Minimierung ungeplanter Downtimes

4. Secure Linux Administration Conference

10. Dezember 2009

Bernd Strößenreuther

Sparda-Datenverarbeitung eG

Sparda-Datenverarbeitung eG

- IT-Dienstleister
  - der Sparda Banken deutschlandweit (http://www.sparda.de) und
  - der Netbank (http://www.netbank.de)
- Gegründet 1983
- derzeit ca. 350 Mitarbeiter
- 2 Rechenzentren
- Sitz in Nürnberg

Minimierung ungeplanter Downtimes: Warum?

- IT-Systeme gewinnen eine immer größere Bedeutung für immer mehr Bereiche unseres Lebens
- Erwartungshaltung der Nutzer steigt
- SLAs / Zielvereinbarungen

Level 1

- Kunde ruft an, wenn er ein Problem hat

Level 2: Monitoring

- End-to-End-Monitoring
  - Info über Störung vorhanden
  - Keine Information über die verursachende Komponente
  - Ursachenforschung zeitaufwändig oder über Erfahrung des Admin
- Komponenten-Monitoring
  - Einfache Liste aller Komponenten
  - Keine Aussage, ob Anwendungen für den Kunden zur Verfügung stehen
  - Keine Zuordnung von Komponenten zu Anwendungen
  - Keine Priorisierung

Level 3: Bessere Kundenorientierung

- Proaktives Monitoring
  - Messwerte werden über die Zeit aufgetragen
  - Eingriff bevor es zu Auswirkungen für den Kunden kommt
  - Redundanzverluste werden erkannt
- Verknüpfung von Komponenten zu Anwendungen
- Priorisierung von Anwendungen
- Links vom Monitoring zur Doku

Dokumentation: Warum?

- The system is the documentation
- Generally avoid comments. If Your software needs comments to be understood, better rewite it.
- Dick Brandon:
  “Documentation is like Sex:
  When it is good, it is very, very good.
  And when it is bad, it is better than nothing.”
- Je mehr Admins, je komplexer die Anwendungen und je höher die geforderte Verfügbarkeit, desto sinnvoller ist wirklich gute und aktuelle Betriebs- und Notfall-Dokumentation

Das Problem mit der Dokumentation

- Erstellung einer Betriebs- und Notfall-Dokumentation klappt oft noch
- Aktualisierung nicht
- Ergebnis: Doku wird bei Ausfall nicht genutzt, da veraltete Doku schlechter ist als gar keine
- Compliance ≠ beste Verfügbarkeit

Der Informatiker-Ansatz

- Modularisierung
- Wiederverwendung
- Redundanzen vermeiden
- Zusamenfassen

Blickrichtungen auf IT-Systeme

- Anwendung
  - User beschweren sich über lange Antwortzeiten und Verbindungsabbrüche im Webshop
  - User kann keine Mails mehr versenden
- Komponente
  - JBoss-Instanz X verursacht plötzlich 100% CPU-Auslastung
  - Mehr als 1.000 Mail in der Mail-Queue von Postfix auf SMTP-Relay
- Maschine
  - Hardware-Defekt auf Server Y
  - Server Z bootet nach Kernel-Update (Sicherheitspatch) nicht mehr

Betriebsdokumentation je Anwendung

- In vielen Fällen schon vorhanden
- Administrations- / Anwenderdoku auslagern, insgesamt deutlich verschlanken
- Übersichtsschaubild aus Admin-Sicht
  - Hostnames / Ports / Protokolle
  - active - active oder failover
- je Komponente eine Bildschirmseite mit wichtigsten Infos
- Links auf Komponenten-Dokus
- Wenn mehrere Anwendungen weitgehend die gleiche Infrastruktur nutzen, Dokus zusammenfassen
- Einheitliche Gliederung für alle Betriebsdokus

Doku je Komponente

- Apache, JBoss, Postfix, …
- Allgemeingültig beschreiben, sodass die Beschreibung auf möglichst alle Instanzen passt
- Restart, Logfiles, …
- Übliche Fragestellungen
  - Wie finde ich heraus, warum Mails nicht zugestellt werden?
  - Connection-Problem (IP)?
  - Annahme verweigert?
  - Ist mein Server auf einer Spam-Blacklist?
- Einheitliche Gliederung für alle Komponentendokus

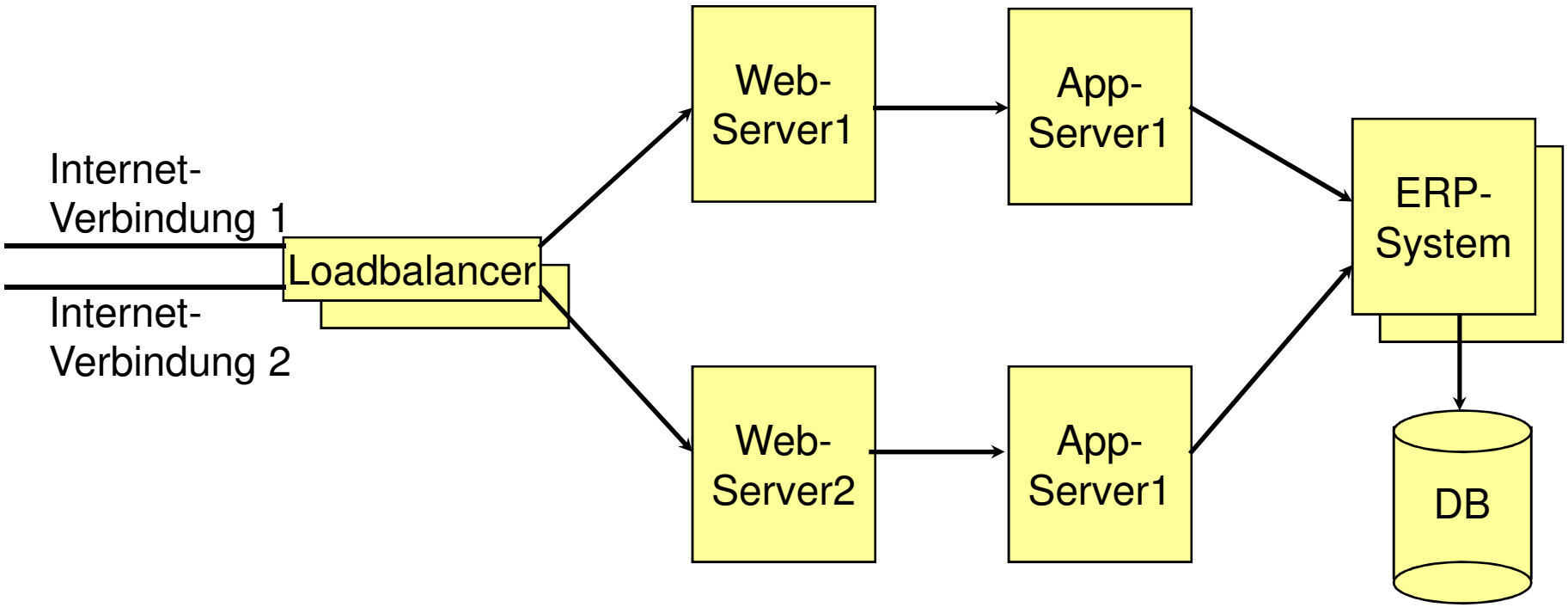
Dokumentation je Maschine

- Inventar-Datenbank
  - Standort
  - Grobe Hardware-Information
- Ansonsten keine separate Doku
  - Monitoring-System bildet Maschinen-Doku vollständig ab

