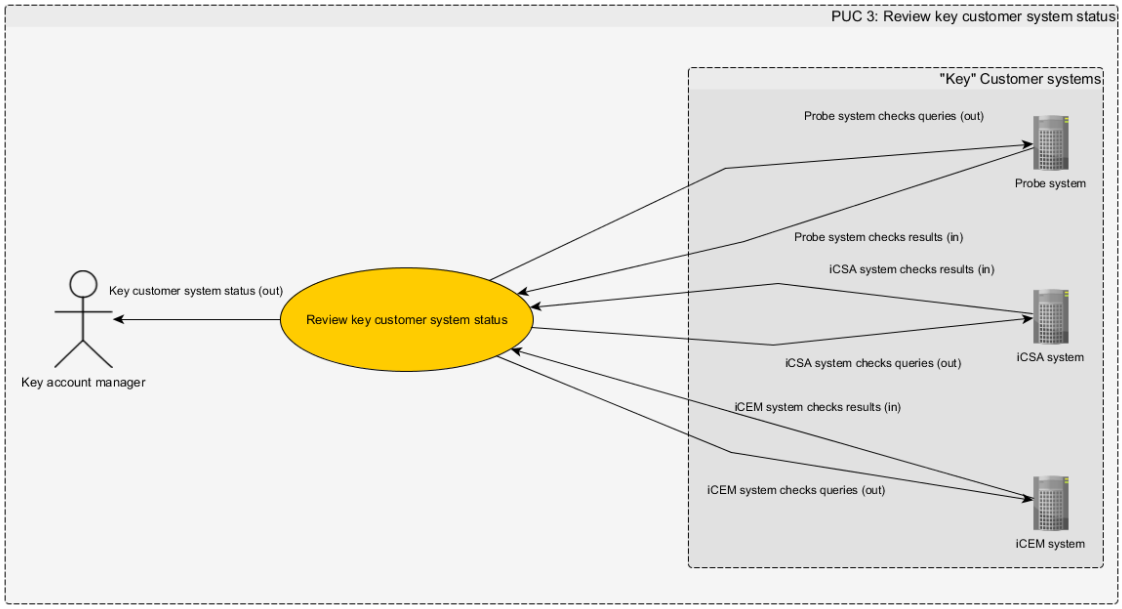
The individual product use case models are presented below:



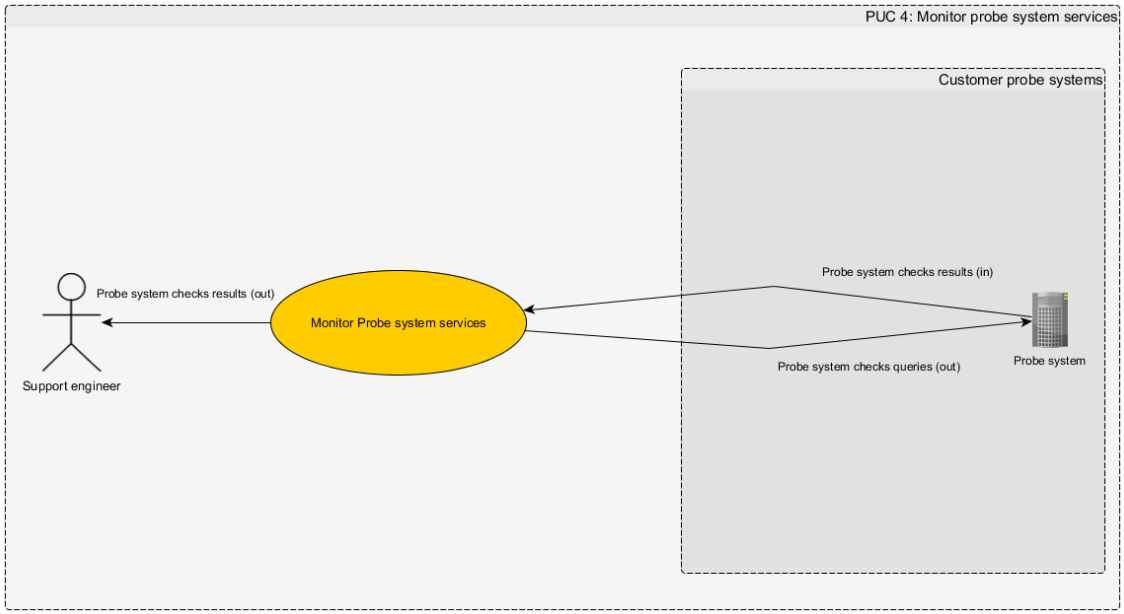
Picture 6 PUC 1: Monitor all customer systems status



