assono

Auf dem Weg zum allsehenden Administrator

Mit Monitoring zur stabileren Infrastruktur

Admincamp 2017

Vorstellung - Ich

Manuel Nientit

Diplom Wirtschaftsinformatiker

Seit knapp 2004 mit IBM Notes und Domino

Seit 2008 IT-Consultant der Firma assono GmbH

Erst Entwickler dann Administrator

Agenda

- Was ist gemeint?
- Holschuld
- Probes und Events/Bringschuld
- Externe Überwachung

Wofür?

- Fehler möglichst frühzeitig erkennen
- Protokollierung für Sicherheitsmanagement (z.B. Zugriffe)
- Kapazität planen und steuern
- Abrechnen

Wann?

Die Konfiguration ist niemals einmalig, sondern muss dauernd verfeinert werden.

Philosophie

Über Symptome informieren

Ideal: Clientzugriff simulieren

Alternativ: Zustände die Symptome zeitigen oder zeitigen werden

Benachrichtigung? Wie?

1. Record: zentral gespeichert als Unterstützung zur Fehlersuche
2. Notification: Aktive Alarmierung von Zuständigen (Mail, IM, Ticket…). Reaktion erforderlich, aber nicht sofort
3. Alert: Höchste Prio. Sofortige Maßnahmen erforderlich (SMS, Pager, Push-Nachricht…)

Benachrichtigung? Wer?

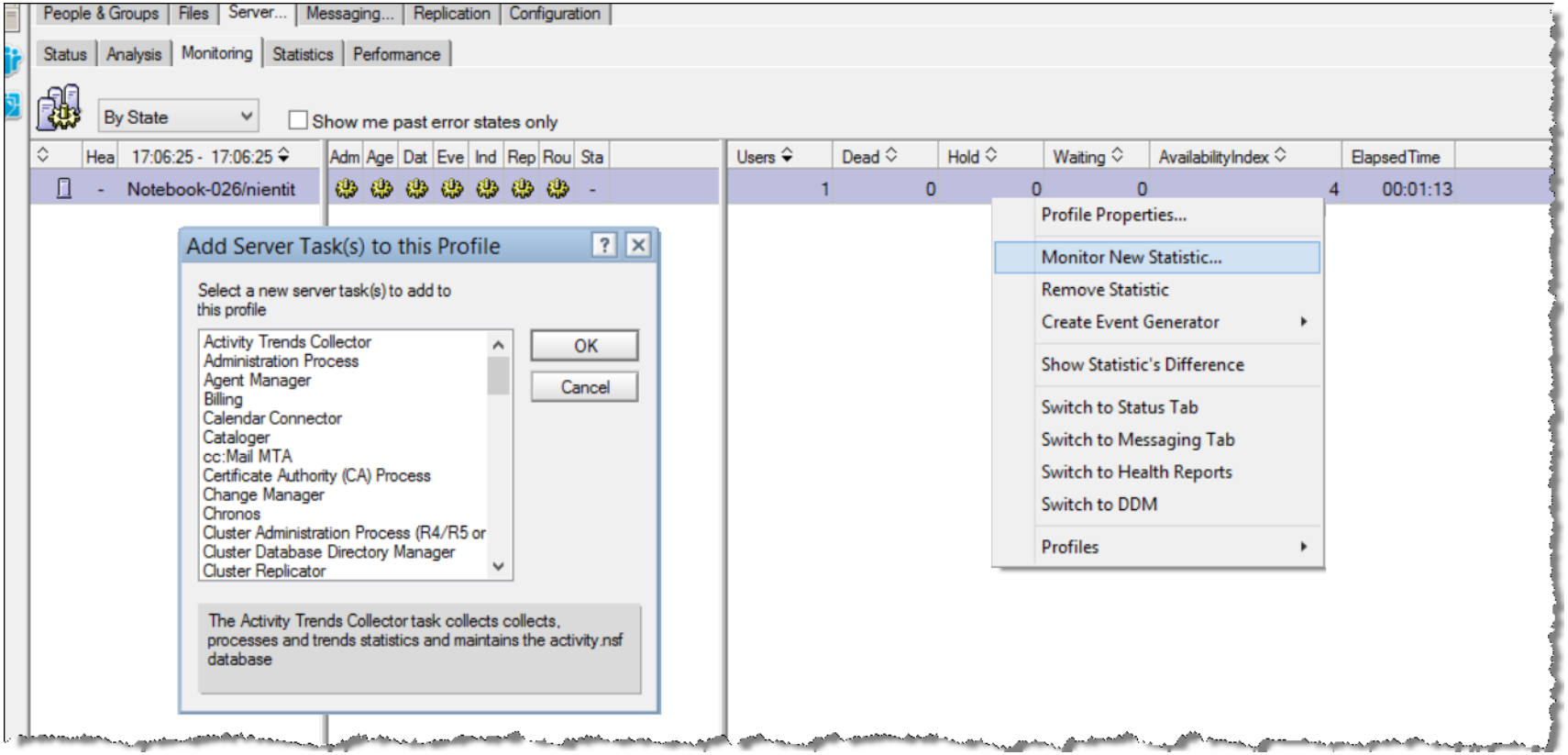
- Systemverantwortliche
- Abhängig Systemverantwortliche: z.B. Wen interessiert noch, dass Mails nicht zugestellt werden?
- „Notfallmanager“/“Continuity Manager“
- Fachlich Verantwortliche
- VIP

Domino ist keine Insel

- Domino ist abhängig:
  - Firewall
  - Mailgateway
  - SAN
  - Switches
- Domino macht abhängig:
  - SMTP Relay
  - LDAP Service
  - IMAP/POP3

