



Monitoring Procedure

Digiplug UMGI Supply Chain Program

Any reproduction, even partial, any transfer to a third in some form that it is, are strictly prohibited without written authorization of Digiplug.

Filename	DIGIPLUG_UMGI_Monitoring_Management_Procedure_1.0.doc	Page 1 of 18
-----------------	---	--------------

STATUS INFORMATION

Security classification:	Confidential	State:	Final
Current version number:	1.0	Date of first issue:	26/02/2008
Prepared by:	Samuel Leucart, Moussa Bagayoko	Date:	07/04/2008
Verified by:	Moulay Younes Alaoui-Rizq	Date:	15/04/2008
Approved by:	Julien Andrieux	Date:	17/04/2008
Copyright notice			
This document may not be reproduced (even partially) or communicated to third parties without the written authorization of the company's General Management.			

DISTRIBUTION LIST

Name	Address	I/A/V
Julien Simon	julien.simon@digiplug.com	V/A
Julien Andrieux	julien.andrieux@digiplug.com	V/A
Digiplug Managers		I/A
IT Operations team		A
Nicolas Tavier	nicolas.tavier@accenture.com	I
Morgan Le Du	morgan.ledu@accenture.com	I
Moussa Bagayoko	moussa.bagayoko@accenture.com	I
Moulay Younes Alaoui Rizq	moulay.y.alaoui-rizq@accenture.com	I
Nourou Dine Issaka	nourou.dine.issaka@accenture.com	I
Nicolas Macaire	nicolas.macaire@accenture.com	I

(I = for information, A = for action, V=for validation)

DOCUMENT CHANGE RECORD

Version	Date	Description	Affected sections
2.0D	26/02/2008	Obsoletes first release 1.0 (called « Monitoring/Propositions diverses »)	All
2.0	03/03/2008	Proofreading	All
0.1	07/04/2008	Re start of the document	All
1.0	23/04/2008	Validated version	All

Any reproduction, even partial, any transfer to a third in some form that it is, are strictly prohibited without written authorization of Digiplug.



IT CONTACT PEOPLE

Function	
IT Lead	Julien Andrieux
IT Consultant	Moulay Younes Alaoui Rizq
IT Consultant	Nourou Dine Issaka



Table of content

1	PURPOSE.....	5
2	MONITORING SOLUTION AND TECHNOLOGY.....	6
2.1	SOLUTION OVERVIEW.....	6
2.2	POLLING TECHNOLOGY: ACTIVE AND PASSIVE CHECKING	7
2.3	MONITORED INDICATORS.....	7
2.4	HIGH-AVAILABILITY	7
2.4.1	Minimal dependencies	7
2.4.2	Failover.....	7
2.5	RELATED PROCEDURES AND DOCUMENTS.....	7
3	SYSTEM MONITORING TEAM.....	8
3.1	TEAM ORGANIZATION.....	8
3.2	RELATED PROCEDURES AND DOCUMENTS.....	8
4	MONITORING ELEMENTS CLASSIFICATION.....	9
4.1	CLASSIFICATION POLICY	9
4.2	RELATED PROCEDURES AND DOCUMENTS.....	9
5	MONITORING OUTPUTS.....	10
5.1	END USER VIEW	10
5.2	NOTIFICATIONS.....	14
5.2.1	Triggers.....	14
5.2.2	Notification classification	14
5.2.3	Notification methods	15
5.2.4	Notification audience	15
5.2.5	Acknowledgement	16
5.3	RELATED PROCEDURES AND DOCUMENTS.....	17
6	SAMPLE SCENARIO.....	18



1 Purpose

The purpose of this document is to present the technology, tools, indicators, procedures and actors associated with the Monitoring Procedure.

A system monitoring Team has been set up to monitor the UMGI Supply Chain Program production platform with the help of supporting tools and technology resources.

The role of the monitoring process is to identify the needs for performance tuning, or for hardware /software / network upgrades or replacements. Monitoring also enables the supervision of the platform and the detection of errors, in order to anticipate and resolve any bugs which could impact service levels. Thus, it facilitates Incident Management.

This documentation assumes that the reader:

- Has a working knowledge of data center concepts and troubleshooting approaches;
- Is familiar with monitoring management strategies, concepts, tools and technologies.

2 Monitoring solution and technology

2.1 Solution overview

The aim of the monitoring solution is to gather up to date, near real-time information needed to anticipate and correct errors, which could have an impact on the SLAs agreed between Digiplug and its clients.

To achieve this, Digiplug dedicates technical and human resources to monitor all aspects of its platform on a 24/7 basis: networks, hardware, systems, software and business services.

Digiplug has set up an infrastructure and a human organization that enables to monitor in a 24/7 basis networks, hardware, systems, software and business services.

The aim is to be permanently informed in order to correct and anticipate errors to meet the SLAs agreed on with its clients.