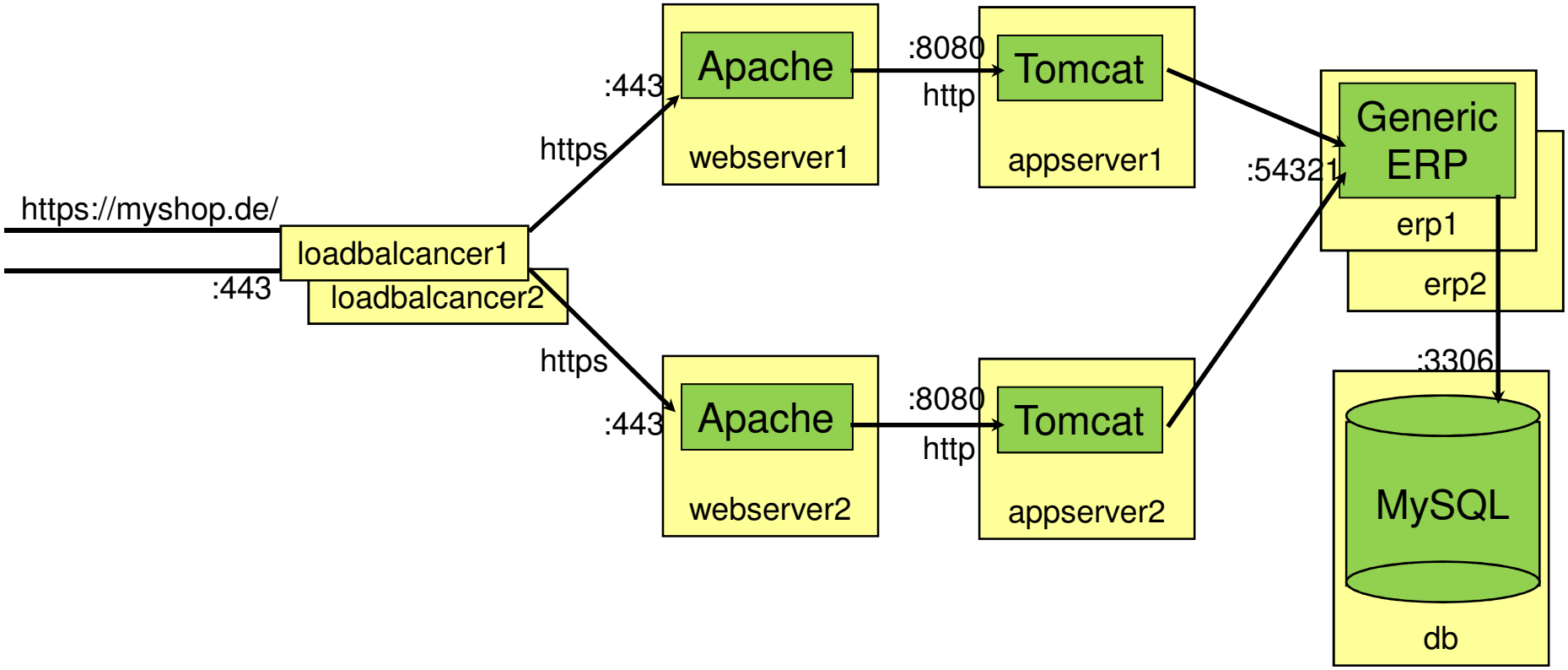
Das Monitoring-System

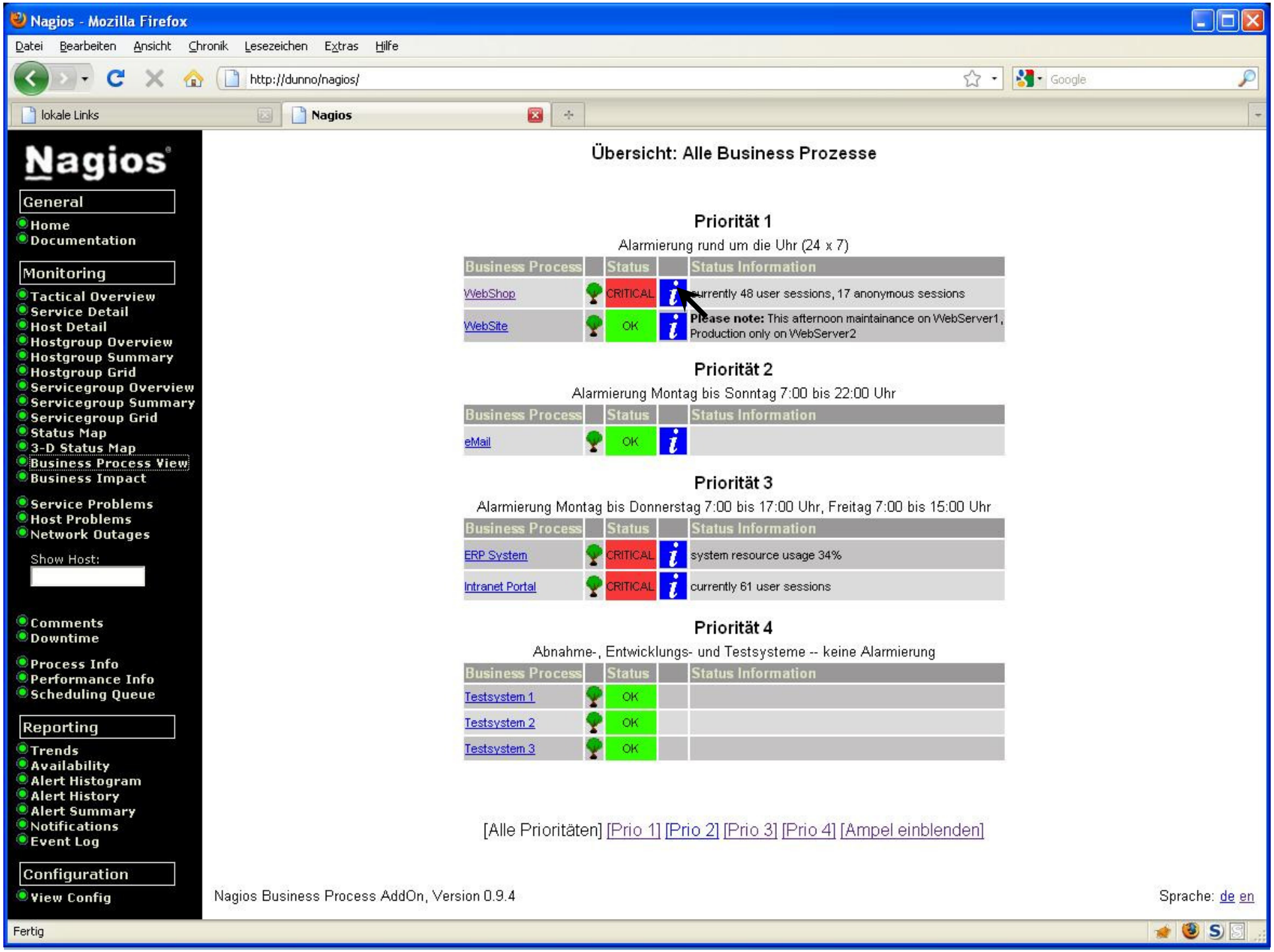
- Komponenten-Monitoring aller beteiligter Komponenten
- Verknüpfung zu Geschäftsprozessen
- Drill down / root-cause Analyse