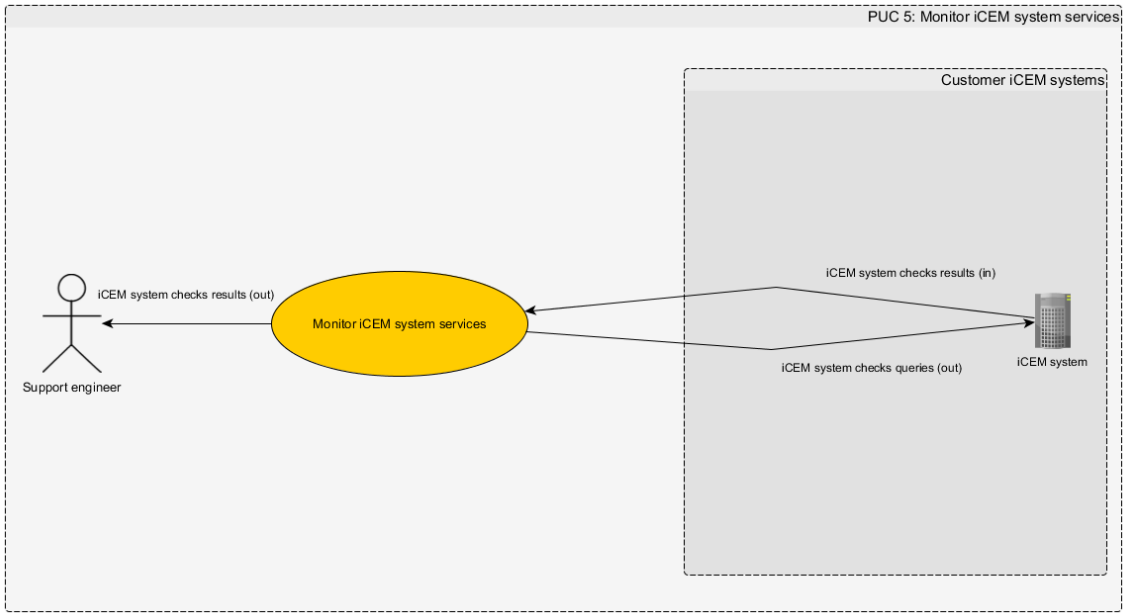
Picture 7 PUC 2: Identify faulty customer systems



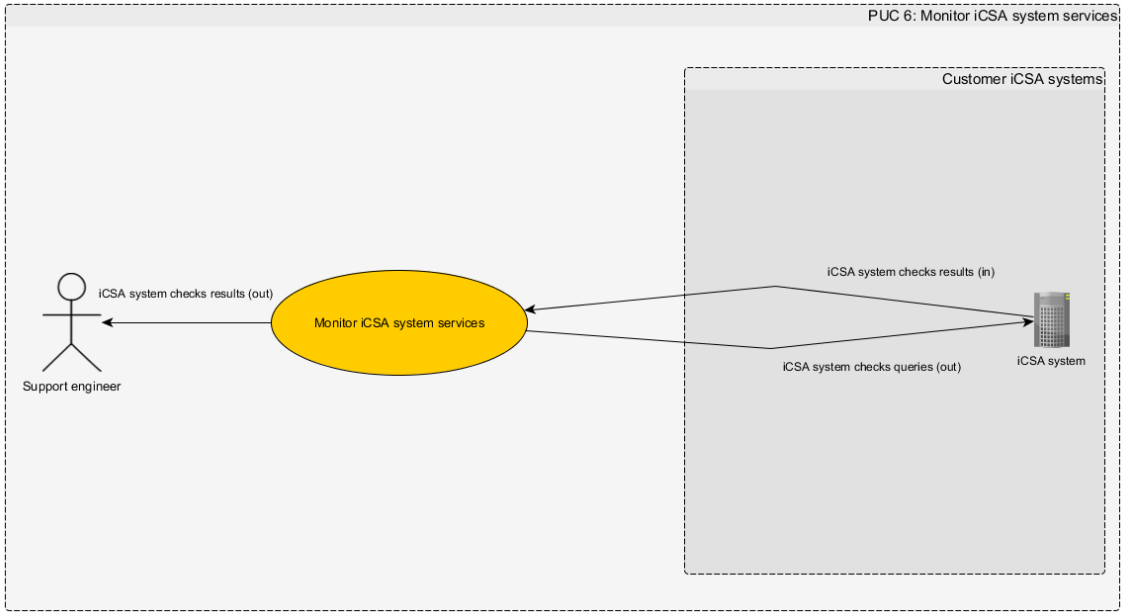
Picture 8 PUC 3: Review key customer system status