This means that the monitoring solution must track meaningful indicators such as:

- System status;
- Performance indicators;
- Technical flaw indicators;
- Applications health;
- System load;
- Hardware status;
- Network availability.

The tools used to perform the monitoring are:

- **Nagios (www.nagios.org)**
Nagios is an open source basis solution widely deployed in data centers. It delivers efficient, adaptive and high performance monitoring services.
Using external "plugins" which return status information to Nagios, the monitoring daemon runs periodic checks on hosts and services. When problems are encountered, the daemon sends notifications to administrative contacts through different ways (email, instant message, SMS, etc.). Current status information, historical logs and reports can all be accessed via a web browser.
- **Cacti (www.cacti.net)**
Cacti is a complete graphing solution. Out of the box, Cacti provides a fast polling system, an advanced graph templates, multiple data acquisition methods, and user management features. Cacti will help generating up to date reporting, and besides pure monitoring, the system will collect data, and make it available for performance analysis or capacity planning. For example, this data will be used to:
 - Study and increase the system performance by adding hardware resources where really needed (CPU, RAM...);
 - Locate bottlenecks;
 - Improve overall application performance;
 - Plan storage evolutions.
- **SmokePing (oss.oetiker.ch/smokeping/)**
SmokePing is a complete network latency graphing and monitoring solution, based on RRDTool.
- **Syslog (www.syslog.org)**
Syslog is not really a monitoring tool but it helps Monitoring Team to analyze incident root causes and to audit the platform security.
A centralized Syslog server will be installed. Syslog is supported by a wide variety of devices and receivers across multiple platforms. Thanks to this, Syslog will be used to integrate log data from many different types of systems into a central repository.

Any reproduction, even partial, any transfer to a third in some form that it is, are strictly prohibited without written authorization of Digiplug.

2.2 Polling technology: Active and passive checking

Two checking modes are available in monitoring:

- Active checking consists in regularly sending requests to the monitored system or application to obtain its status.
- Passive checking consists in catching notifications sent by the system or application itself. Passive checking alone is less reliable than active checking, because it relies on the monitored system to get its status.

The checking mode used in the platform is the active mode. The polling frequency is function of the type and criticality of the monitored element or service (*See Operations Excel Spreadsheet*).

The checking protocols are:

- SNMP (Simple Network Management Protocol): SNMP is used in network management systems to monitor devices for conditions that warrant administrative attention.
- ICMP (pings).
- HTTP POST, XML POST, etc., for application-level monitoring

Each monitoring system handles plug-in technologies, enabling IT Operations to develop specific scripts (using either the Perl or C programming languages) in order to perform complex tasks, such as deep application monitoring.

Nagios can also check application logs, but this kind of procedure is heavy to perform and maintain. This kind of monitoring should consequently be rarely used, with a mandatory approval from IT Operations.

2.3 Monitored Indicators

The complete monitored indicators list is detailed in the *Operations Excel Spreadsheet*.

2.4 High-Availability

2.4.1 Minimal dependencies

The monitoring systems must be as standalone as possible. In other words, no dependencies between the monitoring systems and the elements monitored can exist. Monitored systems must be able to continue working even if monitoring elements are down, and vice versa.

2.4.2 Failover

The reliability of the monitoring systems is enhanced by a failover/recovery mechanism. The monitoring system servers are redundant.

2.5 Related Procedures and Documents

- Technical Infrastructure Design
- Capacity & scalability Management (database, file storage, etc.) - Monitoring

3 System monitoring team

3.1 Team Organization

People in charge of monitoring are organized to enable a 24/7 basis supervision.

- 5 administrators are in charge of monitoring. There are always 2 administrators on duty: one primary, one backup.
- During business hours, they can all be notified and be assigned to an incident.
- Outside business hours, a procedure is in place to enable administrators on call to log into the monitoring system through a VPN, wherever they are. They can then perform a deeper diagnosis (for more information, see the Incident Management Procedure).
- Administrators report to the IT Lead for incident escalations.