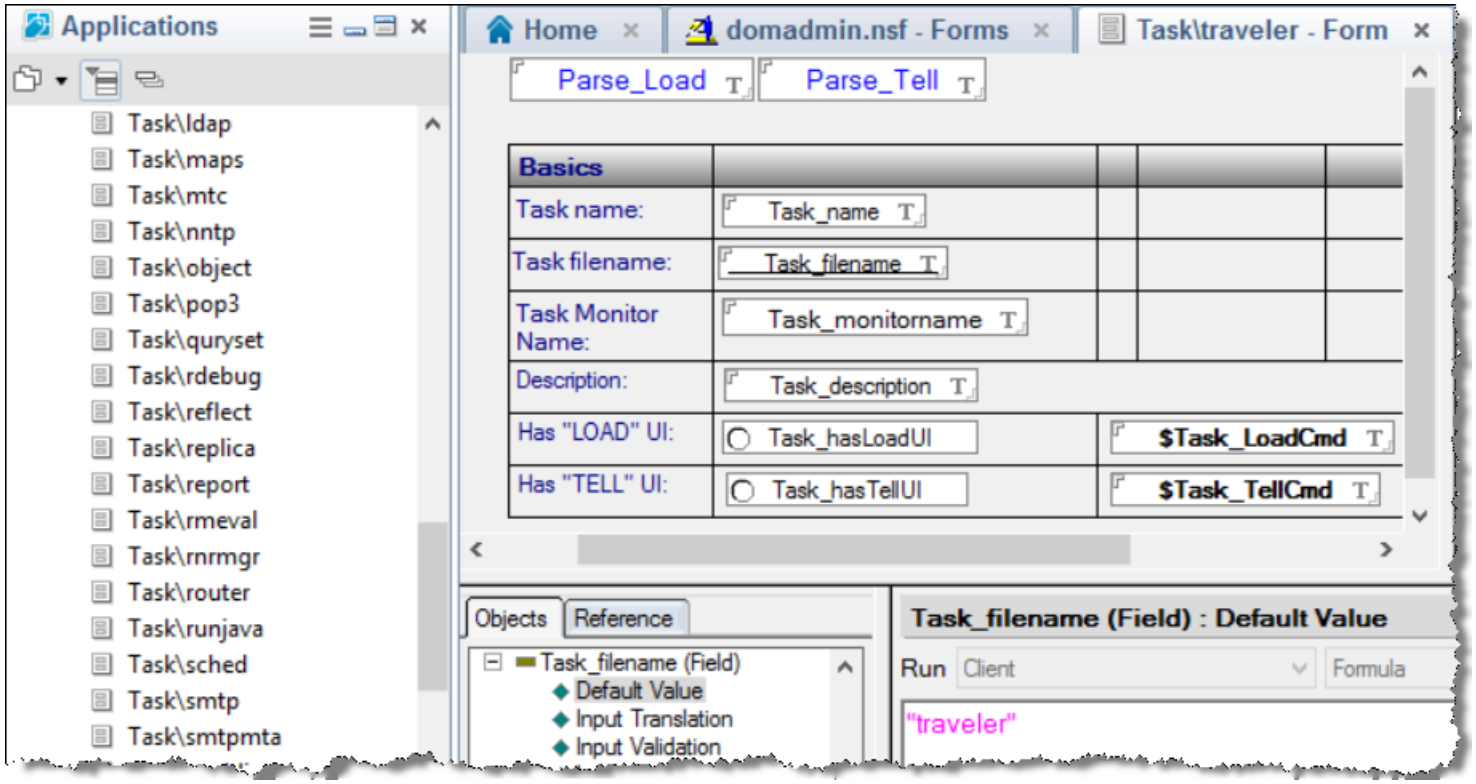
-> Abhängigkeiten darstellen

Holschuld - Monitoring Tab

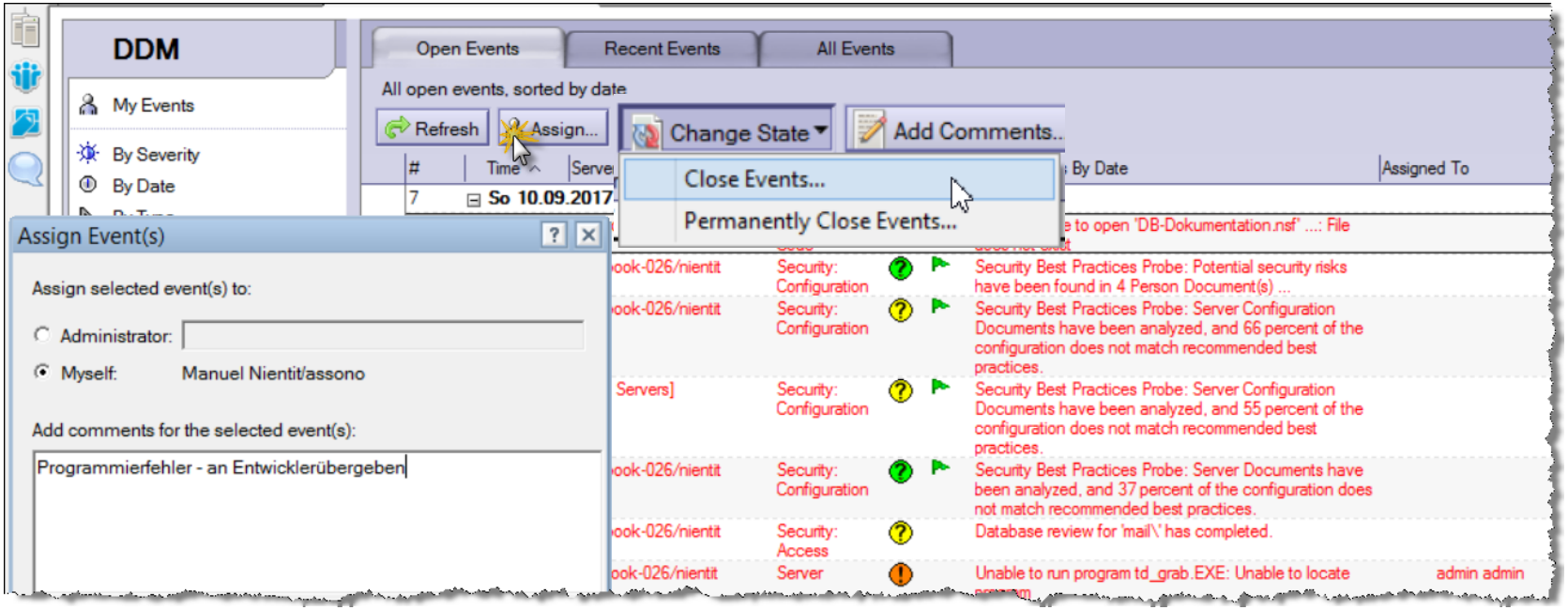


Holschuld - Monitor-Tab – Traveler Task

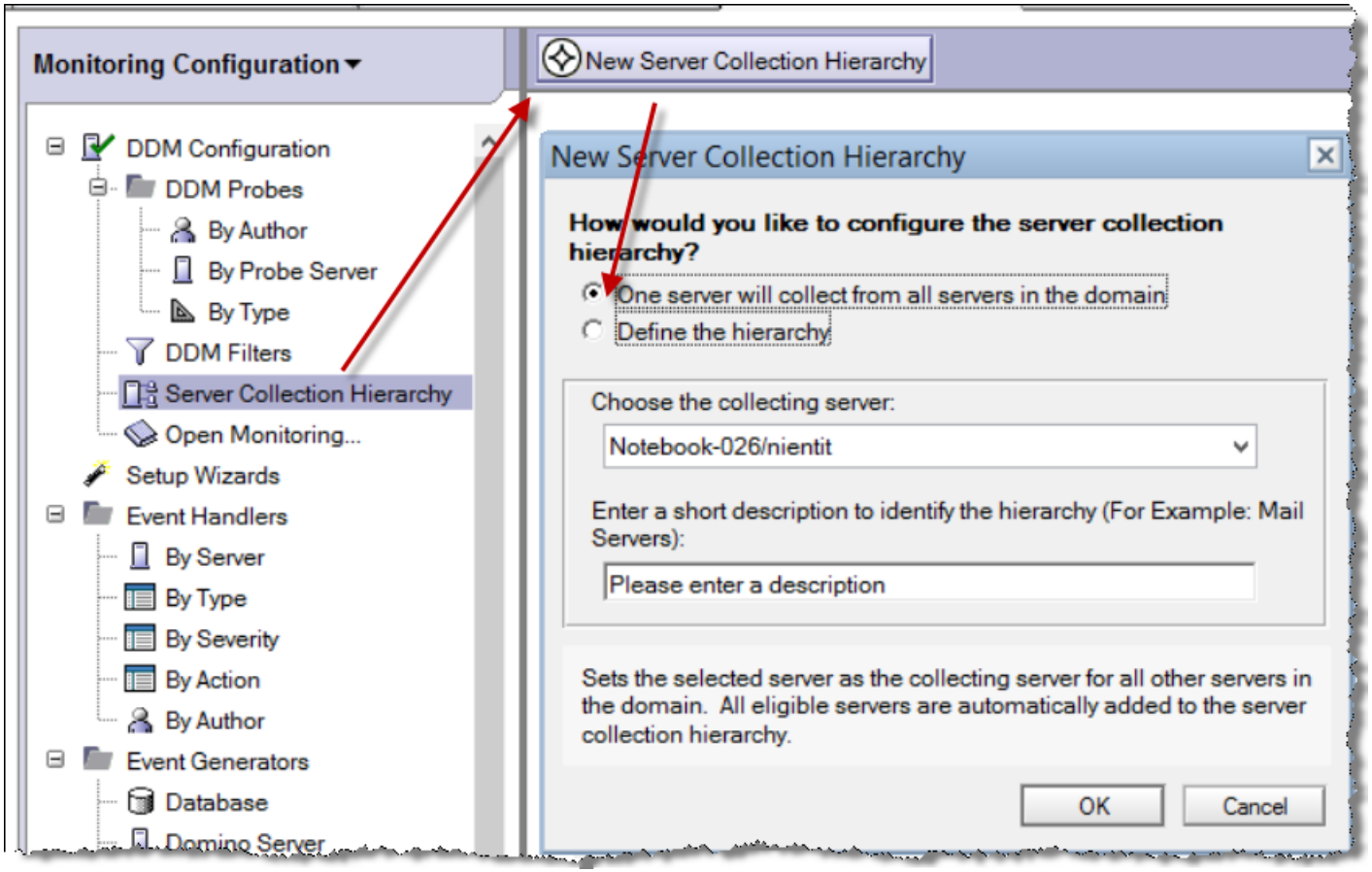
In der lokalen domadmin.nsf eine Taskmaske (z.B. calconn) kopieren und die „Defaultwerte“ der Felder anpassen



Holschuld - DDM



Holschuld – DDM Collection Hierarchy



assono

Holschuld – DDM Collection Hierarchy

Beispiel – nach Funktion:

1. Gesamt (auf „Admin-Server“)
    1. DMZ – Domain
        1. Traveler
        2. Webserver
        3. Kommunikation
    2. Interne Domain
        1. App-Cluster
        2. Mail-Cluster
    3. Entwickler Domain

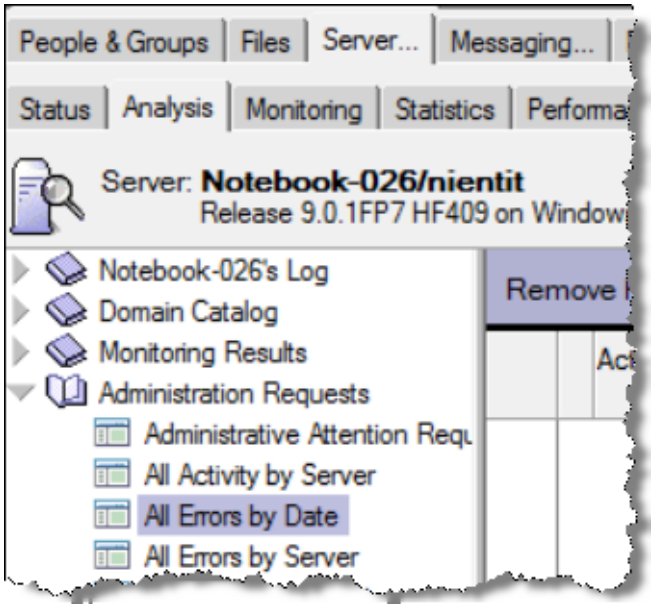
Beispiel – nach Prio:

1. Mailrouting/Kommunikation
2. App-Server
3. Web/Traveler

Holschuld – Adminp/4

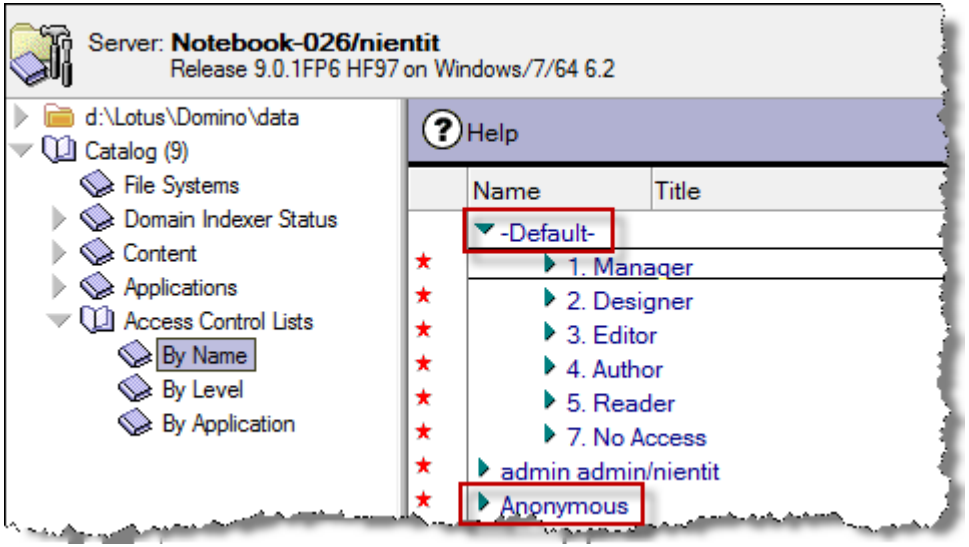
Ca. wöchentlich (Montags) Admin4.nsf prüfen

- Fehler bei der Nutzerverwaltung
  - Recert
  - Löschung
  - Umbenennung
- HTTP-Passwortänderungen



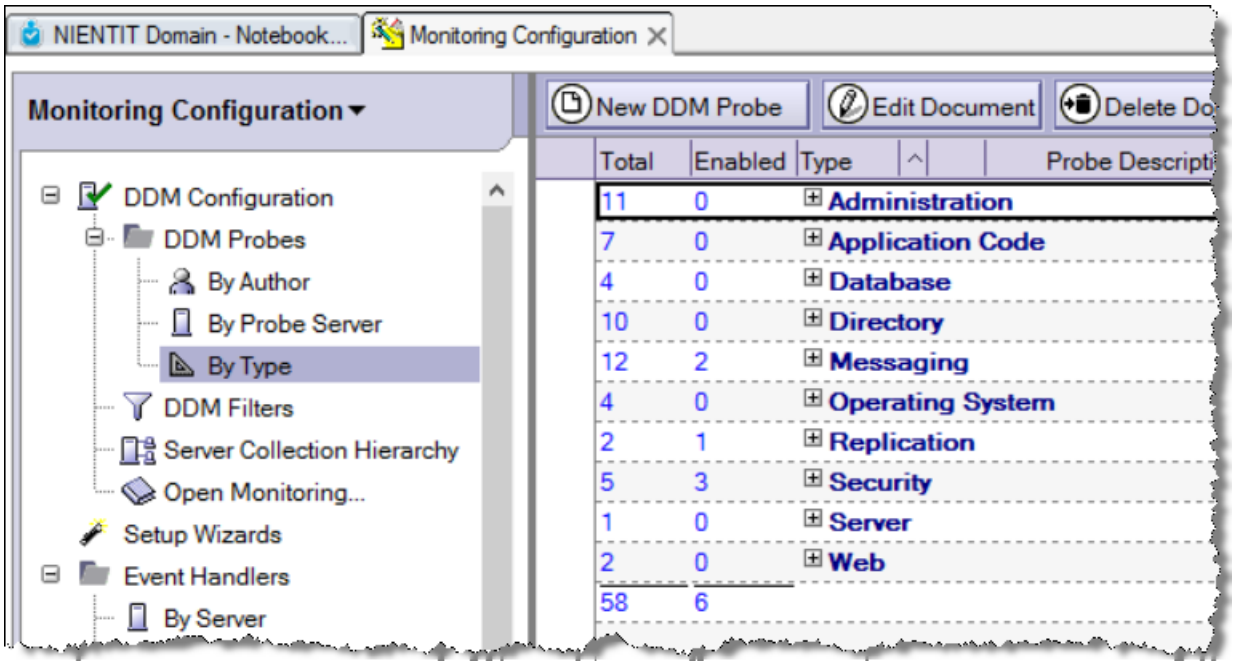
Holschuld– Domänenkatalog

z.B. einmal im Quartal, um z.B. zu hohe Berechtigungen zu finden



Probes und Events – Allgemein

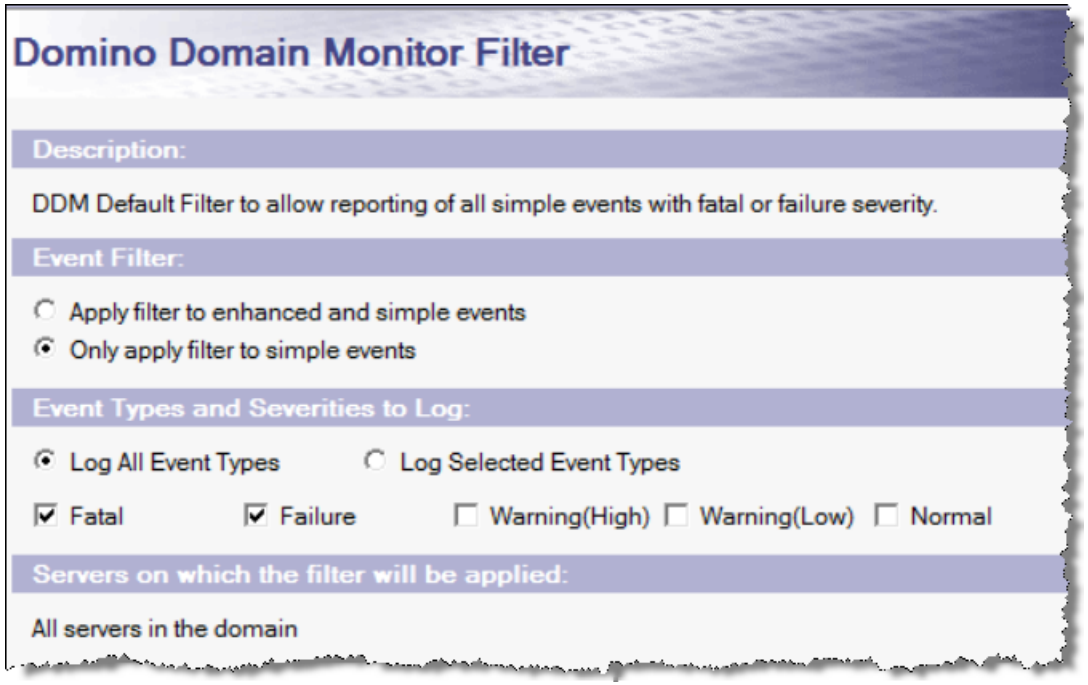
Probes sind im Prinzip Agenten, die regelmäßig Funktionen ausführen und ggf. die Reaktion registrieren und daraus records generieren