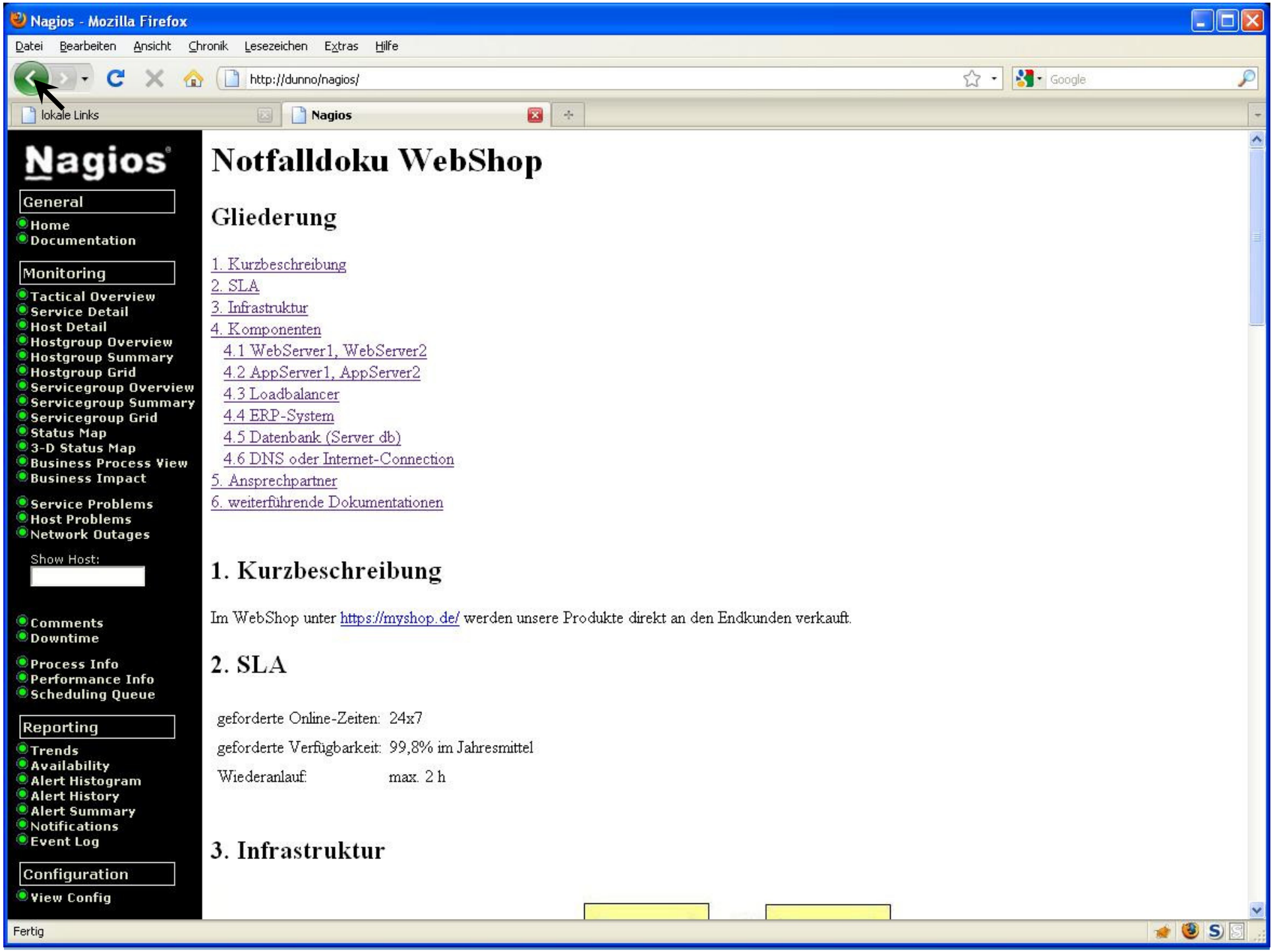
Beispiel-Anwendung: WebShop

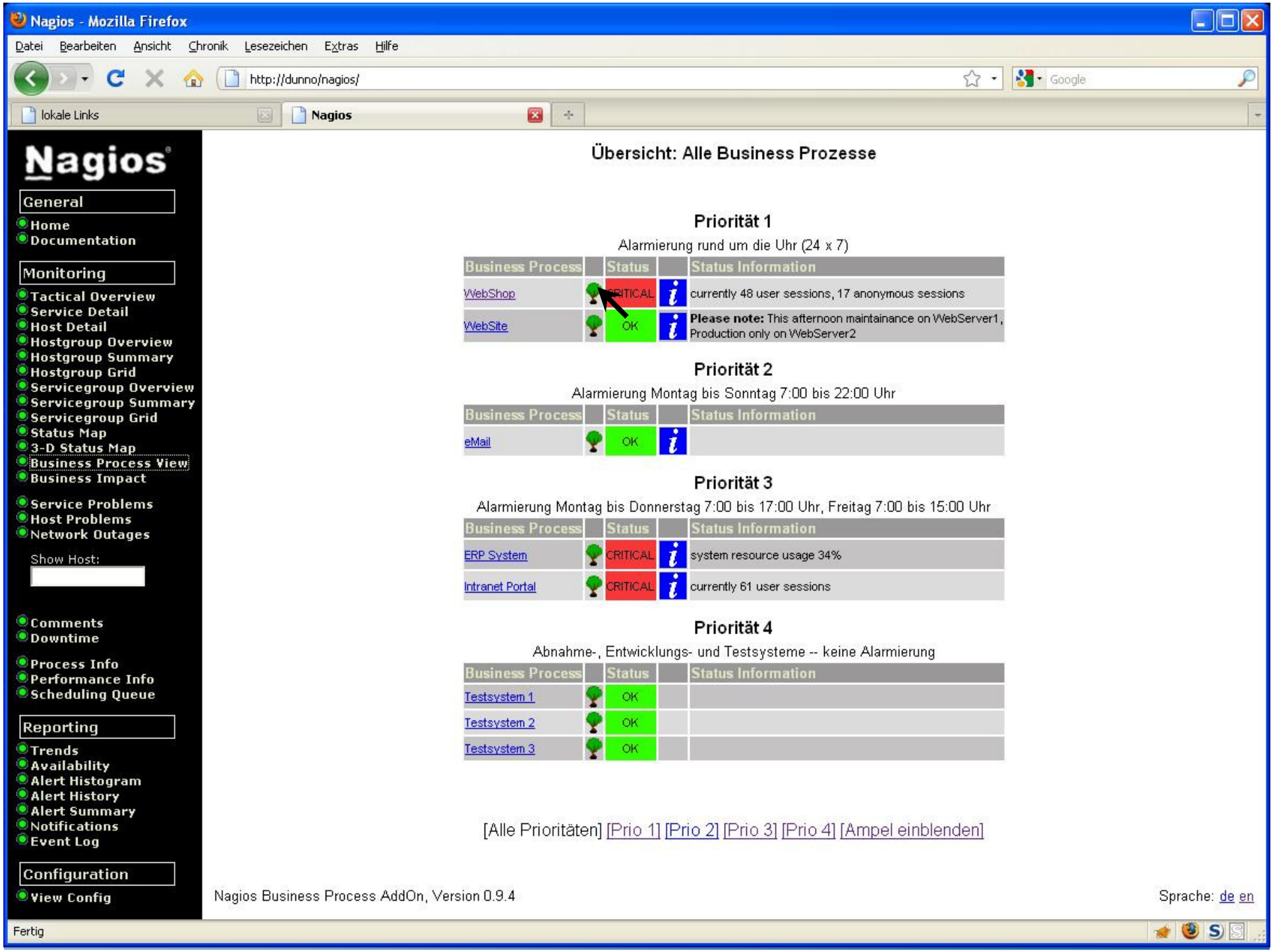