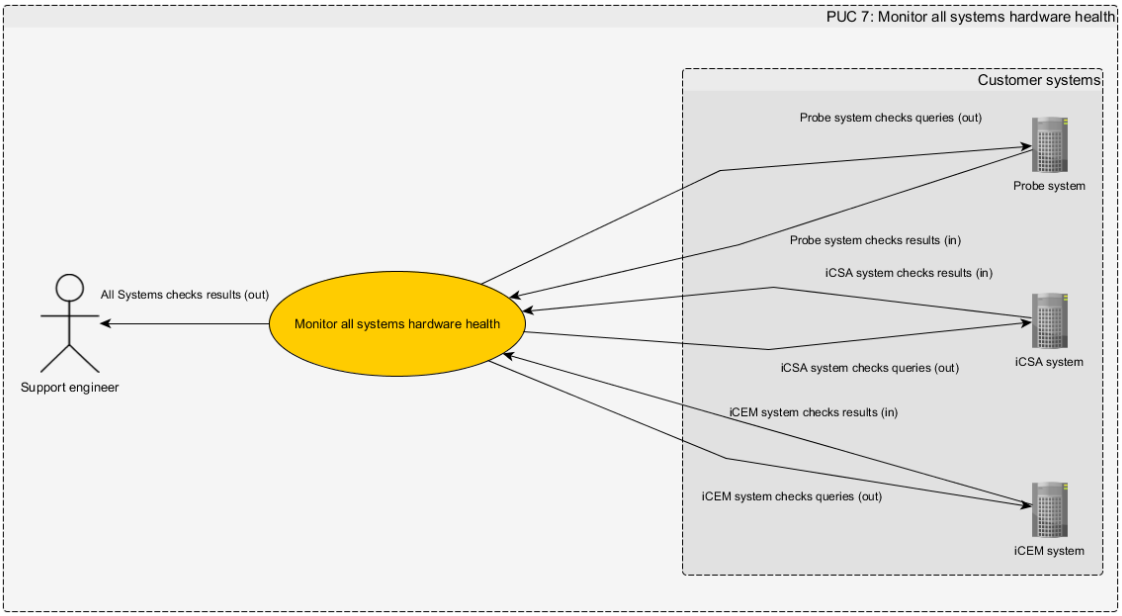
Picture 9 PUC 4: Monitor Probe system services



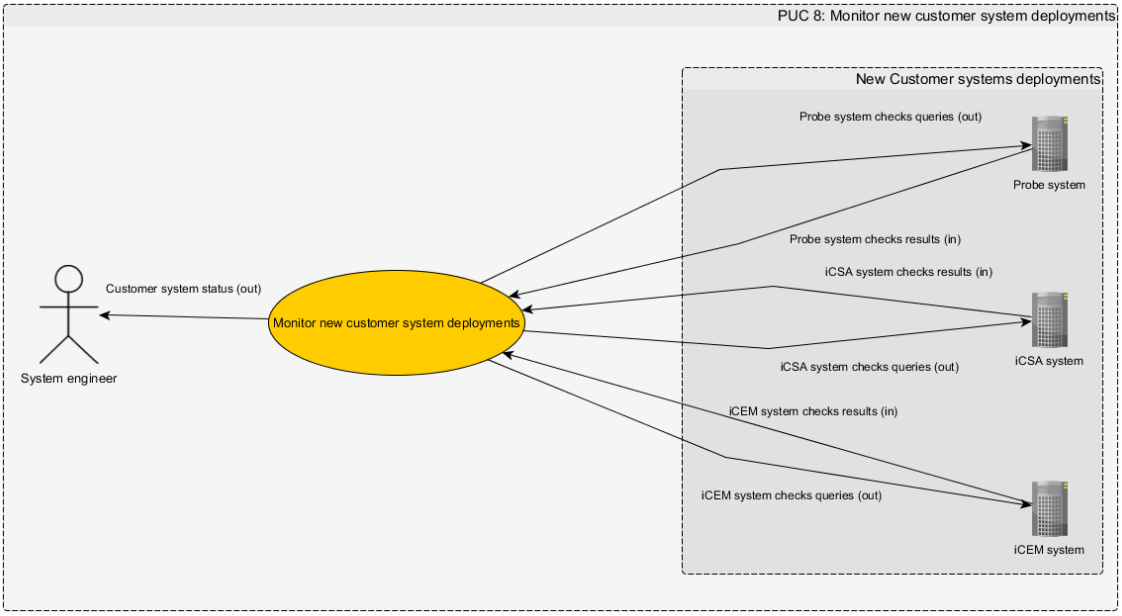
Picture 10 PUC 5: Monitor iCEM system services



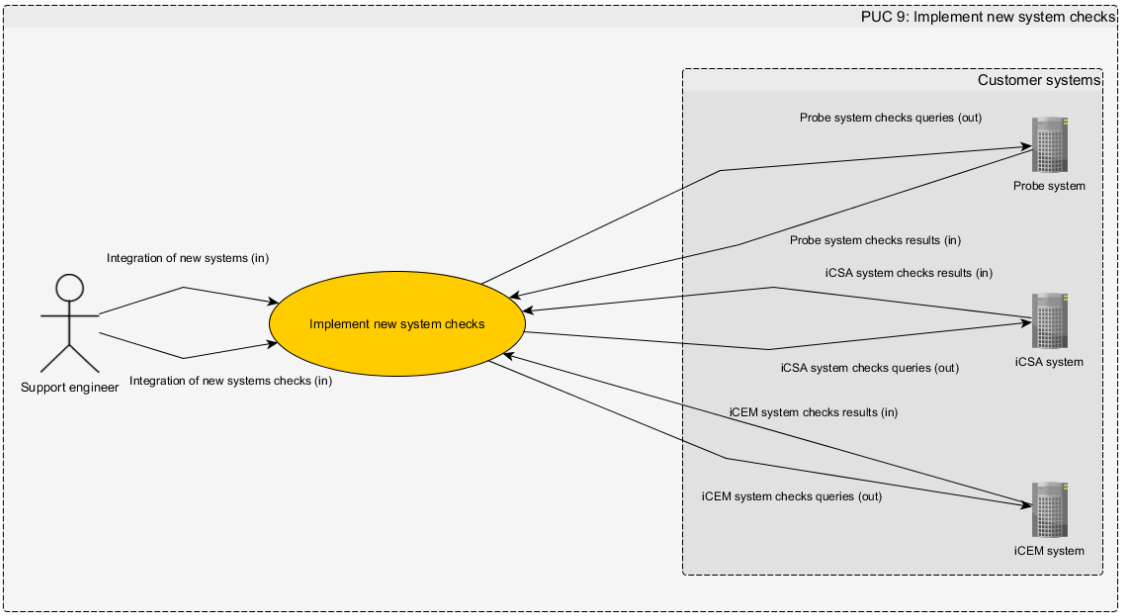
Picture 11 PUC 6: Monitor iCSA system services