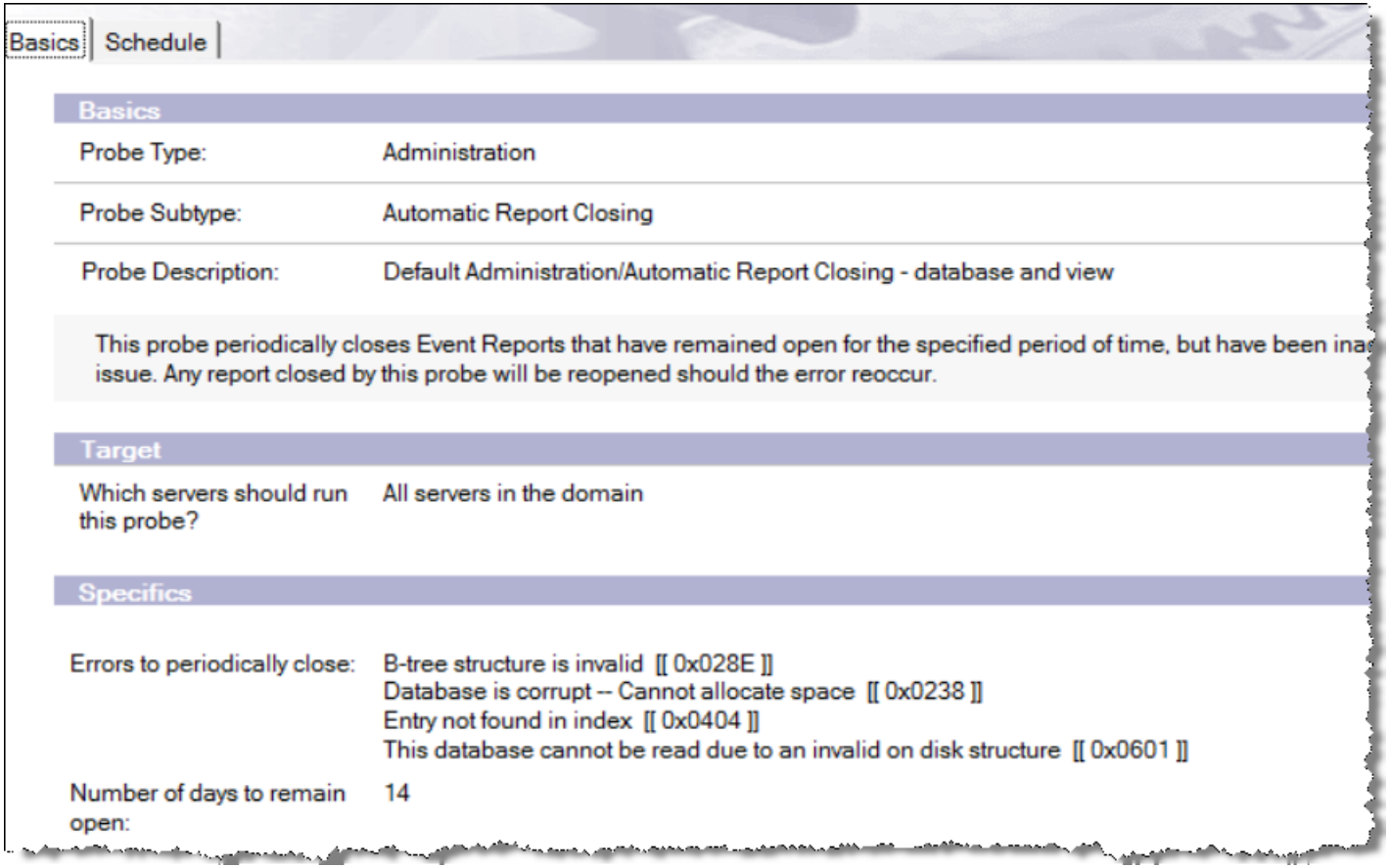
Probes and Events - Filters

Welche Events sollen überhaupt in die Protokolle respektive Konsole geschrieben werden?

- Log Filter: Nur Fatal und Failure?
- DDM: alles?



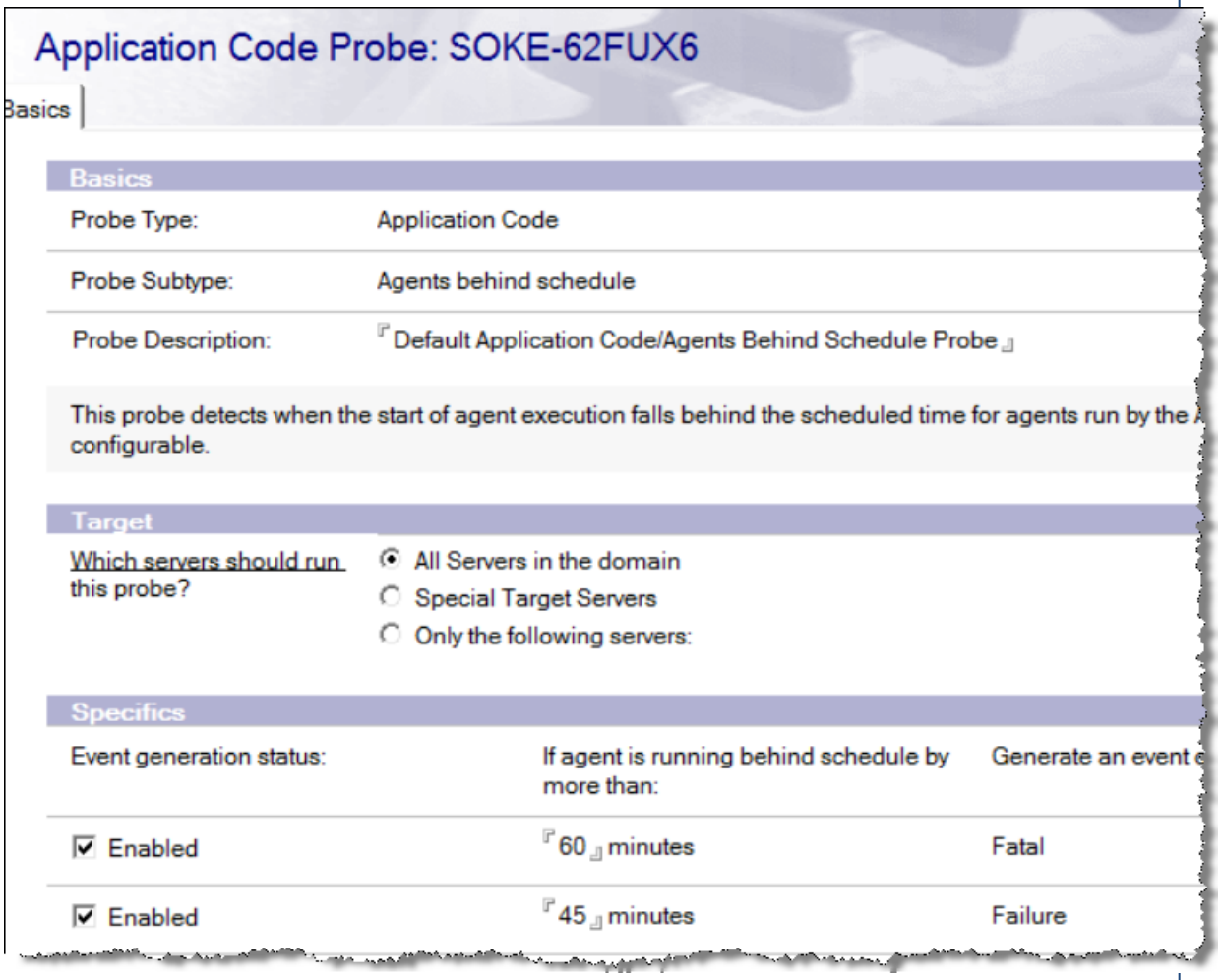
Probes & Events - Automatic Report Closing



Probes and Events – Application Code

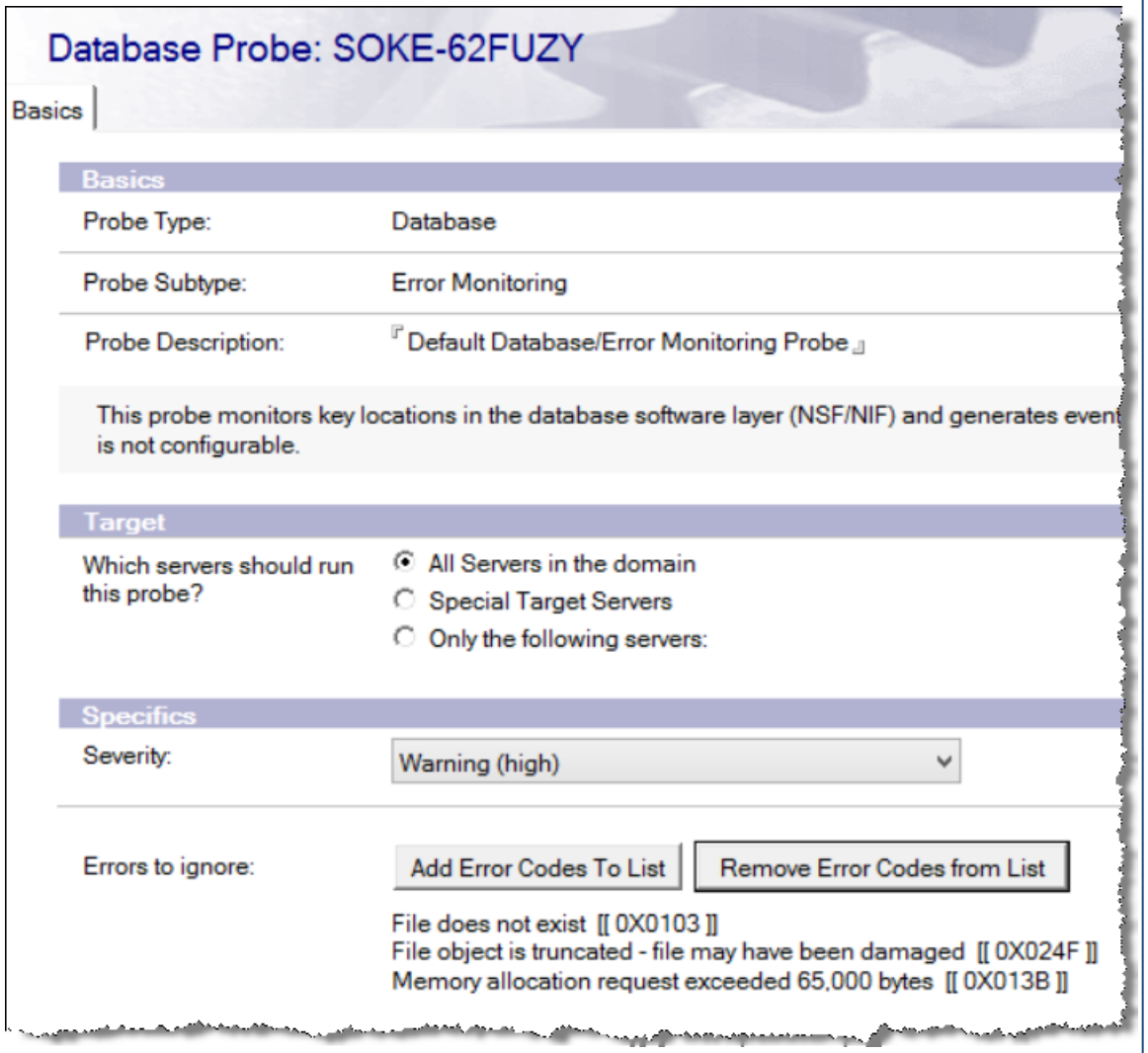
Agenten:

- Lang laufend
- verspätet
- Hohe CPU-Last

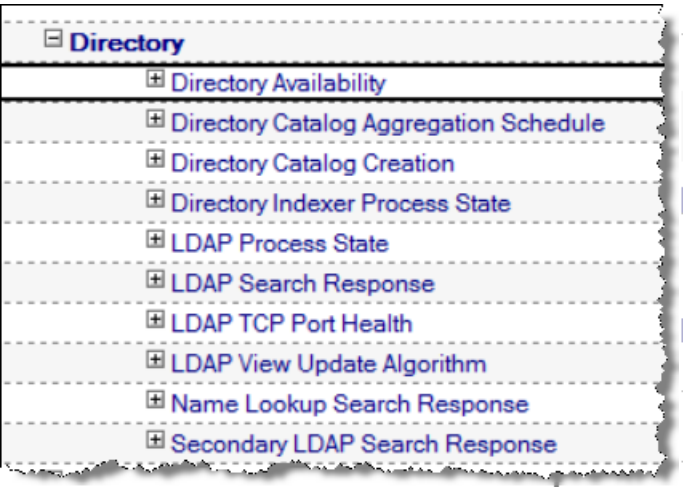


Probes und Events - Database Probes

- DB Fehler
- (In-)Aktivität
- Design Fehler
- Compact Fehler



Probes und Events - Namelookup Probe



Directory Probe: SOKE-62FV4R - DISABLED

Basics

Basics

Probe Type:	Directory
Probe Subtype:	Name Lookup Search Response
Probe Description:	Default Directory/NAMELookup Search Response Probe

This probe monitors the average search response time for user name lookups on the target server. The search response is based on sta
Monitor if search response times meet or exceed configured thresholds. The schedule for this type of probe is not configurable.

Target

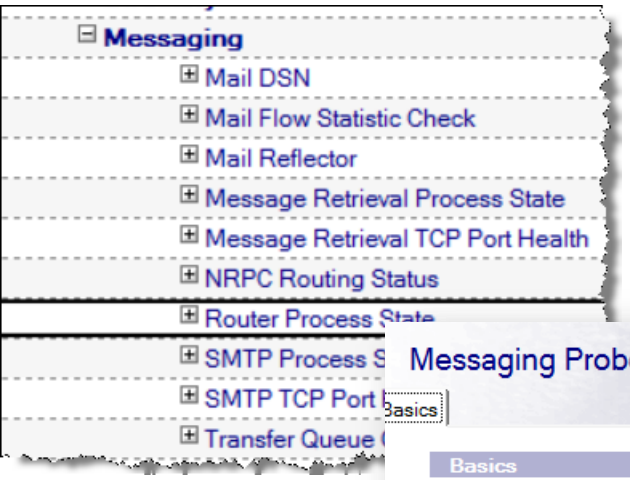
Which servers should run this probe?

- (•) All Servers in the domain
- ( ) Special Target Servers
- ( ) Only the following servers:

Specifics

Event generation status:	If the Name Lookup response exceeds:	Generate an event of severity:
☑ Enabled	2000 milliseconds	Fatal
☑ Enabled	1500 milliseconds	Failure
☑ Enabled	1200 milliseconds	Warning High
☐ Enabled	800 milliseconds	Warning Low

Probes und Events - Mail Flow Statistic



Messaging Probe: SOKE-62FV6H - DISABLED

Basics

Basics

Probe Type:	Messaging
Probe Subtype:	Mail Flow Statistic Check
Probe Description:	Default Messaging/Mail Flow Statistic Check Probe

This probe monitors the quantity of mail within a Domino server and will generate an event in the Domino Domain Monitor when pending messages meet or ex
(causing mail delivery to fall behind). This option applies only to the 'Fatal' severity because of its impact on successful & timely mail delivery. The slack percen

Target

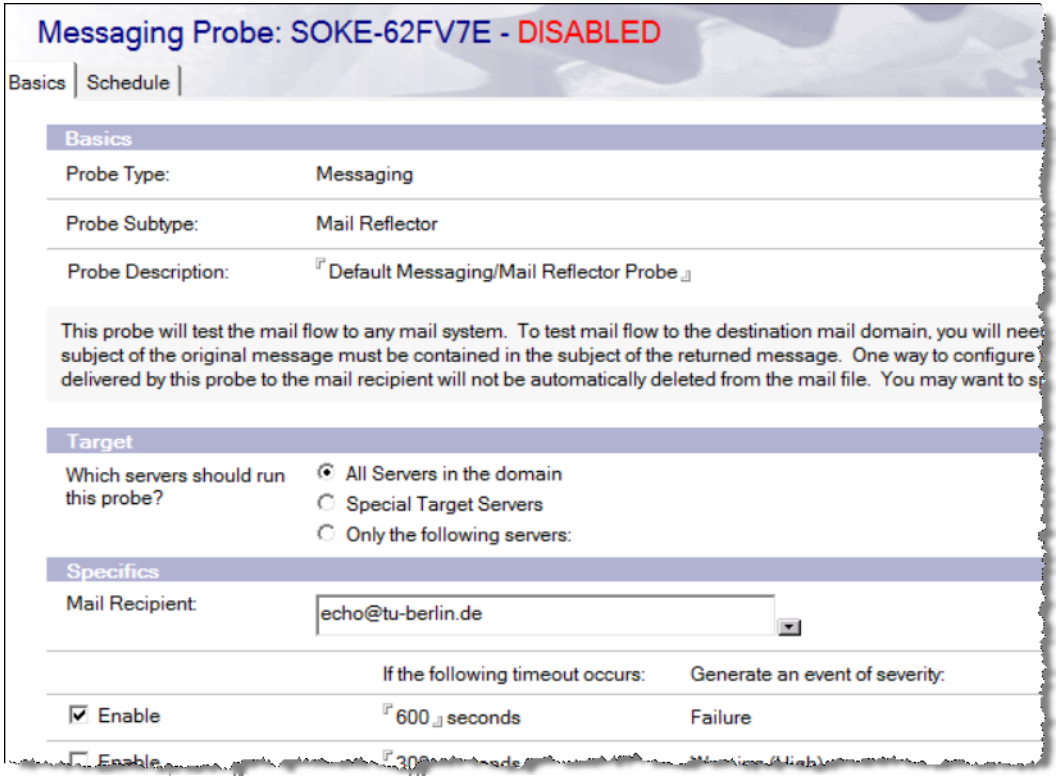
Which servers should run this probe?	All servers in the domain

Specifics

	If the pend limit exceeds	or the slack percentage exceeds	then generate an event of the following severity:
☑ Enable	Not Applicable	20	Fatal
☐ Enable	100	Not Applicable	Failure
☐ Enable	50	Not Applicable	Warning (High)
☐ Enable	25	Not Applicable	Warning (Low)

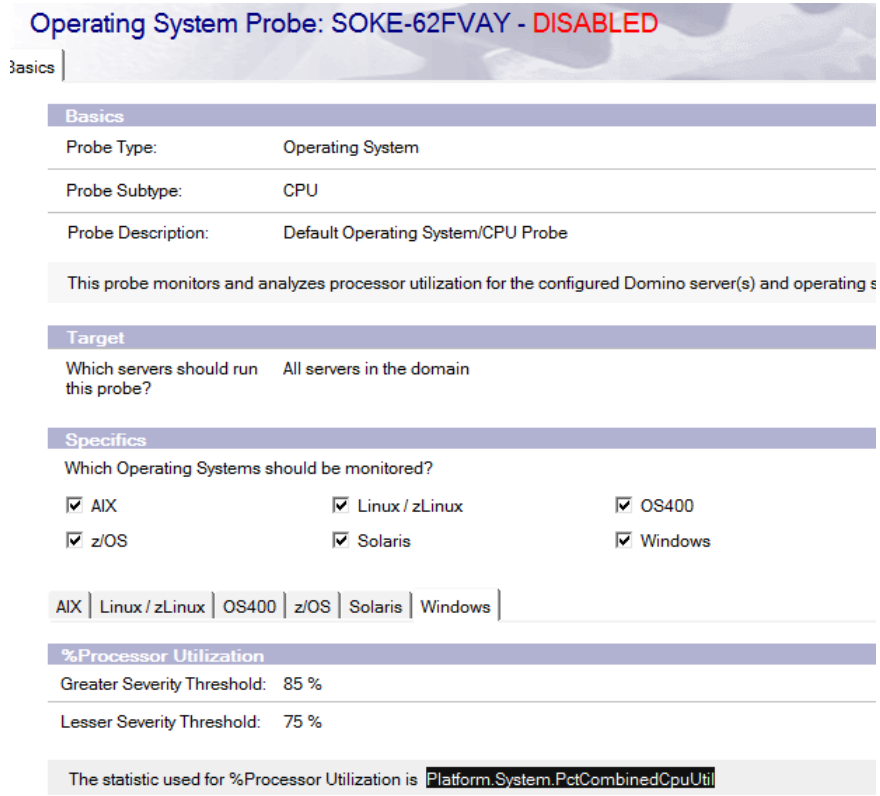
Probes und Events – Mail Reflector Probe