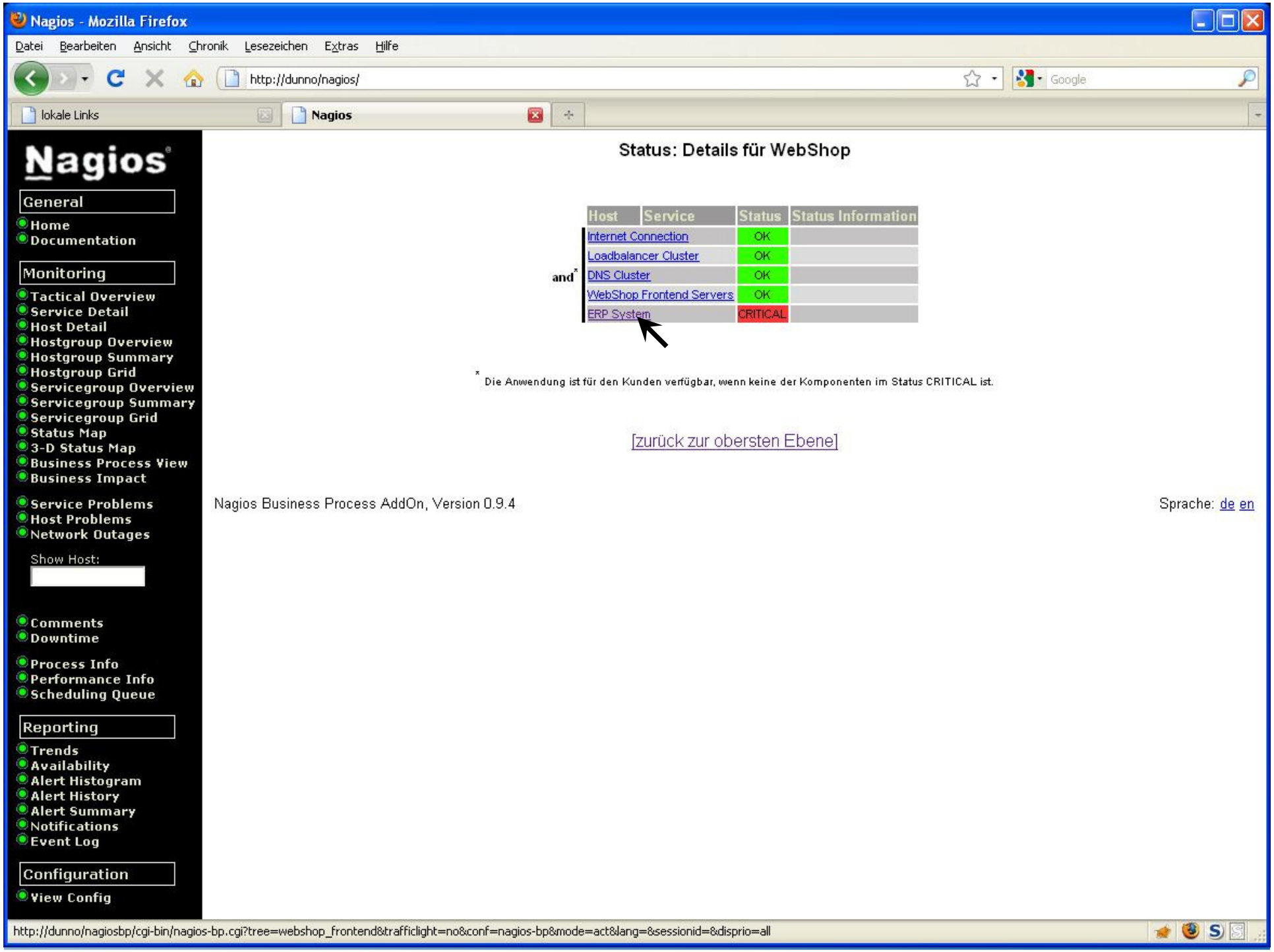
Beispiel-Anwendung: WebShop – Admin-View