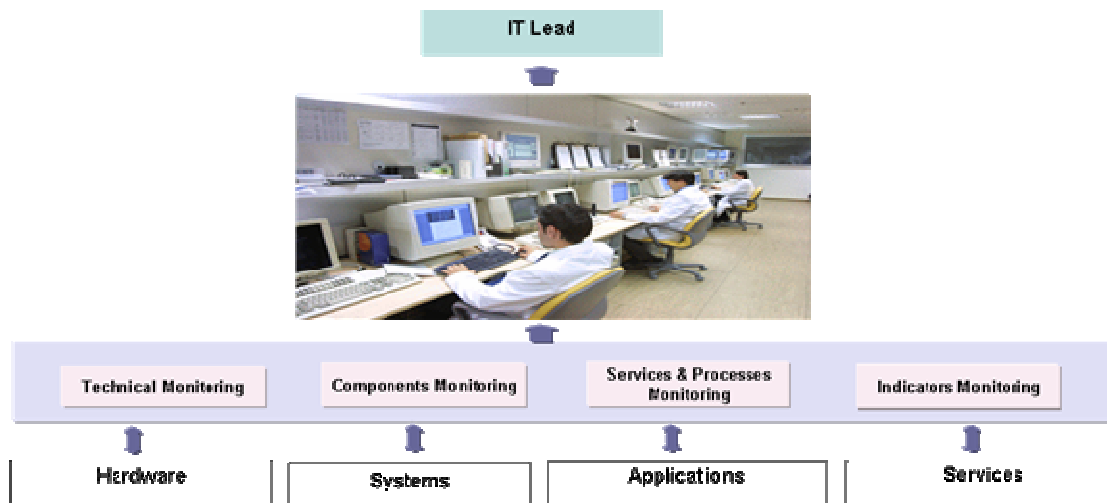


Illustration 1: Team organization

3.2 Related Procedures and Documents

- Incident Management Procedure

4 Monitoring elements classification

4.1 Classification Policy

Once the platform is set up and each time a new device/service is planned to be put in production, the System monitoring team has to identify the Users Request and give a Criticality classification to the element.

Devices/Services are divided into three Criticality categories:

- **Critical**
A device/service which must always be available, i.e. no downtime is acceptable; the failure of this device will affect entire business and application processes.
Examples: Core Routers
- **Major**
A device/service which must be available most of the time; the failure of this device will affect a certain part of a business or application process.
Examples: WAM! Net connection
- **Minor**
A device/service which must be available during business hours, the failure of which will not affect the critical business and application processes during the business hours
Examples: Router degradation in performance or outages that have no impact on users.

The systems monitoring team has to:

- Identify the list of parameters or services to be monitored and assign them a criticality level.
- Add the device and its related service to the list of monitored parameters.
- Coordinate with the Requester to configure a new device/service, so that it is appropriately monitored, with the right thresholds.
- Monitor devices and prepare monitoring reports.
- Provide and maintain a dashboard.

4.2 Related Procedures and Documents

- Operations Excel Spreadsheet
- Data Classification

5 Monitoring outputs

Monitoring data is accessible in two ways:

- Front-end user views to present real-time status of the platform,
- Alerts and notifications from the systems to the Operations Team.

5.1 End user view

Nagios and Cacti provide different screens to administrators, which display real-time status of the platform. A few illustrations of these views are shown below.

Note: When needed, administrators can browse more specific screens for a deeper investigation.