Mail an Echomailer – Antwortzeit wird gemessen

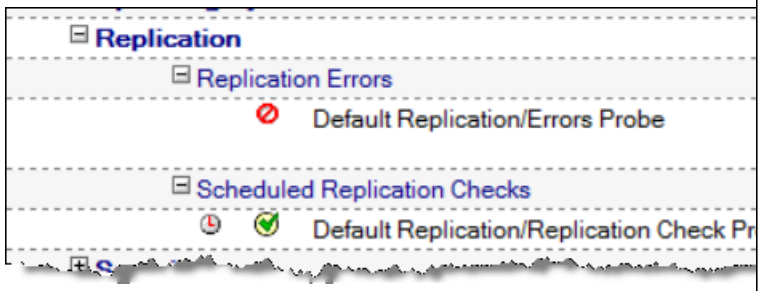


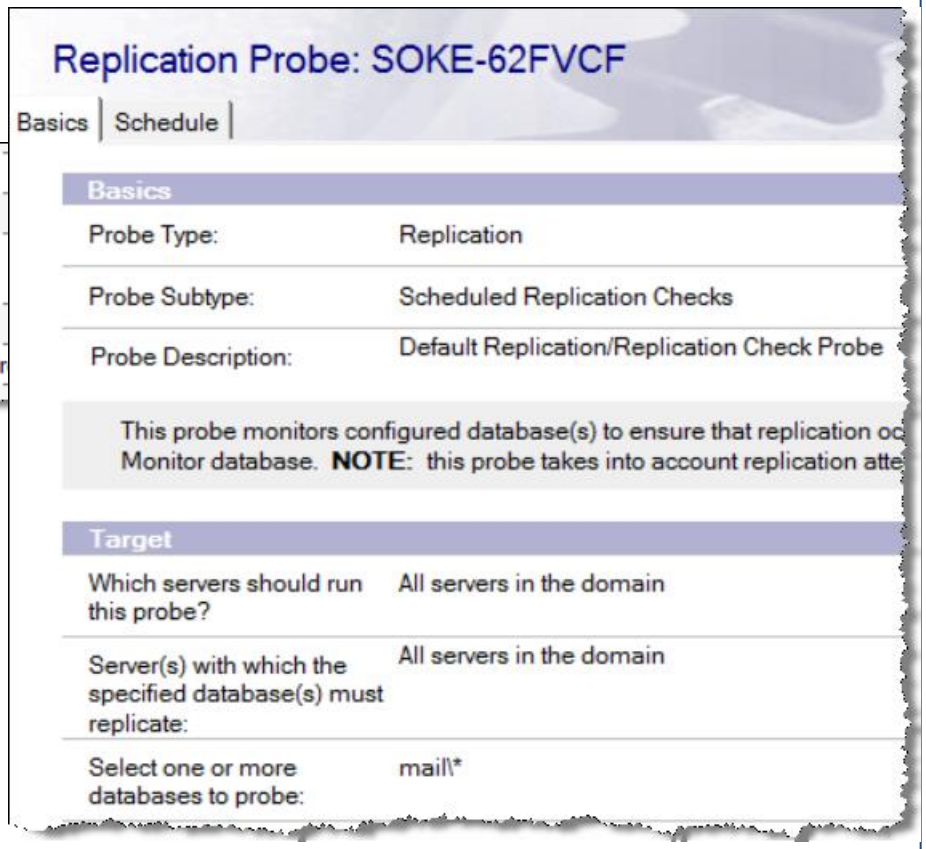
Probes und Events – Operating System Probe

Widerspricht dem Prinzip „prüfe Symptome“ ist, allerdings bei Disk-Queue-Length wichtig