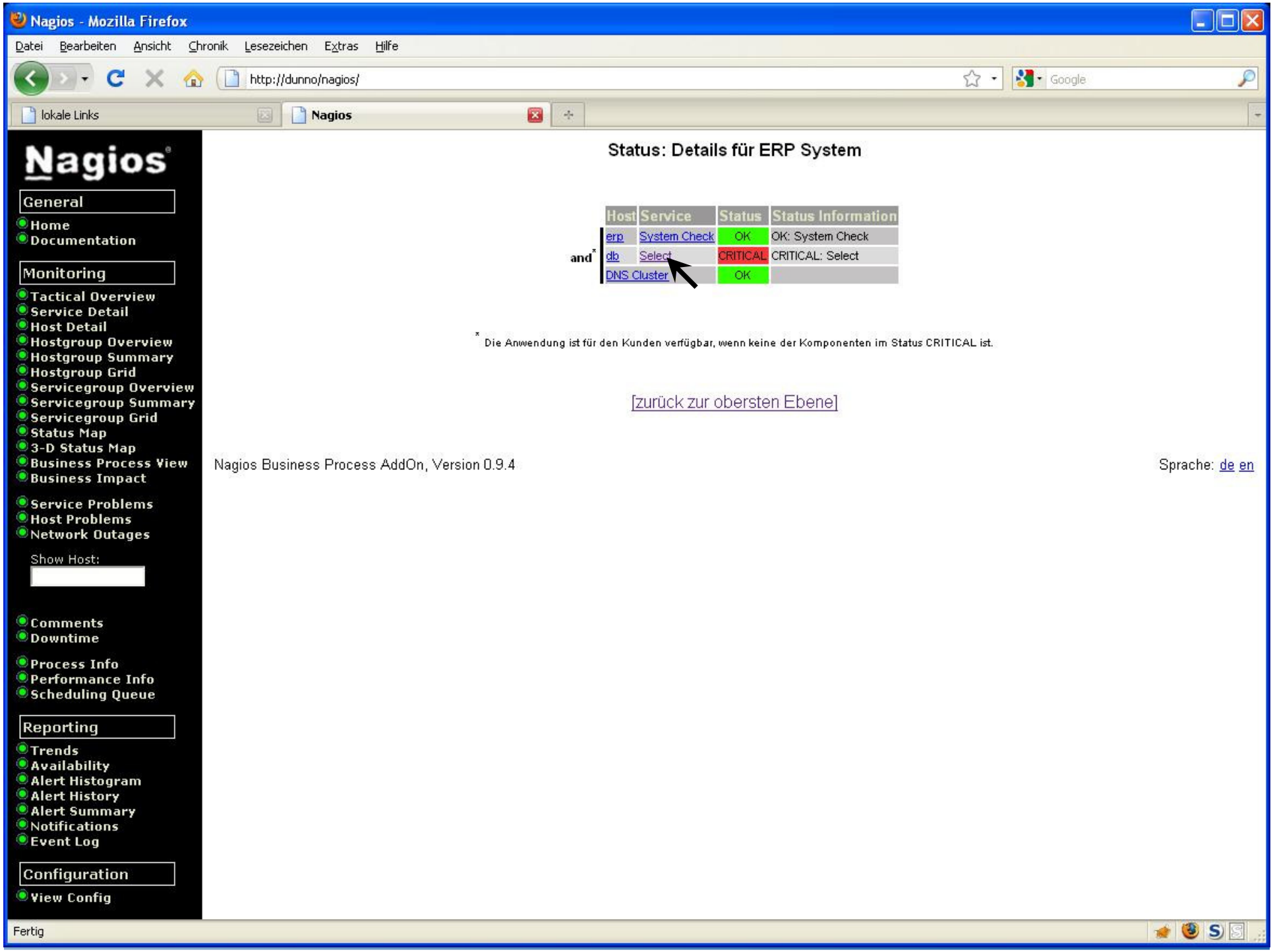



Nagios - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://dunno/nagios/
lokale Links
Nagios
Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Hostgroup Overview
Hostgroup Summary
Hostgroup Grid
Servicegroup Overview
Servicegroup Summary
Servicegroup Grid
Status Map
3-D Status Map
Business Process View
Business Impact
Service Problems
Host Problems
Network Outages
Show Host:
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
Event Log
Configuration
View Config
Übersicht: Alle Business Prozesse
Priorität 1
Alarmierung rund um die Uhr (24 x 7)
Business Process
Status
Status Information
WebShop
CRITICAL
currently 48 user sessions, 17 anonymous sessions
WebSite
OK
Please note: This afternoon maintainance on WebServer1, Production only on WebServer2
Priorität 2
Alarmierung Montag bis Sonntag 7:00 bis 22:00 Uhr
Business Process
Status
Status Information
eMail
OK
Priorität 3
Alarmierung Montag bis Donnerstag 7:00 bis 17:00 Uhr, Freitag 7:00 bis 15:00 Uhr
Business Process
Status
Status Information
ERP System
CRITICAL
system resource usage 34%
Intranet Portal
CRITICAL
currently 61 user sessions
Priorität 4
Abnahme-, Entwicklungs- und Testsysteme -- keine Alarmierung
Business Process
Status
Status Information
Testsystem 1
OK
Testsystem 2
OK
Testsystem 3
OK
[Alle Prioritäten] [Prio 1] [Prio 2] [Prio 3] [Prio 4] [Ampel einblenden]
Nagios Business Process AddOn, Version 0.9.4
Sprache: de en
Fertig


Nagios - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://dunno/nagios/
Google
lokale Links
Nagios
Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Hostgroup Overview
Hostgroup Summary
Hostgroup Grid
Servicegroup Overview
Servicegroup Summary
Servicegroup Grid
Status Map
3-D Status Map
Business Process View
Business Impact
Service Problems
Host Problems
Network Outages
Show Host:
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
Event Log
Configuration
View Config
Notfalldoku WebShop
Gliederung
1. Kurzbeschreibung
2. SLA
3. Infrastruktur
4. Komponenten
4.1 WebServer1, WebServer2
4.2 AppServer1, AppServer2
4.3 Loadbalancer
4.4 ERP-System
4.5 Datenbank (Server db)
4.6 DNS oder Internet-Connection
5. Ansprechpartner
6. weiterführende Dokumentationen
1. Kurzbeschreibung
Im WebShop unter https://myshop.de/ werden unsere Produkte direkt an den Endkunden verkauft.
2. SLA
geforderte Online-Zeiten: 24x7
geforderte Verfügbarkeit: 99,8% im Jahresmittel
Wiederanlauf: max. 2 h
3. Infrastruktur
Fertig


Nagios - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://dunno/nagios/
Google
lokale Links
Nagios
Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Hostgroup Overview
Hostgroup Summary
Hostgroup Grid
Servicegroup Overview
Servicegroup Summary
Servicegroup Grid
Status Map
3-D Status Map
Business Process View
Business Impact
Service Problems
Host Problems
Network Outages
Show Host:
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
Event Log
Configuration
View Config
Übersicht: Alle Business Prozesse
Priorität 1
Alarmierung rund um die Uhr (24 x 7)
Business Process
Status
Status Information
WebShop
CRITICAL
currently 48 user sessions, 17 anonymous sessions
WebSite
OK
Please note: This afternoon maintainance on WebServer1, Production only on WebServer2
Priorität 2
Alarmierung Montag bis Sonntag 7:00 bis 22:00 Uhr
Business Process
Status
Status Information
eMail
OK
Priorität 3
Alarmierung Montag bis Donnerstag 7:00 bis 17:00 Uhr, Freitag 7:00 bis 15:00 Uhr
Business Process
Status
Status Information
ERP System
CRITICAL
system resource usage 34%
Intranet Portal
CRITICAL
currently 61 user sessions
Priorität 4
Abnahme-, Entwicklungs- und Testsysteme -- keine Alarmierung
Business Process
Status
Status Information
Testsystem 1
OK
Testsystem 2
OK
Testsystem 3
OK
[Alle Prioritäten] [Prio 1] [Prio 2] [Prio 3] [Prio 4] [Ampel einblenden]
Nagios Business Process AddOn, Version 0.9.4
Sprache: de en
Fertig


Nagios - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://dunno/nagios/
Google
lokale Links
Nagios
Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Hostgroup Overview
Hostgroup Summary
Hostgroup Grid
Servicegroup Overview
Servicegroup Summary
Servicegroup Grid
Status Map
3-D Status Map
Business Process View
Business Impact
Service Problems
Host Problems
Network Outages
Show Host:
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
Event Log
Configuration
View Config
Status: Details für WebShop
Host
Service
Status
Status Information
and*
Internet Connection
OK
Loadbalancer Cluster
OK
DNS Cluster
OK
WebShop Frontend Servers
OK
ERP System
CRITICAL
* Die Anwendung ist für den Kunden verfügbar, wenn keine der Komponenten im Status CRITICAL ist.
[zurück zur obersten Ebene]
Nagios Business Process AddOn, Version 0.9.4
Sprache: de en
http://dunno/nagiosbp/cgi-bin/nagios-bp.cgi?tree=webshop_frontend&trafficlight=no&conf=nagios-bp&mode=act&lang=&sessionid=&disprio=all


Nagios - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://dunno/nagios/
Google
lokale Links
Nagios
Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Hostgroup Overview
Hostgroup Summary
Hostgroup Grid
Servicegroup Overview
Servicegroup Summary
Servicegroup Grid
Status Map
3-D Status Map
Business Process View
Business Impact
Service Problems
Host Problems
Network Outages
Show Host:
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
Event Log
Configuration
View Config
Status: Details für ERP System
Host
Service
Status
Status Information
erp
System Check
OK
OK: System Check
and*
db
Select
CRITICAL
CRITICAL: Select
DNS Cluster
OK
* Die Anwendung ist für den Kunden verfügbar, wenn keine der Komponenten im Status CRITICAL ist.
[zurück zur obersten Ebene]
Nagios Business Process AddOn, Version 0.9.4
Sprache: de en
Fertig

Nagios - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

http://dunno/nagios/

lokale Links | Nagios

Nagios

General
- Home
- Documentation

Monitoring
- Tactical Overview
- Service Detail
- Host Detail
- Hostgroup Overview
- Hostgroup Summary
- Hostgroup Grid
- Servicegroup Overview
- Servicegroup Summary
- Servicegroup Grid
- Status Map
- 3-D Status Map
- Business Process View
- Business Impact
- Service Problems
- Host Problems
- Network Outages

Show Host:

- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue

Reporting
- Trends
- Availability
- Alert Histogram
- Alert History
- Alert Summary
- Notifications
- Event Log

Configuration
- View Config

Service Information
Last Updated: Mon Dec 7 18:29:19 CET 2009
Updated every 30 seconds
Nagios® - www.nagios.org
Logged in as *u00stro*

View Information For This Host
View Status Detail For This Host
View Alert History For This Service
View Availability Report For This Service
View Notifications For This Service

Service
Select
On Host
db
(db)

Member of
No servicegroups.

127.0.0.1

(siehe Betriebsdoku, Kapitel ERP)

Wenn hier Probleme gemeldet werden,
siehe Betriebsdoku ERP, Abschnitt Datenbank
Wo wird diese Komponente verwendet?