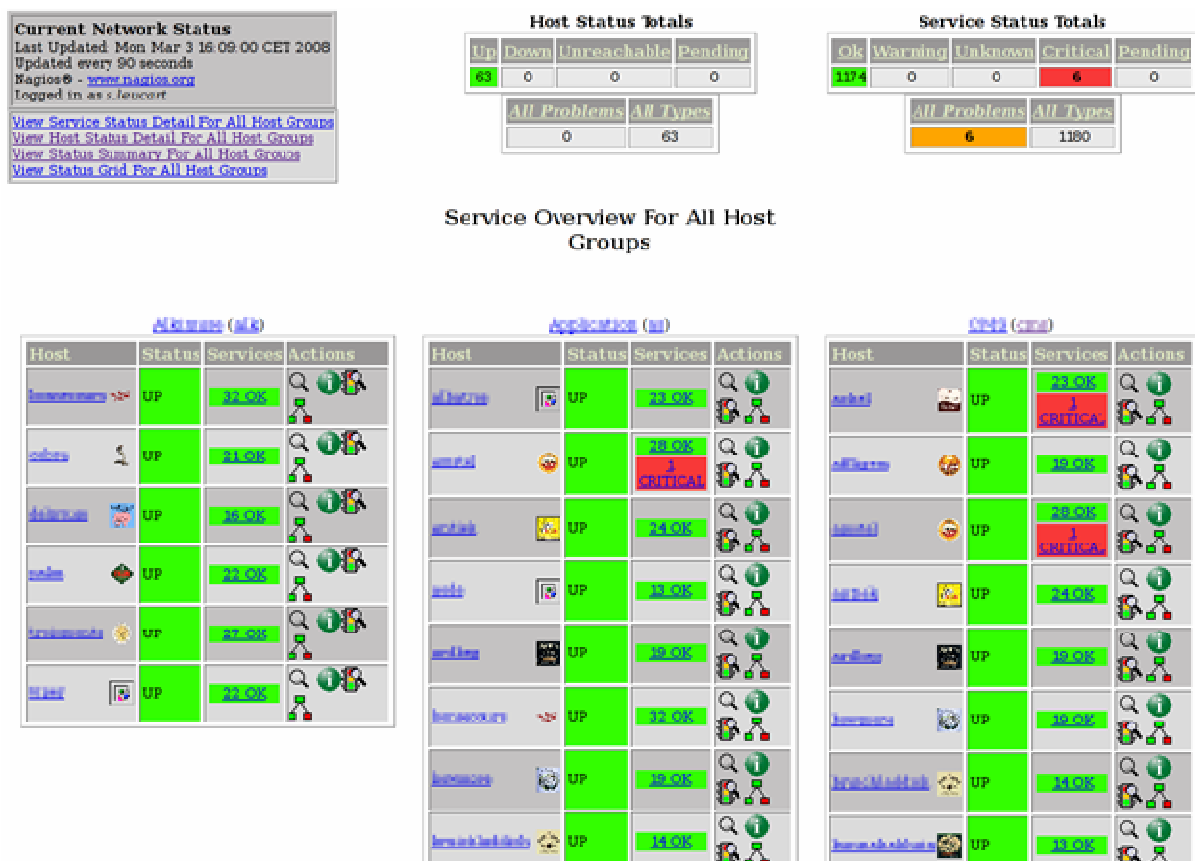


Illustration 2: End user front view in Nagios

Service Status Details For Host 'lamiek'
























Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
stable 	/procnt : avail : used 	OK 	01-03-2008 16:02:23	109d 4h 22m 2s	1/2	SNMP OK - 25389381 122153
	/boot procnt : avail : used 	OK 	01-03-2008 16:02:29	109d 4h 21m 40s	1/2	SNMP OK - 9 215416 20029
	/logs procnt : avail : used 	OK 	01-03-2008 16:02:34	109d 4h 21m 41s	1/2	SNMP OK - 28 626296 146538
	/opt procnt : avail : used 	OK 	01-03-2008 16:02:39	109d 4h 21m 29s	1/2	SNMP OK - 73 64309 116455
	/servers procnt : avail : used 	OK 	01-03-2008 16:02:52	109d 4h 21m 20s	1/2	SNMP OK - 51 236369 245165
	/spool procnt : avail : used 	OK 	01-03-2008 16:00:11	109d 4h 21m 4s	1/2	SNMP OK - 0 53817455 66316
	/tmp procnt : avail : used 	OK 	01-03-2008 16:00:51	109d 4h 21m 0s	1/2	SNMP OK - 34 319711 151823
	/var procnt : avail : used 	OK 	01-03-2008 16:01:01	109d 4h 23m 47s	1/2	SNMP OK - 27 1427624 631628
	/var procnt : avail : used 	OK 	01-03-2008 16:01:06	66d 21h 59m 55s	1/2	SNMP OK - 17 401757 79777
	CPU idle : user : sys 	OK 	01-03-2008 16:01:22	109d 4h 23m 39s	1/2	SNMP OK - 99 0 0
	CPU load 	OK 	01-03-2008 16:01:05	109d 4h 23m 28s	1/2	SNMP OK - 1
	Ecart avec l'heure de lamiek 	OK 	01-03-2008 16:02:02	109d 4h 21m 18s	1/3	ecart de temps OK - 0
	INGESTION_CMS_DGP 	OK 	01-03-2008 16:01:21	5d 1h 22m 58s	1/2	HTTP OK HTTP/1.1 200 OK - 125624 bytes in 0.039 seconds
	Memory available procnt : kb 	OK 	01-03-2008 16:02:03	109d 4h 20m 57s	1/3	SNMP OK - 21 840512
	PING	OK 	01-03-2008 15:58:16	345d 10h 55m 15s	1/4	PING OK - Packet loss = 0%, RTA = 0.21 ms