Probes and Events - Replication



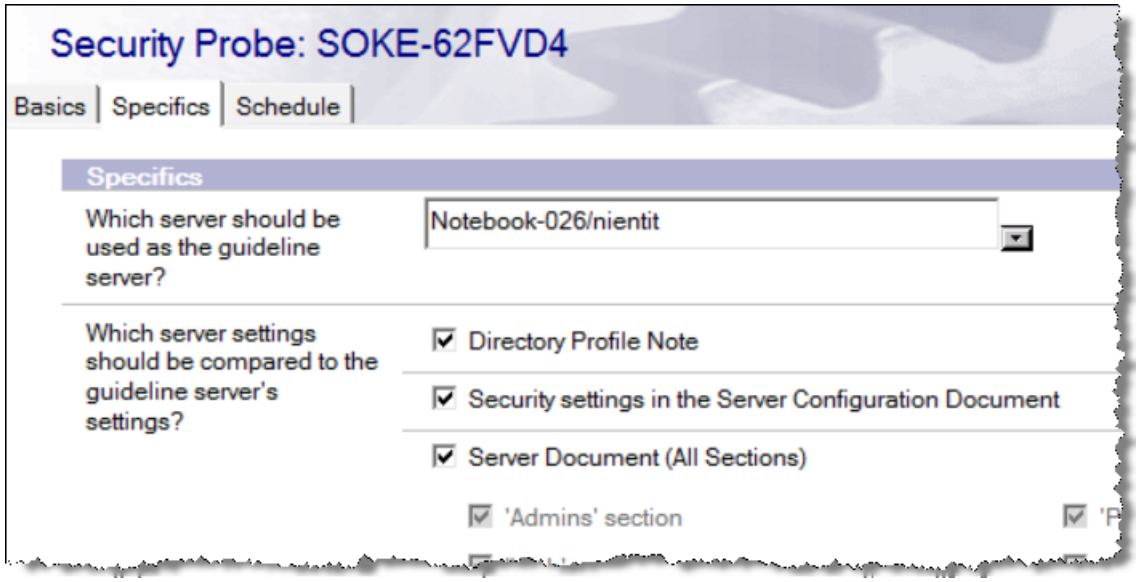


Probes and Events - Security

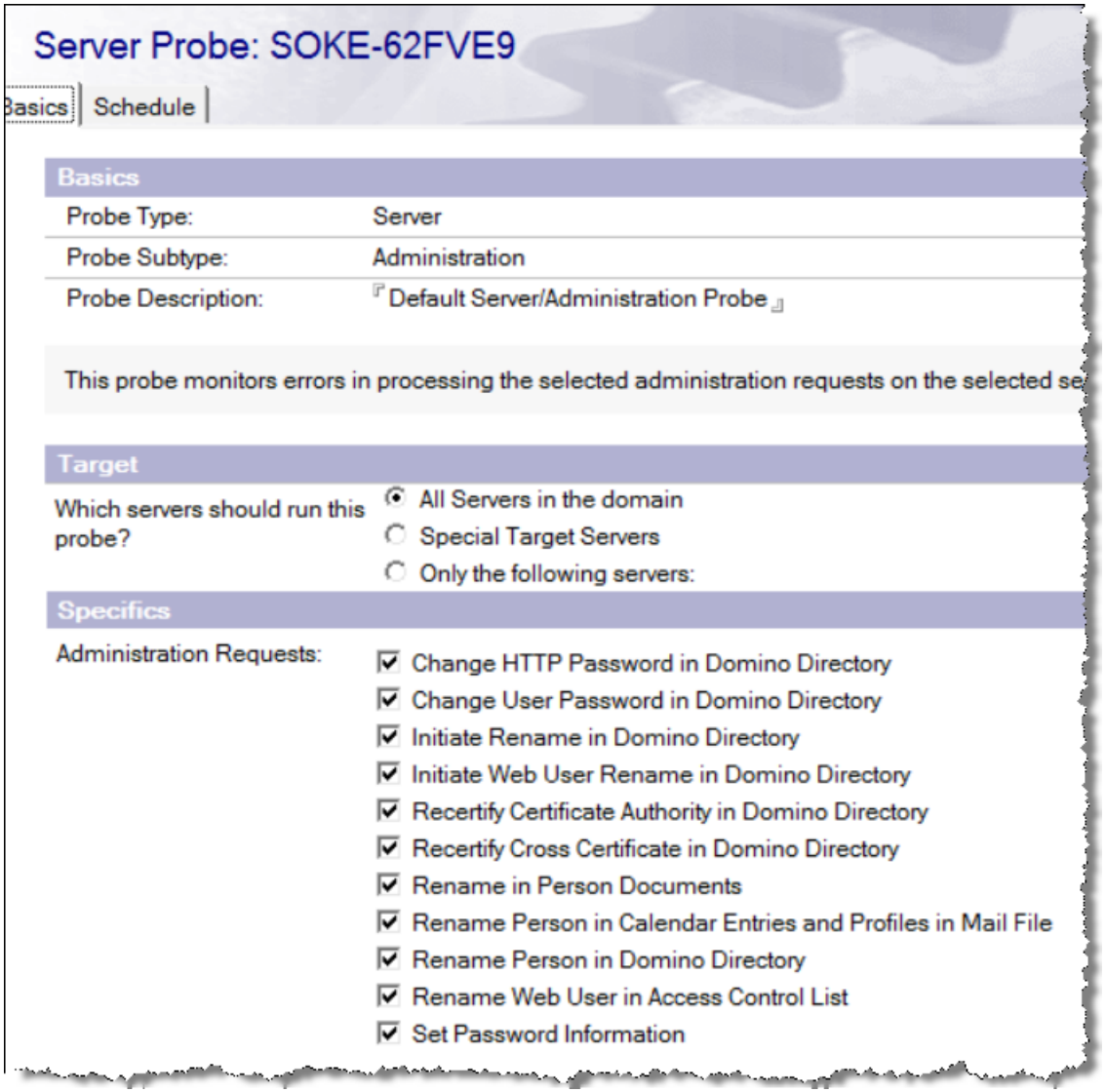
Viele Best Practice Probes

Database Security Probe kann Standard-ACL-Einstellungen prüfen (consistent ACL, Adminserver…)

Database ACL-Probe findet Anwendungen, in denen bestimmte Nutzer zu hohe Rechte haben (Default, Anonymous)



Probes and Events – Administration Probe



Probes und Events - Generators

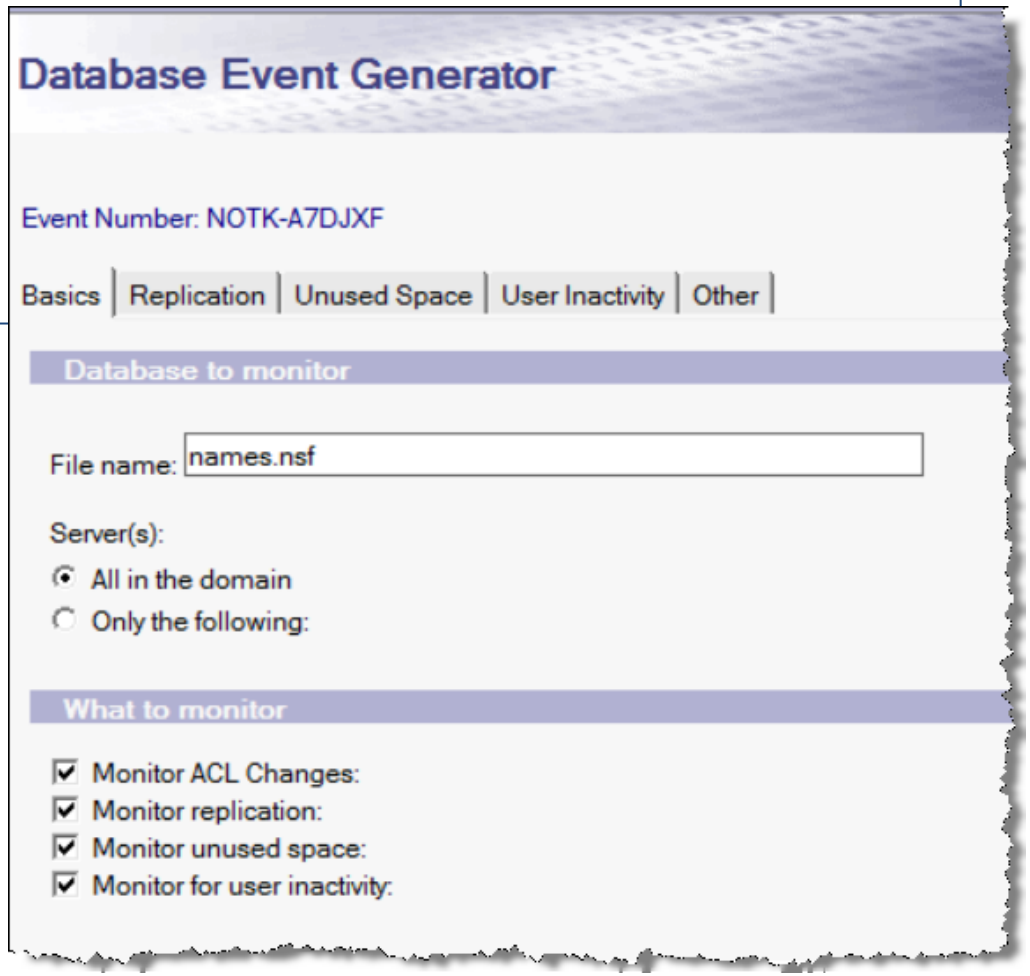
Es gibt sechs Arten von Generators:

- Database
- Domino Server
- TCP Server
- Mail Routing
- Statistic
- Task Status

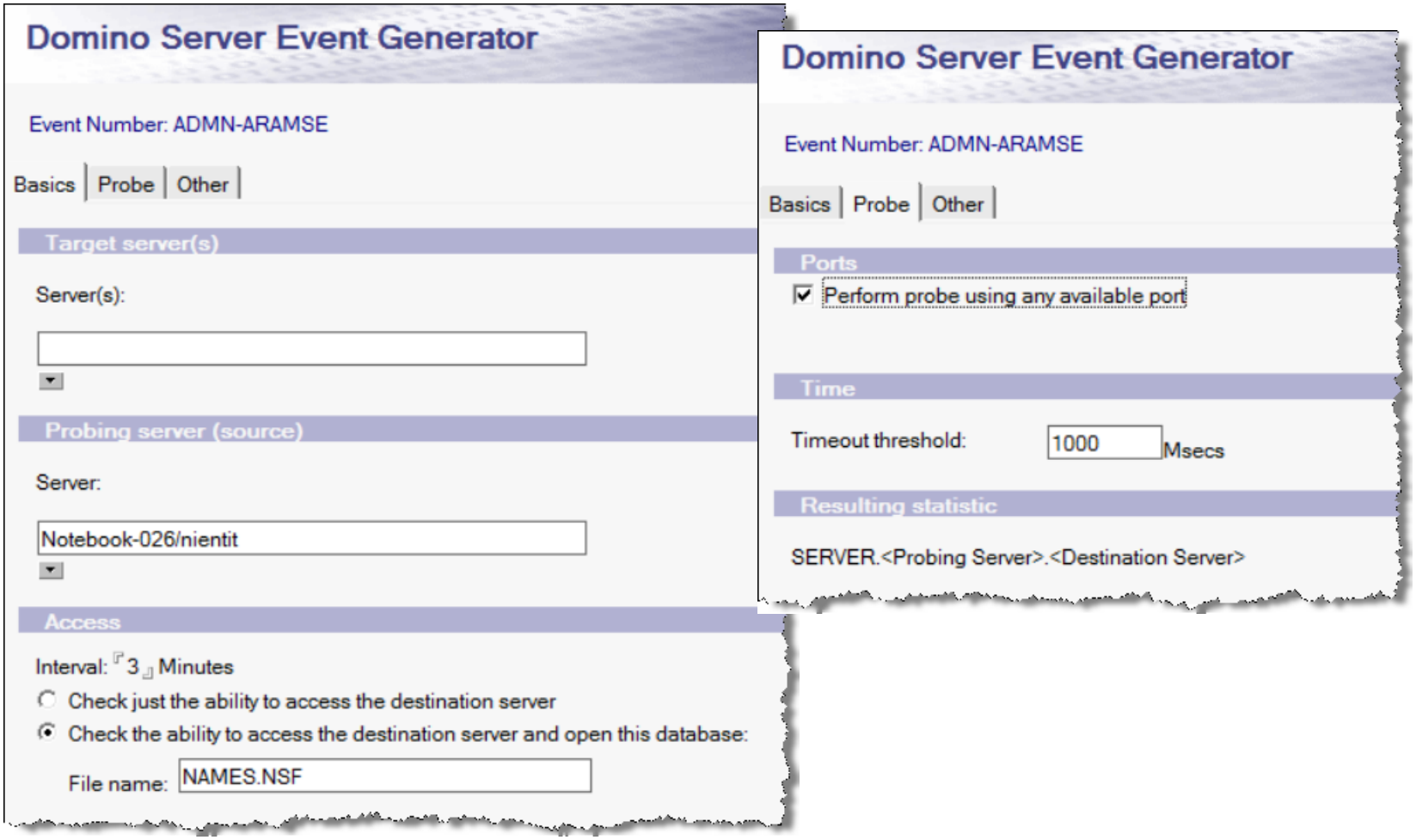
Jeder Generator braucht min. einen Handler damit etwas passiert