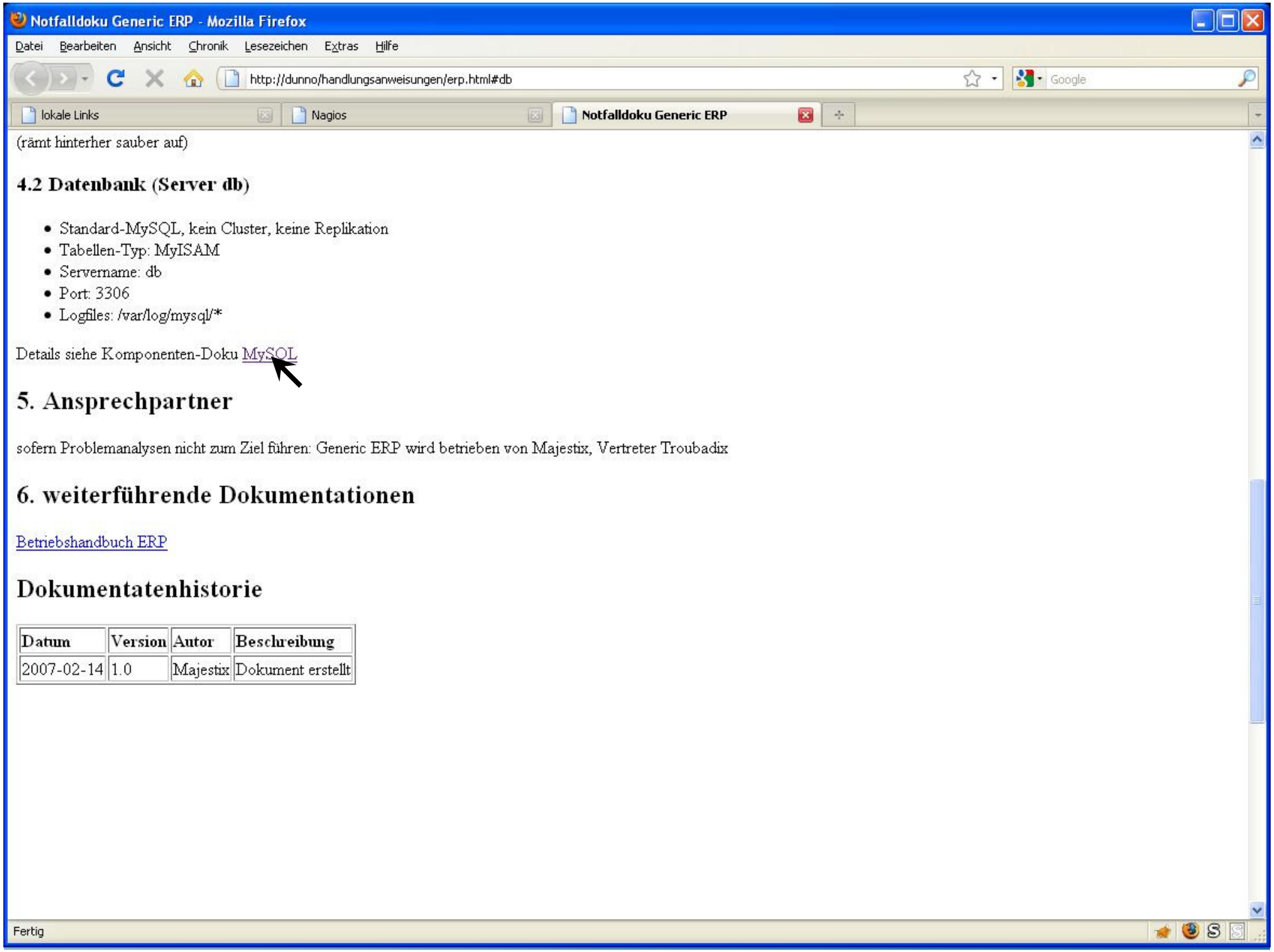
Extra Service Actions

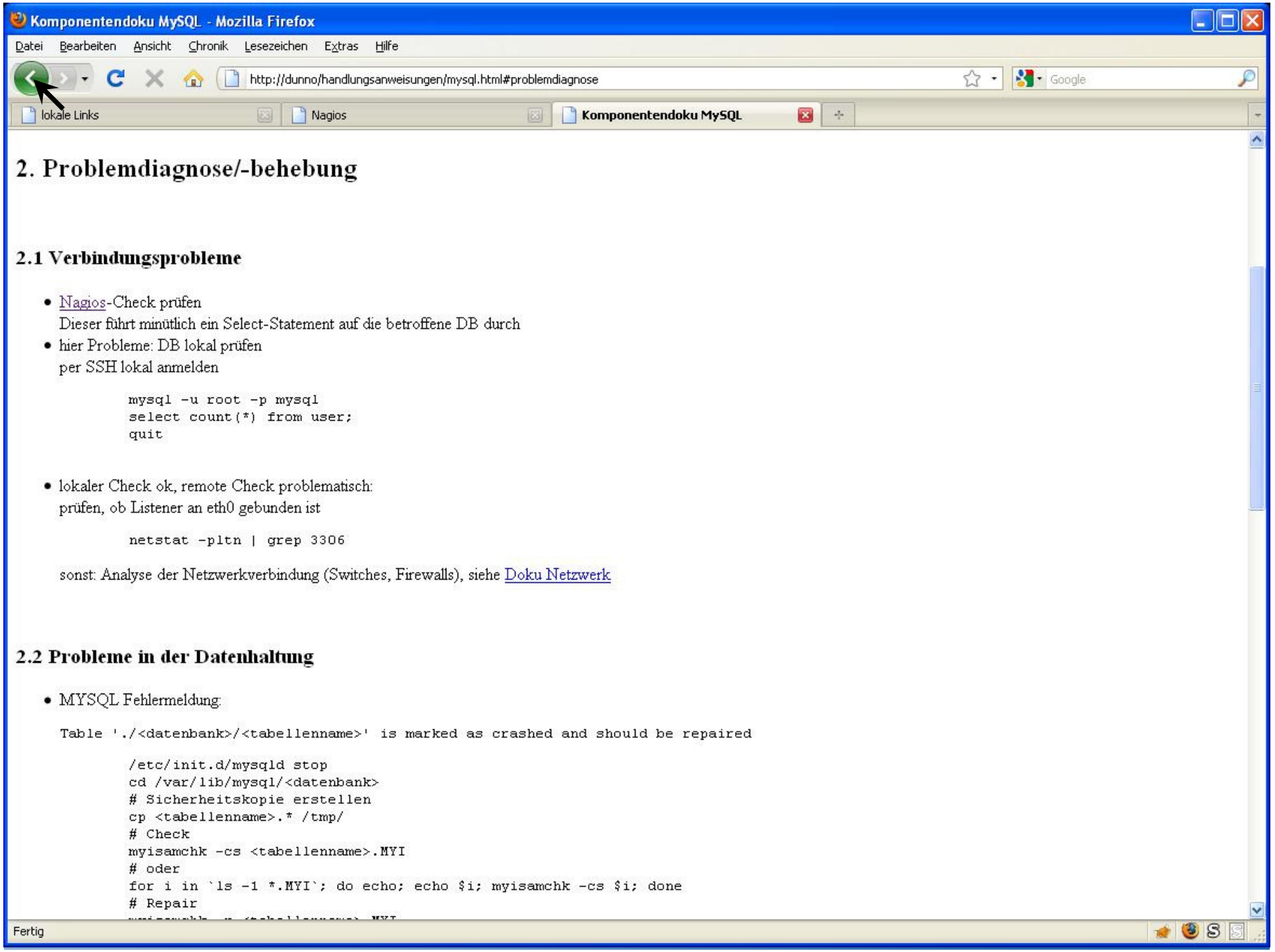
Service State Information

Current Status:	CRITICAL
Status Information:	CRITICAL: Select
Performance Data:	
Current Attempt:	2/2
State Type:	HARD
Last Check Type:	ACTIVE
Last Check Time:	12-07-2009 18:28:48
Status Data Age:	0d 0h 0m 31s
Next Scheduled Active Check:	12-07-2009 18:29:48
Latency:	0.259 seconds
Check Duration:	0.180 seconds
Last State Change:	12-07-2009 15:31:42
Current State Duration:	0d 2h 57m 37s
Last Service Notification:	N/A
Current Notification Number:	0
Is This Service Flapping?	N/A
Percent State Change:	N/A
In Scheduled Downtime?	NO