Picture 12 PUC 7: Monitor all systems hardware health



Picture 13 PUC 8: Monitor new customer system deployments



Picture 14 PUC 9: Implement new system checks

9 FUNCTIONAL AND DATA REQUIREMENTS

9.1. Functional Requirements

Detailed functional requirements are listed in below table:

Table 2 Functional requirements

Product Use Case (PUC) Number	Requirement Type	Description	Rationale	Fit Criterion
6	Functional	It shall be possible to monitor the iCSA server NRPE client version.	It is necessary for CC engineer to see the Windows server NRPE client version.	The NRPE client version is displayed.
4, 5, 6	Functional	It shall be possible to monitor the server CPU load.	It is necessary for CC engineer to see server CPU load averages.	The server CPU load average is displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
4, 5, 6	Functional	It shall be possible to monitor the server disk utilization.	It is necessary for CC engineer to see server disk utilization so that file systems are not full.	The server file system partitions "free space" is displayed with the status information according to the configured thresholds

				(OK/WARN/CRIT).
4, 5, 6	Functional	It shall be possible to monitor the server swap space usage.	It is necessary for CC engineer to see if the server is swapping.	The server free (%) SWAP space is displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
4, 5, 6	Functional	It shall be possible to monitor the server "zombie" processes.	It is necessary for CC engineer to see if the server has "zombie" processes.	The amount of "zombie" processes are displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
6	Functional	It shall be possible to monitor the server SDF Loader Queue.	It is necessary for CC engineer to see if there is a data loading queues on the system to ensure real-time loading.	The amount of "unloaded" files is displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
6	Functional	It shall be possible to monitor the server iCSA log.	It is necessary for CC engineer to see if there are er-	The amount of ERRORs and WARNINGs are displayed with the

			rors in the iCSA web application log.	status information according to the configured thresholds (OK/WARN/CRIT).
6	Functional	It shall be possible to monitor the Oracle database.	It is necessary for CC engineer to see if Oracle database is running and accepting connections.	The status of "tnsping" is displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
6	Functional	It shall be possible to monitor the Oracle Database CDRPROT Tablespace.	It is necessary for CC engineer to see Oracle database CDRPROT tablespace utilization rate.	The CDRPROT tablespace utilization rate (used %) is displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
6	Functional	It shall be possible to monitor the Oracle Database TREND Tablespace.	It is necessary for CC engineer to see Oracle database TREND tablespace utilization rate.	The TREND tablespace utilization rate (used %) is displayed with the status information according to the configured thresholds (OK/WARN/CRIT).

6	Functional	It shall be possible to monitor the Oracle Database DCS Tablespace.	It is necessary for CC engineer to see Oracle database DCS tablespace utilization rate.	The DCS tablespace utilization rate (used %) is displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
6	Functional	It shall be possible to monitor the Oracle Database ALARM Tablespace.	It is necessary for CC engineer to see Oracle database ALARM tablespace utilization rate.	The ALARM tablespace utilization rate (used %) is displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
6	Functional	It shall be possible to monitor the server Oracle Database process count.	It is necessary for CC engineer to see the current amount of Oracle database processes.	The sum of Oracle database processes is displayd with the status information according to the configured thresholds (OK/WARN/CRIT).
6	Functional	It shall be possible to monitor the server Tomcat process.	It is necessary for CC engineer to see the status of the Tomcat process.	The count (1) of Tomcat process is displayed with the status information according to the configured thresh-

				olds (OK/CRIT).
6	Functional	It shall be possible to monitor the server Oracle BI process.	It is necessary for CC engineer to see the status of the Oracle BI server process.	The count (1) of Oracle BI server process is displayed with the status information according to the configured thresholds (OK/CRIT).
6	Functional	It shall be possible to monitor the server DCS_Admin process.	It is necessary for CC engineer to see the status of the DCS_Admin process.	The count (1) of DCS_Admin process is displayed with the status information according to the configured thresholds (OK/CRIT).
6	Functional	It shall be possible to monitor the server DataCollector process.	It is necessary for CC engineer to see the status of the DataCollector process.	The count (1) of DataCollector process is displayed with the status information according to the configured thresholds (OK/CRIT).
6	Functional	It shall be possible to monitor the server DCS_Proxy process.	It is necessary for CC engineer to see the status of the DCS_Proxy process.	The count (1) of DCS_Proxy process is displayed with the status information according to the configured thresholds