Illustration 3: Service Status for a host in Nagios

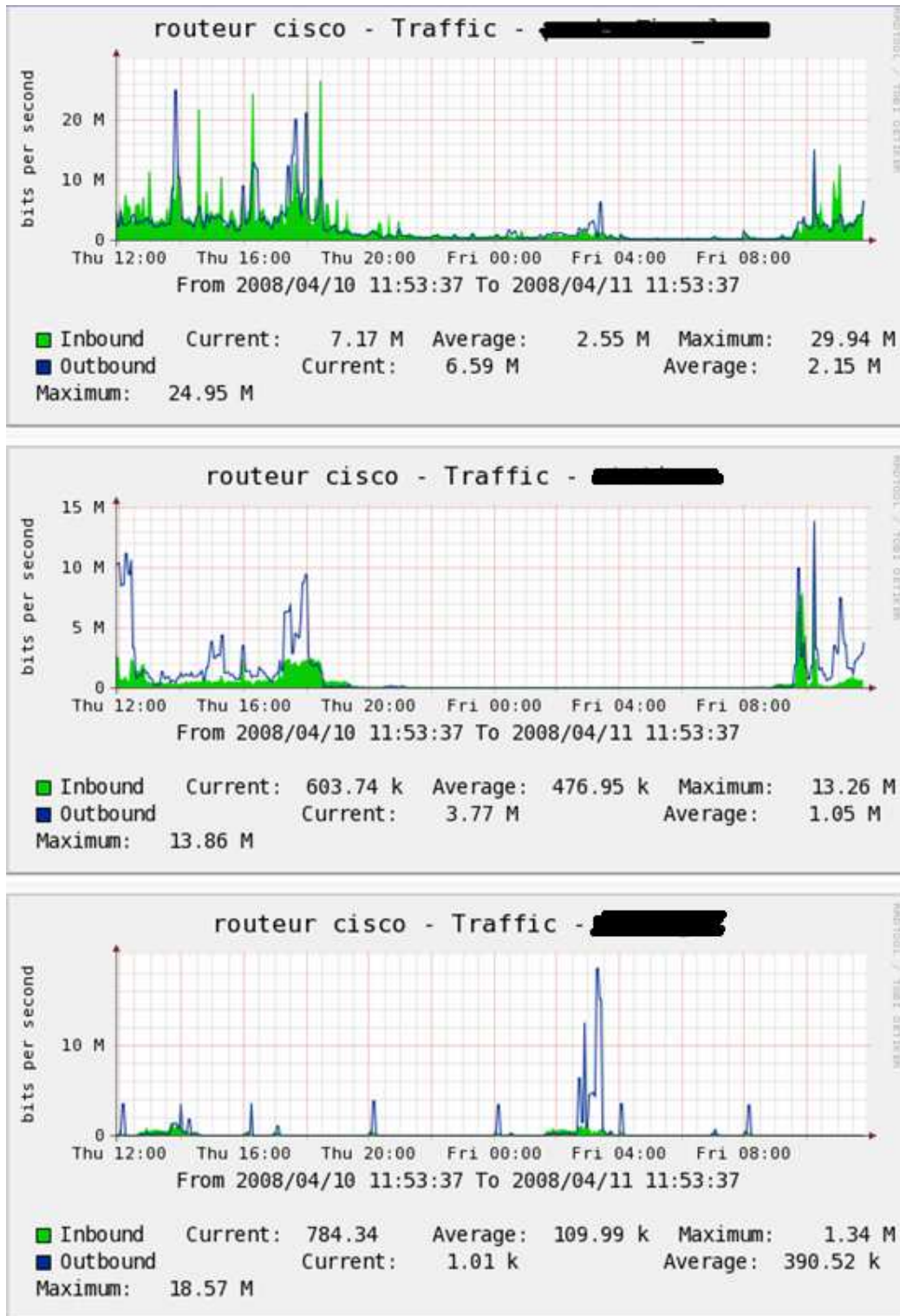


Illustration 4: Graphic view of a host in Cacti

Any reproduction, even partial, any transfer to a third in some form that it is, are strictly prohibited without written authorization of Digiplug.