Service Commands
- Disable active checks of this service
- Re-schedule the next check of this service
- Submit passive check result for this service
- Stop accepting passive checks for this service
- Stop obsessing over this service
- Acknowledge this service problem
- Disable notifications for this service
- Delay next service notification
- Schedule downtime for this service
- Disable event handler for this service
- Disable flap detection for this service

Fertig


Notfalldoku Generic ERP - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://dunno/handlungsanweisungen/erp.html#db
Google
lokale Links
Nagios
Notfalldoku Generic ERP
(rämt hinterher sauber auf)
4.2 Datenbank (Server db)
Standard-MySQL, kein Cluster, keine Replikation
Tabellen-Typ: MyISAM
Servername: db
Port: 3306
Logfiles: /var/log/mysql/*
Details siehe Komponenten-Doku MySQL
5. Ansprechpartner
sofern Problemanalysen nicht zum Ziel führen: Generic ERP wird betrieben von Majestix, Vertreter Troubadix
6. weiterführende Dokumentationen
Betriebshandbuch ERP
Dokumentatenhistorie
Datum Version Autor Beschreibung
2007-02-14 1.0 Majestix Dokument erstellt
Fertig



2. Problemdiagnose/-behebung

2.1 Verbindungsprobleme

- Nagios-Check prüfen
  Dieser führt minütlich ein Select-Statement auf die betroffene DB durch
- hier Probleme: DB lokal prüfen
  per SSH lokal anmelden

```
mysql -u root -p mysql
select count(*) from user;
quit
```

- lokaler Check ok, remote Check problematisch:
  prüfen, ob Listener an eth0 gebunden ist

```
netstat -pltn | grep 3306
```

  sonst: Analyse der Netzwerkverbindung (Switches, Firewalls), siehe Doku Netzwerk

2.2 Probleme in der Datenhaltung

- MYSQL Fehlermeldung:

```
Table './<datenbank>/<tabellenname>' is marked as crashed and should be repaired

        /etc/init.d/mysqld stop
        cd /var/lib/mysql/<datenbank>
        # Sicherheitskopie erstellen
        cp <tabellenname>.* /tmp/
        # Check
        myisamchk -cs <tabellenname>.MYI
        # oder
        for i in `ls -1 *.MYI`; do echo; echo $i; myisamchk -cs $i; done
        # Repair
```

Nagios - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

http://dunno/nagios/

lokale Links | Nagios

Nagios

General
- Home
- Documentation

Monitoring
- Tactical Overview
- Service Detail
- Host Detail
- Hostgroup Overview
- Hostgroup Summary
- Hostgroup Grid
- Servicegroup Overview
- Servicegroup Summary
- Servicegroup Grid
- Status Map
- 3-D Status Map
- Business Process View
- Business Impact
- Service Problems
- Host Problems
- Network Outages

Show Host:

- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue

Reporting
- Trends
- Availability
- Alert Histogram
- Alert History
- Alert Summary
- Notifications
- Event Log

Configuration
- View Config

Service Information
Last Updated: Mon Dec 7 18:29:19 CET 2009
Updated every 30 seconds
Nagios® - www.nagios.org
Logged in as *u00stro*

View Information For This Host
View Status Detail For This Host
View Alert History For This Service
View Availability Report For This Service
View Notifications For This Service

Service
Select
On Host
db
(db)

Member of
No servicegroups.

127.0.0.1

(siehe Betriebsdoku, Kapitel ERP)

Wenn hier Probleme gemeldet werden,
siehe Betriebsdoku ERP, Abschnitt Datenbank
Wo wird diese Komponente verwendet?

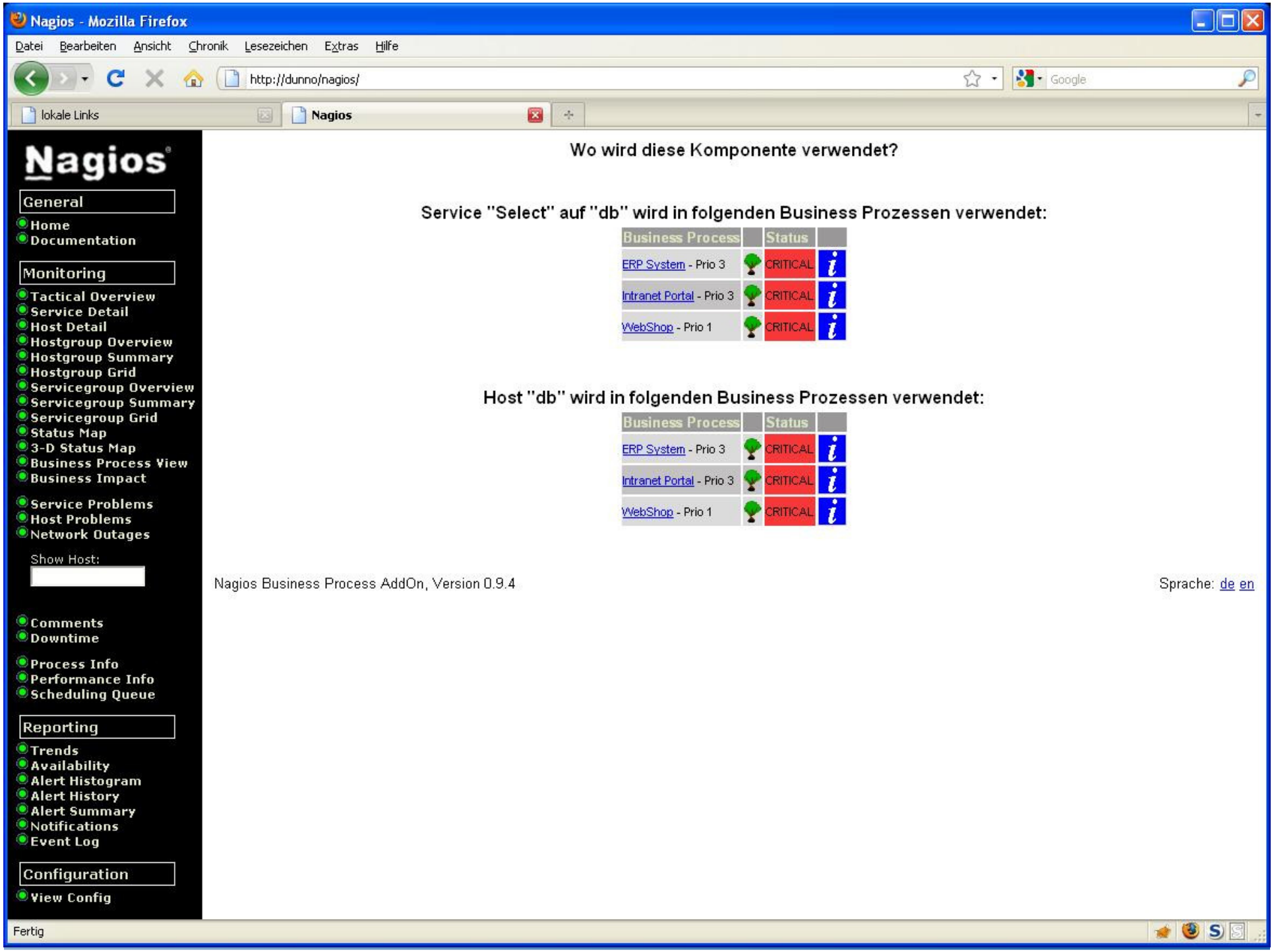
Extra Service Actions

Service State Information

Current Status:	CRITICAL
Status Information:	CRITICAL: Select
Performance Data:	
Current Attempt:	2/2
State Type:	HARD
Last Check Type:	ACTIVE
Last Check Time:	12-07-2009 18:28:48
Status Data Age:	0d 0h 0m 31s
Next Scheduled Active Check:	12-07-2009 18:29:48
Latency:	0.259 seconds
Check Duration:	0.180 seconds
Last State Change:	12-07-2009 15:31:42
Current State Duration:	0d 2h 57m 37s
Last Service Notification:	N/A
Current Notification Number:	0
Is This Service Flapping?	N/A
Percent State Change:	N/A
In Scheduled Downtime?	NO