				(OK/CRIT).
6	Functional	It shall be possible to monitor the server DCS_Correlator process.	It is necessary for CC engineer to see the status of the DCS_Correlator process.	The count (1) of DCS_Correlator process is displayed with the status information according to the configured thresholds (OK/CRIT).
6	Functional	It shall be possible to monitor the server FileMover process.	It is necessary for CC engineer to see the status of the FileMover process.	The count (1) of FileMover process is displayed with the status information according to the configured thresholds (OK/CRIT).
6	Functional	It shall be possible to monitor the server NamingService process.	It is necessary for CC engineer to see the status of the NamingService process.	The count (1) of NamingService process is displayed with the status information according to the configured thresholds (OK/CRIT).
6	Functional	It shall be possible to monitor the server Oracle BI Scheduler process.	It is necessary for CC engineer to see the status of the BI Scheduler process.	The count (1) of Bi Scheduler process is displayed with the status information according to the configured thresholds

				(OK/CRIT).
4, 5, 6	Functional	It shall be possible to monitor the server hardware disks RAID status.	It is necessary for CC engineer to see health of the server disks RAID.	The status of the configured disks/LUNs RAID is displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
7	Functional	It shall be possible to monitor the server (HP) Hardware Status.	It is necessary for CC engineer to see health of the server HP hardware.	The status of the server (HP) hardware is displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
6	Functional	It shall be possible to monitor the Oracle database table (Max) partitions status.	It is necessary for CC engineer to see the max/newest "dates" of all the protocol tables partitions.	The status of all the protocol tables partitions are displayed with the status information according to the configured thresholds (OK/WARN/CRIT).

6	Functional	It shall be possible to monitor the received/downloaded SDF delays by each data source.	It is necessary for CC engineer to see if some data source is not producing any SDF files.	The SDF files receiving delay for each of the data sources are displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
6	Functional	It shall be possible to monitor the server CDR Load Count.	It is necessary for CC engineer to see the sum of loaded CDR row counts for ALL protocol(s) from the last 1 hour(s).	The sum of loaded CDR row count for ALL protocol(s)is displayed for the last 1 hour(s) with the status information according to the configured thresholds (OK/WARN/CRIT).
2	Functional	It shall be possible to get "Service Problems" from Iginga server in HTML format.	It is necessary for COC dashboard functionaly to get "Service Problems" from all Customers in HTML format.	The "Service Problems" HTML is downloaded from Customer Icinga server to the Accanto COC server.
1	Functional	It shall be possible to parse the "Service Problems" HTML and retrieve	It is necessary for COC dashboard functionaly to	All "Service Problems" meaning Warning and Critical service alarm

		the required information for each Customer to the COC dashboard.	parse "Service Problems" HTML data for each Customer and show it in COC dashboard.	counts as well as Alarms Details for All Customers are displayed in the COC dashboard.
1	Functional	It shall be possible to "Drill Down" from Accanto COC dashboard to the latest "Service Problems" HTML page for each Customer.	It is necessary for CC engineer to see detailed Service Problems information for each Customer by drilling down / clicking the Customer name link on the COC dashboard.	Clicking the Customer name link opens detailed "Service Problems" page for that specific Customer.
5	Functional	It shall be possible to monitor the iCEM server NRPE client version.	It is necessary for CC engineer to see the Windows server NRPE client version.	The NRPE client version is displayed with the status information according to the configured thresholds (OK/CRIT).
5	Functional	It shall be possible to monitor the server EngineAdabter process.	It is necessary for CC engineer to see the status of the EngineAdapter process.	The count (1) of EngineAdabter server process is displayed with the status information according to the

				configured thresholds (OK/CRIT).
5	Functional	It shall be possible to monitor the server EngineLoader process.	It is necessary for CC engineer to see the status of the EngineLoader process.	The count (1) of EngineLoader server process is displayed with the status information according to the configured thresholds (OK/CRIT).
5	Functional	It shall be possible to monitor the server QueryTool general log for any errors or warnings.	It is necessary for CC engineer to see if there are errors or warnings in the QueryTool general log.	The amount of ERRORs and WARNINGs are displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
5	Functional	It shall be possible to monitor the server QueryTool error log for any errors or warnings.	It is necessary for CC engineer to see if there are errors or warnings in the QueryTool error log.	The amount of ERRORs and WARNINGs are displayed with the status information according to the configured thresholds (OK/WARN/CRIT).

5	Functional	It shall be possible to monitor the server VectorWice database process(es).	It is necessary for CC engineer to see the status of the VectorWice database main process(es).	The count (2) of VectorWice main server processes is displayed with the status information according to the configured thresholds (OK/CRIT).
5	Functional	It shall be possible to monitor the server VectorWice database uptime.	It is necessary for CC engineer to see the current uptime of the VectorWice database.	The VectorWice database process uptime is displayed with the status information according to the configured thresholds (OK/CRIT).
5	Functional	It shall be possible to monitor the server VectorWice database open sessions.	It is necessary for CC engineer to see the amount of open sessions on the VectorWice database.	The amount of open VectorWice sessions is displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
5	Functional	It shall be possible to monitor the VectorWice database table (Max) partitions status.	It is necessary for CC engineer to see the max/newest "dates" of all the protocol tables partitions.	The status of all the protocol tables partitions are displayed with the status information according to the configured thresholds (OK/WARN/CRIT

				).
5	Functional	It shall be possible to monitor the amount of SSD writes on the server SSD disks.	It is necessary for CC engineer to see the amount of completed SSD writes on the SSD disks.	The number of completed SSD writes on each SSD device are displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
5	Functional	It shall be possible to monitor the server Linux file system partitions "free space" capacity.	It is necessary for CC engineer to see server disk utilization so that file systems are not full.	The server file system partitions "free space" is displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
5	Functional	It shall be possible to monitor the server EngineAdabter process load queue.	It is necessary for CC engineer to see if there is a data processing queues on the system to ensure real-time loading.	The amount of "unparsed" files is displayed with the status information according to the configured thresholds (OK/WARN/CRIT).