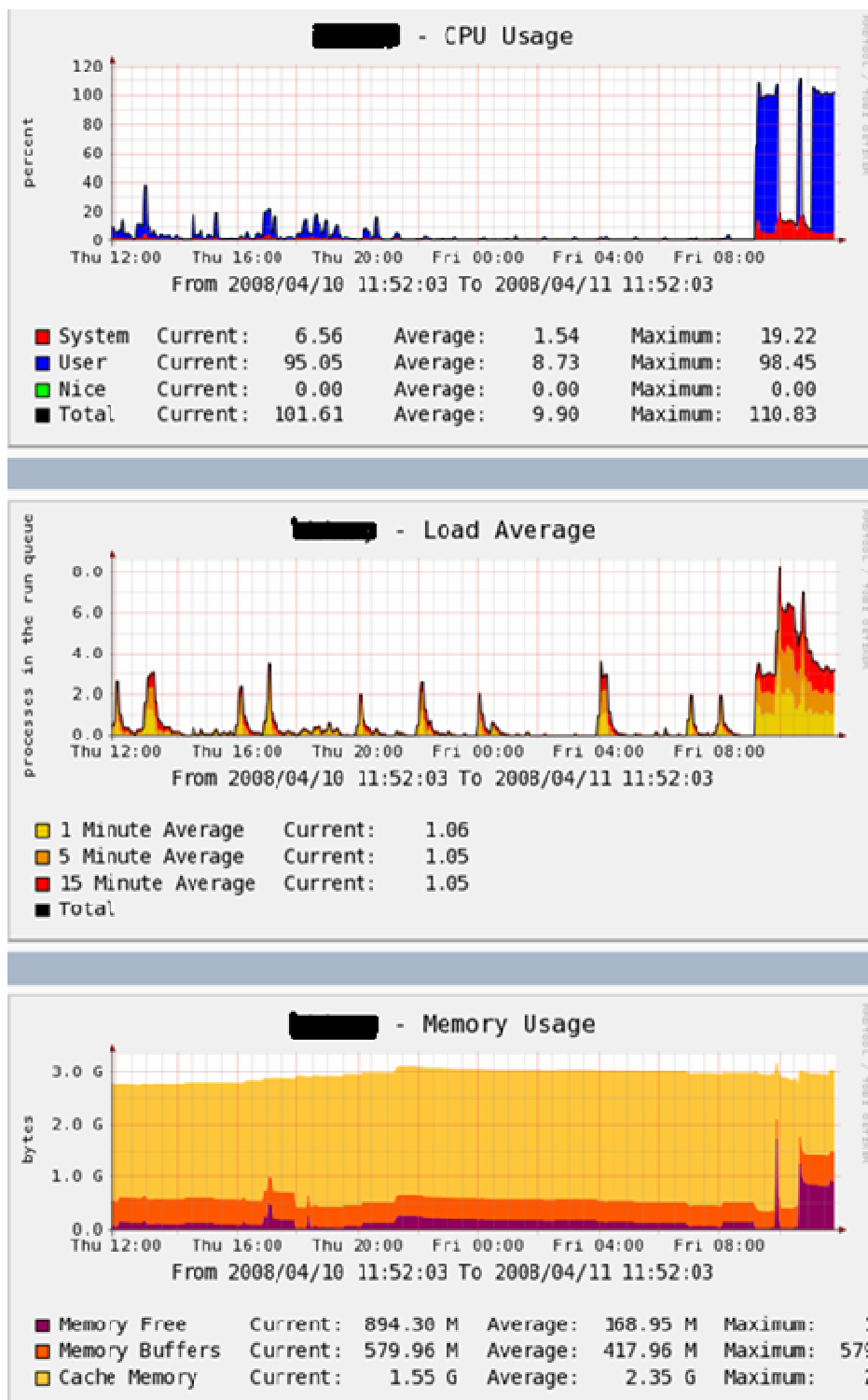


Illustration 5: Graphic view of services in Cacti

Any reproduction, even partial, any transfer to a third in some form that it is, are strictly prohibited without written authorization of Digiplug.

5.2 Notifications

The systems can send notifications to the Operations Team when necessary, on a 24/7 basis.

5.2.1 Triggers

Different events can trigger an alert when:

- A threshold is reached (for warning, critical states...);
- An application process is working;
- A system is down;
- Some hardware fails.

Alerts are used to perform an impact analysis and to quickly find out the root cause of the incident.

5.2.2 Notification classification

During its regular polling of monitored elements, the monitoring system collects the status of monitored elements and sends alerts if needed. These notifications contain the state of the monitored element, including:

- Failure state;
- Recovery state;
- Unknown state;
- Warning state.

According to the state, the monitoring system computes the impact of the error and automatically selects the notification methods and audience. The alert can be:

- A critical error with an important impact on business.
- A warning for errors with a limited impact on business which still need to be corrected before they get worse.

(See Operations Excel Spreadsheet for more details).

Service Information
 Last Updated: Mon Mar 3 16:10:05 CET 2008
 Updated every 90 seconds
 Nagios® - www.nagios.org
 Logged in as s.leucourt

[View Information For This Host](#)
[View Status Detail For This Host](#)
[View Alert History For This Service](#)
[View Trends For This Service](#)
[View Alert Histogram For This Service](#)
[View Availability Report For This Service](#)
[View Notifications For This Service](#)

Service
Process nsd running :
 amount
 On Host
FTP
 (critical)

Member of
sysService, system

achol


 Extra Service Notes

Service State Information	Service Commands
Current Status: CRITICAL (Has been acknowledged)	Disable active checks of this service
Status Information: SNMP CRITICAL - *1* 0	Re-schedule the next check of this service
Performance Data: UCD-SNMP-MIB::prErrorFlag.4= 1	Start accepting passive checks for this service
UCD-SNMP-MIB::prCount.4= 0	Stop obsessing over this service
Current Attempt: 2/2	Remove problem acknowledgement
State Type: HARD	Disable notifications for this service
Last Check Type: ACTIVE	Delay next service notification
Last Check Time: 03-03-2008 16:08:04	Schedule downtime for this service
Status Data Age: 0d 0h 2m 1s	Disable event handler for this service
Next Scheduled Active Check: 03-03-2008 16:11:04	Disable flap detection for this service
Latency: 0.165 seconds	
Check Duration: 0.166 seconds	
Last State Change: 12-31-2007 10:37:54	
Current State Duration: 63d 5h 32m 11s	
Last Service Notification: 12-31-2007 10:39:59	
Current Notification Number: 1	
Is This Service Flapping? N/A	
Percent State Change: N/A	
In Scheduled Downtime? NO	
Last Update: 03-03-2008 16:10:03	

Illustration 6: Service detailed status

5.2.3 Notification methods

The notification methods are:

- E-mail
- SMS

E-mails and SMS are automatically sent by the monitoring system to a predefined list of people. The frequency is each time an error is detected. Several group lists can be configured.