Service Commands
- Disable active checks of this service
- Re-schedule the next check of this service
- Submit passive check result for this service
- Stop accepting passive checks for this service
- Stop obsessing over this service
- Acknowledge this service problem
- Disable notifications for this service
- Delay next service notification
- Schedule downtime for this service
- Disable event handler for this service
- Disable flap detection for this service

Fertig


Nagios - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://dunno/nagios/
Google
lokale Links
Nagios
Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Hostgroup Overview
Hostgroup Summary
Hostgroup Grid
Servicegroup Overview
Servicegroup Summary
Servicegroup Grid
Status Map
3-D Status Map
Business Process View
Business Impact
Service Problems
Host Problems
Network Outages
Show Host:
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
Event Log
Configuration
View Config
Wo wird diese Komponente verwendet?
Service "Select" auf "db" wird in folgenden Business Prozessen verwendet:
Business Process
Status
ERP System - Prio 3
CRITICAL
Intranet Portal - Prio 3
CRITICAL
WebShop - Prio 1
CRITICAL
Host "db" wird in folgenden Business Prozessen verwendet:
Business Process
Status
ERP System - Prio 3
CRITICAL
Intranet Portal - Prio 3
CRITICAL
WebShop - Prio 1
CRITICAL
Nagios Business Process AddOn, Version 0.9.4
Sprache: de en
Fertig

Verknüpfung von Monitoring und Dokumentation

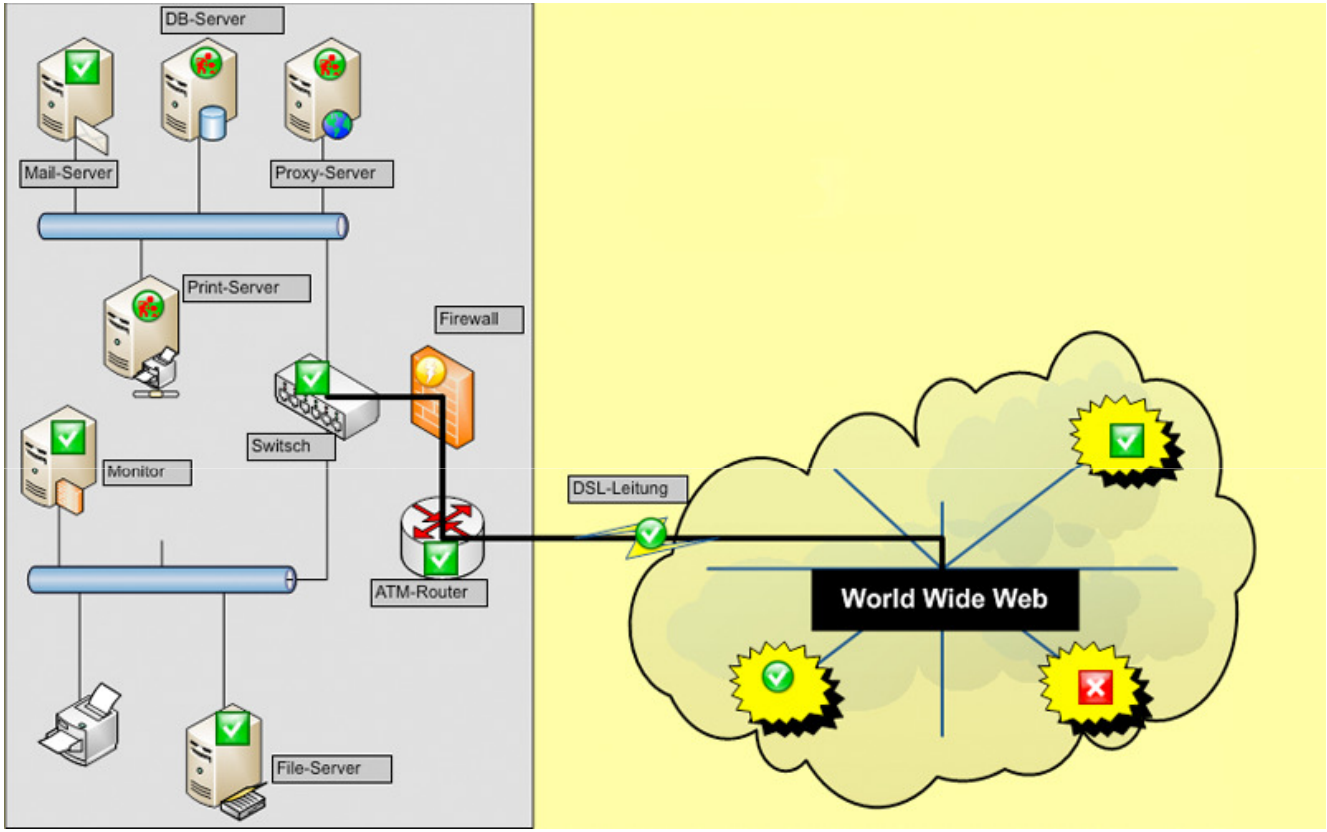
- Top-Level: Link auf Anwendungs-Doku
- Komponente: Link auf entsprechende Seite der Doku
- whereUsed zur Maschinen-Dokumentation

Welches Tool zur Dokumentation?

- Ein gutes Tool macht noch keine gute Doku!
- Keine Barrieren über das verwendete Tool aufbauen!
- Alles, was verlinkbar ist oder HTML exportiert kommt grundsätzlich in Frage
  - Wiki
  - Word oder OpenOffice
  - Docbook oder Apache Forrest
  - Nagvis
  - …
- Offline verfügbar machen!

Beispiel

NagVis



Quelle: http://www.netways.de (http://www.netways.de/uploads/pics/nagvis_netzwerk.png)

Weitere Beispiele: http://www.nagvis.org/screenshots

Tipps und Tricks

- FSP (Frequently Solved Problems)
  - z. B. als eine Seite im Wiki
  - maximal 10 Einträge
- Schnittstellen-Überwachung zu Partnern
- Change ist erst abgeschlossen, wenn die Doku aktualisiert ist
- Einheitliche Namen und Bezeichnungen im System, im Monitoring und in den Dokus

Literatur

- Nagios
  http://www.nagios.org
- Nagios Business Process AddOns
  http://nagiosbp.projects.nagiosforge.org
- Beispiel-Dokumentationen aus dieser Präsentationen sind in Kürze auch im Demo-System zu finden
  http://nagiosbp.projects.nagiosforge.org/demo.shtml
- NagVis
  http://www.nagvis.org
- End2End-Monitoring mit AutoIT
  http://www.netways.de/de/produkte/nagios_plugins/end2end/

Vielen Dank für Ihre Aufmerksamkeit

Noch Fragen?

- … jetzt und hier
- … in den Pausen
- … jederzeit per Mail
  <bernd.stroessenreuther@spb.de>