5	Functional	It shall be possible to monitor the server Engine-Loader process load queue.	It is necessary for CC engineer to see if there is a data loading queues on the system to ensure real-time loading.	The amount of "unloaded" files is displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
5	Functional	It shall be possible to monitor the amount of loaded rows by the EngineLoader process for each protocol for the last 1 hour.	It is necessary for CC engineer to see the amount of loaded rows for the last 1 hour.	The number of loaded rows are displayed as per protocol with the status information according to the configured thresholds (OK/WARN/CRIT).
5	Functional	It shall be possible to monitor the amount of rejected rows by the database during loading process for each protocol for the last 1 hour.	It is necessary for CC engineer to see the amount of rejected rows for the last 1 hour.	The number of rejected rows are displayed as per protocol with the status information according to the configured thresholds (OK/WARN/CRIT).
5	Functional	It shall be possible to monitor the folder size of the database rejected files.	It is necessary for CC engineer to see the size of the rejected files folder.	The size of the rejected files folder is displayed with the status information according to the configured

				thresholds (OK/WARN/CRIT).
5	Functional	It shall be possible to monitor the percentage of groups for which KPI's are calculated.	It is necessary for the CC engineer to see the percentage of the groups for which the KPI's are calculated.	The percentages of the groups present in the KPIs for the last 12 hours are displayed as per category with the status information according to the configured thresholds (OK/WARN/CRIT).
5	Functional	It shall be possible to monitor the source content delay for each configured data source.	It is necessary for CC engineer to see if some datasource is not producing any SDF files.	The SDF files receiving delay for each of the datasources are displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
4	Functional	It shall be possible to monitor the probe server NSClient version.	It is necessary for CC engineer to see the probe server NSClient version.	The NSClient version is displayed with the status information according to the configured thresholds (OK/WARN/CRIT))..

4	Functional	It shall be possible to monitor the probe server up-time.	It is necessary for CC engi-neer to see the probe server current up-time.	The system uptime is displayed with the status infor-mation according to the configured thresholds (OK/WARN/CRIT).
4	Functional	It shall be possible to monitor the probe server CPU load averages for the last 5 minutes.	It is necessary for CC engi-neer to see the prope server average CPU load for the last 5 minutes.	The system CPU load average for the last 5 minutes is displayed with the status infor-mation according to the configured thresholds (OK/WARN/CRIT).
4	Functional	It shall be possible to monitor the probe server memory usage.	It is necessary for CC engi-neer to see the Windows server memory usage.	The system memory usage details (total, used, free) are displayed with the status in-formation accord-ing to the config-ured thresholds (OK/WARN/CRIT).
4	Functional	It shall be possible to monitor the probe server c:\ drive free space.	It is necessary for CC engi-neer to see the Windows server c:\ drive free space.	The system c:\ drive capacity de-tails (total, used, free) are displayed with the status in-formation accord-ing to the config-

				ured thresholds (OK/WARN/CRIT).
4	Functional	It shall be possible to monitor the probe server d:\ drive free space.	It is necessary for CC engineer to see the Windows server d:\ drive free space.	The system d:\ drive capacity details (total, used, free) are displayed with the status information according to the configured thresholds (OK/WARN/CRIT).
4	Functional	It shall be possible to monitor the probe server Explorer process status.	It is necessary for CC engineer to see the Windows server Explorer process status.	The status of explorer.exe server process is displayed with the status information according to the configured thresholds (OK/CRIT).
4	Functional	It shall be possible to monitor the probe server Application Protocol Engine process status.	It is necessary for CC engineer to see the probe server APE process status.	The status of ape.exe server process is displayed with the status information according to the configured thresholds (OK/CRIT).
4	Functional	It shall be possible to monitor the probe server Filezilla server process status.	It is necessary for CC engineer to see the probe server Filezilla server	The status of filezilla server.exe server process is displayed with the status information

			process status.	according to the configured thresholds (OK/CRIT).
4	Functional	It shall be possible to monitor the probe server RAID controller disks status.	It is necessary for CC engineer to see the probe server RAID controller disks health.	The RAID status is displayed with the status information according to the configured thresholds (OK/WARN/CRIT).

10 NON-FUNCTIONAL REQUIREMENTS

The following sections 10-17 describe the non-functional requirements. The form of these requirements is the same as for the functional requirements as described above.