5.2.4 Notification audience

Based on the notification classification, an e-mail or SMS is automatically sent to:

- The monitoring team
- The administrator who is on call
- Other(s) administrator(s) if the first one has not acknowledged the notification

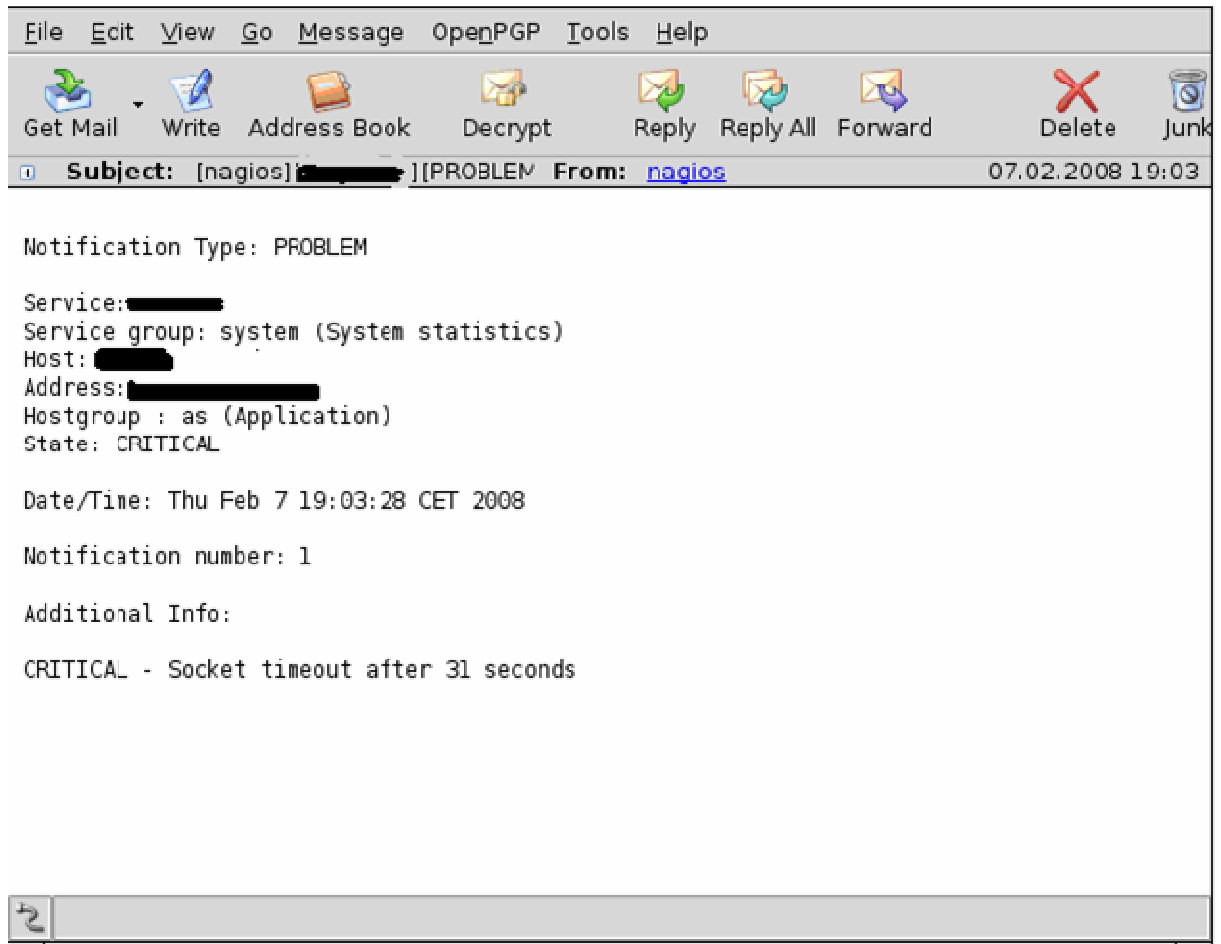


Illustration 7: Mail Notification

5.2.5 Acknowledgement

Once an alert notification has been received, the administrator acknowledges the alert and logs the incident into the incident tracking system.

This guarantees that the incident has been taken into account.

At the end of the intervention, the administrator updates the resolution information.

Service Comments

 [Add a new comment](#)

 [Delete all comments](#)



Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
02-27-2008 20:56:47	ajacart	je regarde...	3117	Yes	Acknowledgement	N/A	
01-21-2008 15:34:03	ajacart	instance chargee, mais neanmoins fonctionnelle - a surveiller	2172	Yes	Acknowledgement	N/A	

Illustration 8: Acknowledgement HMI

Any reproduction, even partial, any transfer to a third in some form that it is, are strictly prohibited without written authorization of Digiplug.