11 LOOK AND FEEL REQUIREMENTS

11.1. Appearance Requirements

Detailed look and feel requirements are listed in below table:

Table 3 Look and feel requirements

Product Use Case (PUC) Number	Requirement Type	Description	Rationale	Fit Criterion
2	Look and Feel	If any Warning alarms exist the field shall be highlighted with "orange" background colour in the COC dashboard.	It is convenient for CC engineer when problems are highlighted in the COC dashboard.	The Warning field are highlighted in "orange" when there are "1" or more alarms.
2	Look and Feel	If any Critical alarms exists the field shall be highlighted with "red" background colour in the COC dashboard.	It is convenient for CC engineer when problems are highlighted in the COC dashboard.	The Critical field are highlighted in "red" when there are "1" or more alarms.
2	Look and Feel	When there are no Critical or Warning alarms, the fields shall be highlighted with "green" background colour in the COC	It is convenient for CC engineer when OK status is highlighted in the COC dashboard.	The Critical and Warning fields are highlighted in "green" when there are "0" alarms.

		dashboard.		
2	Look and Feel	If "Last Update" time is more than 1 hour the field background shall be highlighted with "red".	It is convenient for CC engineer to see if the COC monitoring is up to date for specific Customer.	The Last Update" field is highlighted with "green" when Customer Icinga alarms are 1 hour old or less. When more than 1 hour old then the field is highlighted with "red".
	Look and Feel	The Icinga server web GUI shall have "classic" Icinga GUI look.	The Icinga Classic web client is selected by the product line management.	The Icinga Classic Web GUI is installed together with Icinga Core.
	Look and Feel	The Accanto COC dashboard shall be simple "table" look with columns: Customer, Critical, Warnings, Last Update, Alarm Details.	This is selected look and layout of the COC dashboard by the Professional Services team.	The Accanto COC dashboard includes the selected columns (Customer, Critical, Warnings, Last Update, Alarm Details) for information.

11.2. Style Requirements

Please refer to section 11.1.

12 USABILITY AND HUMANITY REQUIREMENTS

This section is concerned with requirements that make the product usable and ergonomically acceptable to its hands-on users.

12.1. Ease of Use Requirements

Detailed usability and humanity requirements are listed in below table:

Table 4 Usability requirements

Product Use Case (PUC) Number	Requirement Type	Description	Rationale	Fit Criterion
	Usability	The Accanto COC dashboard shall have automatic refresh.	It is convenient for CC engineer to have Accanto COC dashboard automatically refreshed with new data.	The Accanto COC dashboard refreshes automatically every 60 seconds.

12.2. Personalization and Internationalization Requirements

Please refer to section 12.1.

12.3. Learning Requirements

Please refer to section 12.1.

12.4. Understandability and Politeness Requirements

Please refer to section 12.1.

12.5. Accessibility Requirements

Please refer to section 12.1.

13 PERFORMANCE REQUIREMENTS

13.1. Speed and Latency Requirements

Detailed performance requirements are listed in below table:

Table 5 Performance requirements

Product Use Case (PUC) Number	Requirement Type	Description	Rationale	Fit Criterion
	Performance	The Icinga monitoring sofware shall run "light".	The Icinga sowtware shall not effect the product web server performance.	The CPU and memory usage of the Icinga service shall not exceed 5% of CPU and 1G of memory.

13.2. Safety-Critical Requirements

Please refer to section 13.1.

13.3. Precision or Accuracy Requirements

Please refer to section 13.1.

13.4. Reliability and Availability Requirements

Please refer to section 13.1.

13.5. Robustness or Fault-Tolerance Requirements

Please refer to section 13.1.

13.6. Capacity Requirements

Please refer to section 13.1.

13.7. Scalability or Extensibility Requirements

Please refer to section 13.1.

13.8. Longevity Requirements

Please refer to section 13.1.

14 OPERATIONAL AND ENVIRONMENTAL REQUIREMENTS

14.1. Expected Physical Environment

Detailed operational and environmental requirements are listed in below table:

Table 6 Operational and environmental requirements

Product Use Case (PUC) Number	Requirement Type	Description	Rationale	Fit Criterion
	Operational	The Accanto COC dashboard shall run in Mozilla Firefox browser.	To be convenient for the Firefox users.	All product's Web GUI functions must work with the latest Firefox versions.
	Operational	The Accanto COC dashboard shall run in Internet Explorer browser.	To be convenient for the IE users.	All product's Web GUI functions must work with the latest IE versions.
	Operational	The Accanto COC dashboard shall run as web browser-based application.	It is convenient to access the product by using the web browser only.	The broduct features are accessable via web browser.
	Operational	The Accanto COC dashboard shall run on 32-bit Windows 7.	Some customers are using 32-bit Windows 7.	The broduct client sw is compatible with 32-bit Windows 7.
	Operational	The Accanto COC dashboard shall run on 32-bit Windows 8.	Some customers are using 32-bit Windows 8.	The broduct client sw is compatible with 32-bit Windows 8.

	Operational	The Accanto COC dashboard shall run on 64-bit Windows 7.	Some customers are using 64-bit Windows 7.	The broduct client sw is compatible with 64-bit Windows 7.
	Operational	The Accanto COC dashboard shall run on 64-bit Windows 8.	Some customers are using 64-bit Windows 8.	The broduct client sw is compatible with 64-bit Windows 8.

14.2. Requirements for Interfacing with Adjacent Systems

Please refer to section 14.1.

14.3. Productization Requirements

Please refer to section 14.1.

14.4. Release Requirements

Please refer to section 14.1.

15 MAINTAINABILITY AND SUPPORT REQUIREMENTS

15.1. Maintenance Requirements

Detailed maintainability requirements are listed in below table:

Table 7 Maintenance requirements

Product Use Case (PUC) Number	Requirement Type	Description	Rationale	Fit Criterion
	Maintainability	It shall be possible to backup and restore system and configuration files.	System backup is needed to restore system functionality in case of system/human errors.	The system and configuration files are successfully backed up and restored.
	Maintainability	It shall be possible to roll back the system last consistent state.	Prior to system upgrade it is required to create a "snapshot" of the system, which can be restored in case the upgrade fails.	The system snapshot is created and it can be used to restore the system last consistent state.
	Maintainability	It shall be possible to initial install the system within 1 hour. The system administrator is only permitted role for this action.	For maintainability reasons the installation time is limited to 1 hours max.	The system is successfully installed under 1 hours.

	Maintainability	It shall be possible to upgrade the system within 1 hour. The system administrator is only permitted role for this action.	For maintainability reasons the upgrade time is limited to 1 hours max.	The system is successfully upgraded under 1 hours.
	Maintainability	It shall be possible to install the system by command line interface.	It is required that system can be installed by command line interface.	The system is succesfully installed via command line.
	Maintainability	It shall be possible to upgrade the system by command line interface.	It is required that system can be upgraded by command line interface.	The system is succesfully upgraded via command line.

15.2. Supportability Requirements

Please refer to section 15.1.

15.3. Adaptability Requirements

Please refer to section 15.1.

16 SECURITY REQUIREMENTS

16.1. Access Requirements

Detailed security requirements are listed in below table:

Table 8 Security requirements

Product Use Case (PUC) Number	Requirement Type	Description	Rationale	Fit Criterion
	Security	The Customer Icinga server shall have latest RHEL 4.9 patches installed.	For security and stability reasons the system shal be patched with latest RHEL 4.9 patches.	RHEL 4.9 patches are up to date.
	Security	The Customer Icinga server shall have latest RHEL 6.4 patches installed.	For security and stability reasons the system shal be patched with latest RHEL 6.4 patches.	RHEL 6.4 patches are up to date.
	Security	The Accanto COC server shall have latest CentOS 6.5 patches installed.	For security and stability reasons the system shal be patched with latest CentOS 6.5 patches.	CentOS 6.5 patches are up to date.

16.2. Integrity Requirements

Please refer to section 16.1.

16.3. Privacy Requirements

Please refer to section 16.1.

16.4. Audit Requirements

Please refer to section 16.1.

16.5. Immunity Requirements

Please refer to section 16.1.

17 CULTURAL AND POLITICAL REQUIREMENTS

17.1. Cultural Requirements

Currently there are no identified cultural requirements.

17.2. Political Requirements

Currently there are no identified political requirements.

18 LEGAL REQUIREMENTS

18.1. Compliance Requirements

All customer data shall be handled with confidentially.

18.2. Standards Requirements

The product shall comply with Accanto Systems standards.

19 OPEN ISSUES

Currently all open issues are listed below.

Issue1.

References:

Summary:

Stakeholders:

20 OFF-THE-SHELF SOLUTIONS

20.1. Ready-Made Products

Icinga version 1.72 shall be used as the core monitoring software of the Accanto Systems monitoring solution. Icinga is open source software and licensed under the GNU General Public Licence Version 2.

20.2. Reusable Components

-

20.3. Products That Can Be Copied

-

21 NEW PROBLEMS

21.1. Effects on the Current Environment

The Icinga monitoring software shall be installed on iCSA or iCEM web server.

21.2. Effects on the Installed Systems

Icinga Core and Classic Web interface shall be installed on monitoring host. Monitoring agents (NRPE and NSClient++) shall be installed on monitored hosts.

21.3. Potential User Problems

System Administrators needs to be trained for Icinga monitoring and maintenance tasks.

21.4. Limitations in the Anticipated Implementation Environment That May Inhibit the New Product

-

21.5. Follow-Up Problems

-

22 TASKS

22.1. Project Planning

N/A

22.2. Planning of the Development Phases

N/A

23 MIGRATION TO THE NEW PRODUCT

23.1. Requirements for Migration to the New Product

N/A

23.2. Data That Has to Be Modified or Translated for the New System

N/A

24 RISKS

Risk1: Limited resources

25 COSTS

There is no budgeted money for this development task. All “costs” are resources that are allocated to this task whenever possible.

26 USER DOCUMENTATION AND TRAINING

26.1. User Documentation Requirements

The product will be delivered with the following documentation:

1. Icinga installation and configuration instructions
2. Monitoring agents installation and configuration instructions
3. Accanto Systems monitoring portal integration instructions
4. Accanto Systems customers remote connection instructions for monitoring portal

26.2. Training Requirements

Installation and configuration training shall be organized for system engineer. Hands on training are needed for support engineers.

27 WAITING ROOM

-

28 IDEAS FOR SOLUTIONS

-