Astreintes

[nagios][REDACTED][PROBLEM]

FRONT1 [REDACTED] DGP is CRITICAL

Created: 08/Feb/08 01:35 PM

Updated: 08/Feb/08 01:35 PM

Return to search

Issue 2 of 16 issue(s)

<< Previous | ASTR-2 | Next >>

Component/s: None

Affects

Version/s: None

Fix Version/s: None

Original Estimate:	Unknown	Remaining Estimate:	Unknown	Time Spent:	Unknown
--------------------	---------	---------------------	---------	-------------	---------

date de début d'intervention:	07/Feb/08 07:15 PM
date de fin d'intervention:	07/Feb/08 07:45 PM

Description

= Hide

Notification Type: PROBLEM

Service: [REDACTED]

Service group: system (System statistics)

Host: [REDACTED]

Address: [REDACTED]

Hostgroup : as (Application)

State: CRITICAL

Date/Time: Thu Feb 7 19:15:22 CET 2008

Notification number: 3

Additional Info:

CRITICAL - Socket timeout after 31 seconds

Action: Arrêt et redémarrage du front.

Durée d'intervention: 30mn

Illustration 9: Intervention report

5.3 Related Procedures and Documents

- Incident Management Procedure

6 Sample scenario

The example below illustrates a possible scenario:

- An error (hardware, network, service, etc.) is monitored on a server
- The monitoring system analyzes the error, applies predefined rules based on its source and the services impacted, and notifies the appropriate people.
- An alert is displayed on the monitoring screens, an SMS and an e-mail are also sent to the monitoring administrators (during business hours).
- An alert is displayed on the monitoring screens, an SMS and an e-mail are sent to the administrator on call (outside business hours).
- If the monitoring system categorizes the error as critical, an escalation process is followed by the administrator on call to alert Digiplug management, who can then take additional measures (customer communication, etc).

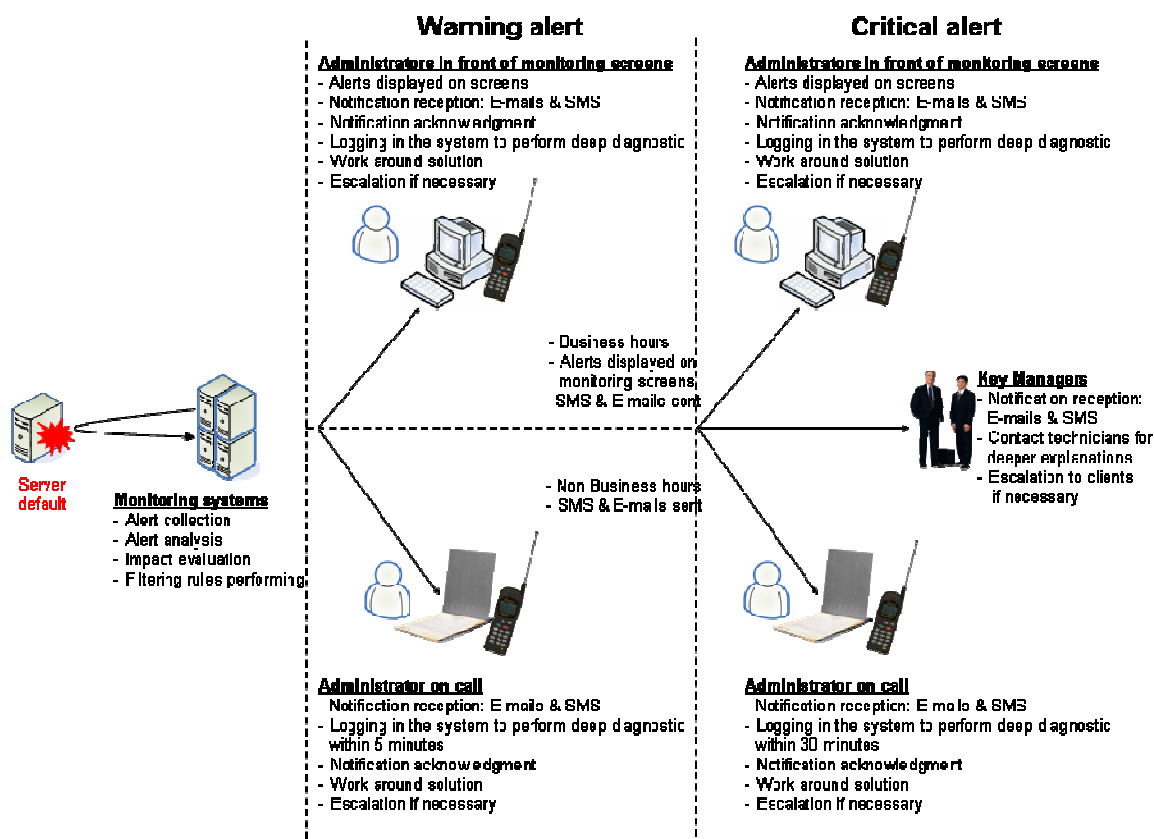


Illustration 10: Notification procedure