Event Generator - Database

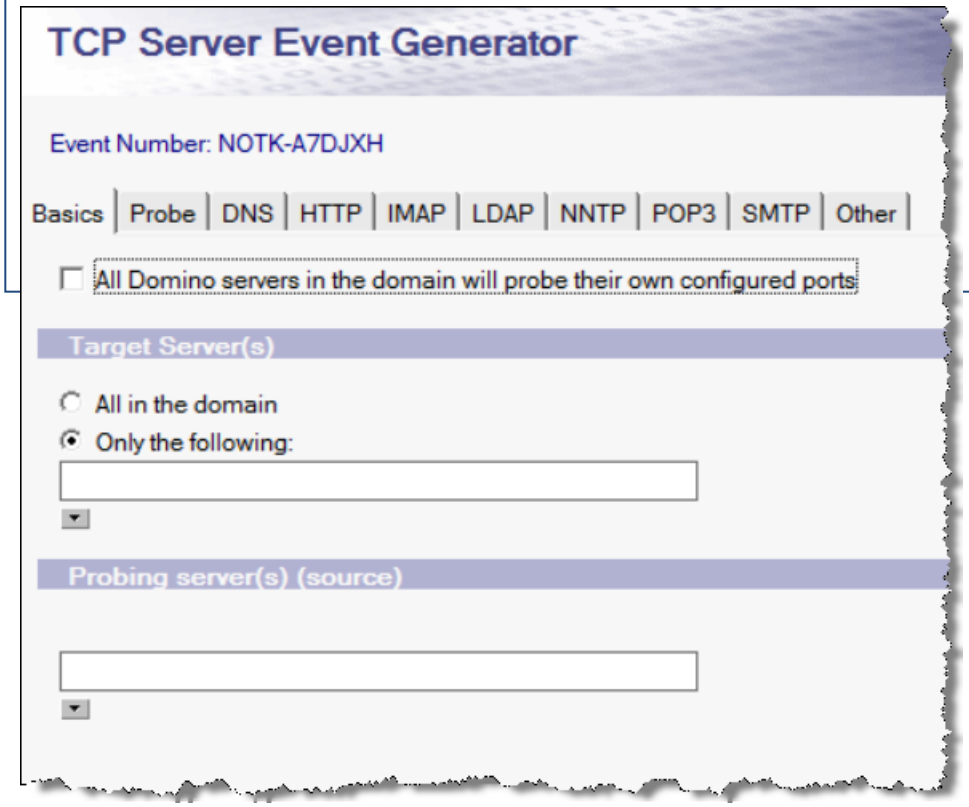
- Ändert jemand die ACL?
- Wird die DB repliziert?
- Nimmt sie zu viel Platz?
- Brauche ich sie noch?



Event Generator - Server

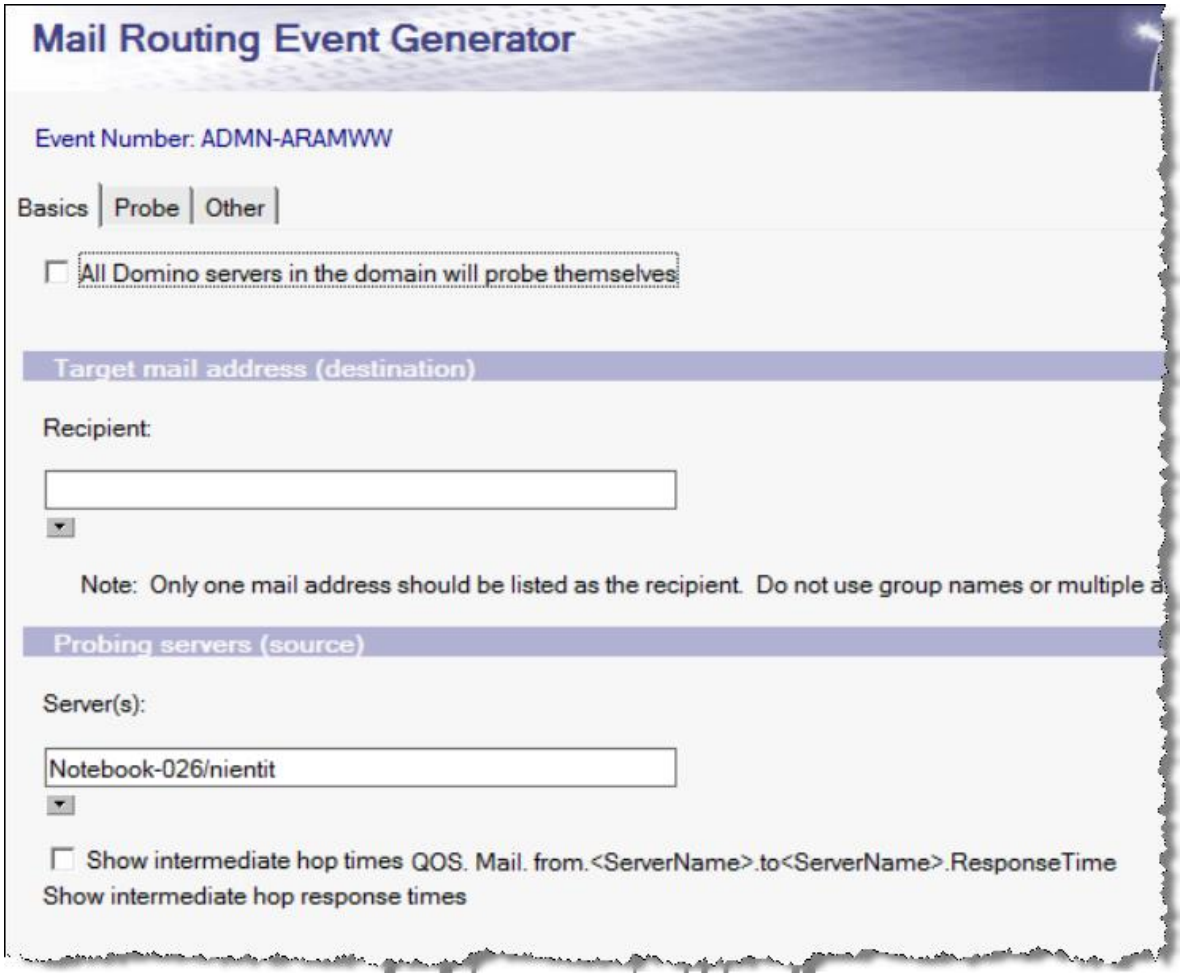


Event Generator – TCP Probes



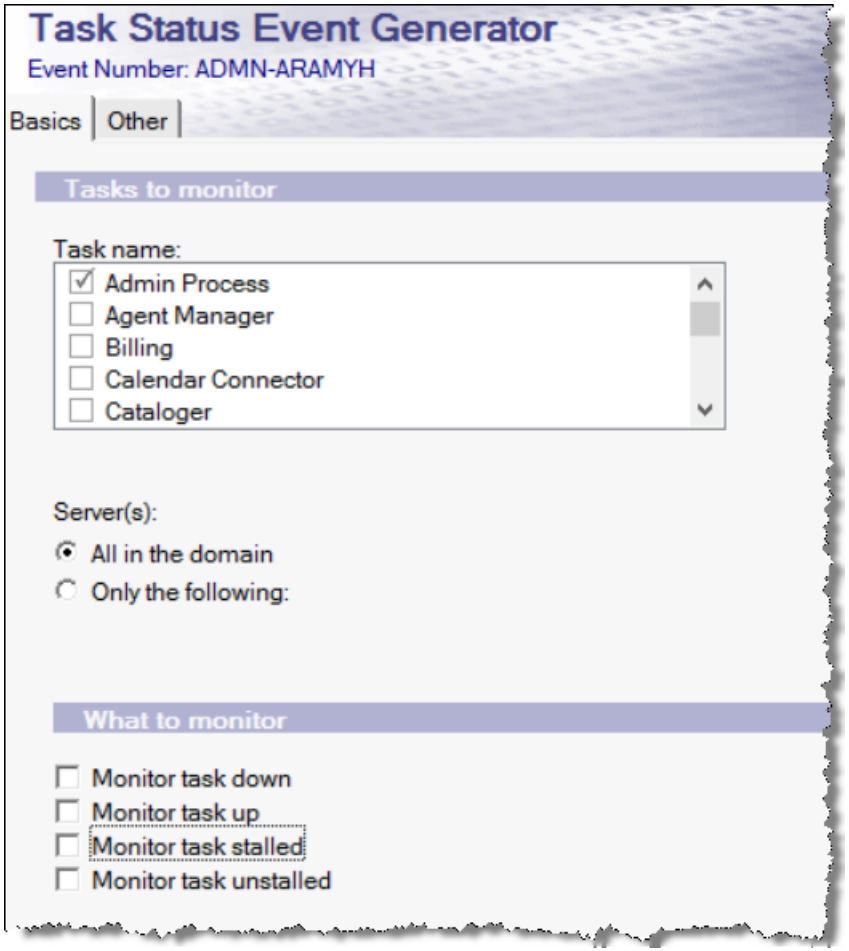
Event Generator – TCP Probes

Event Generator – Mail Routing



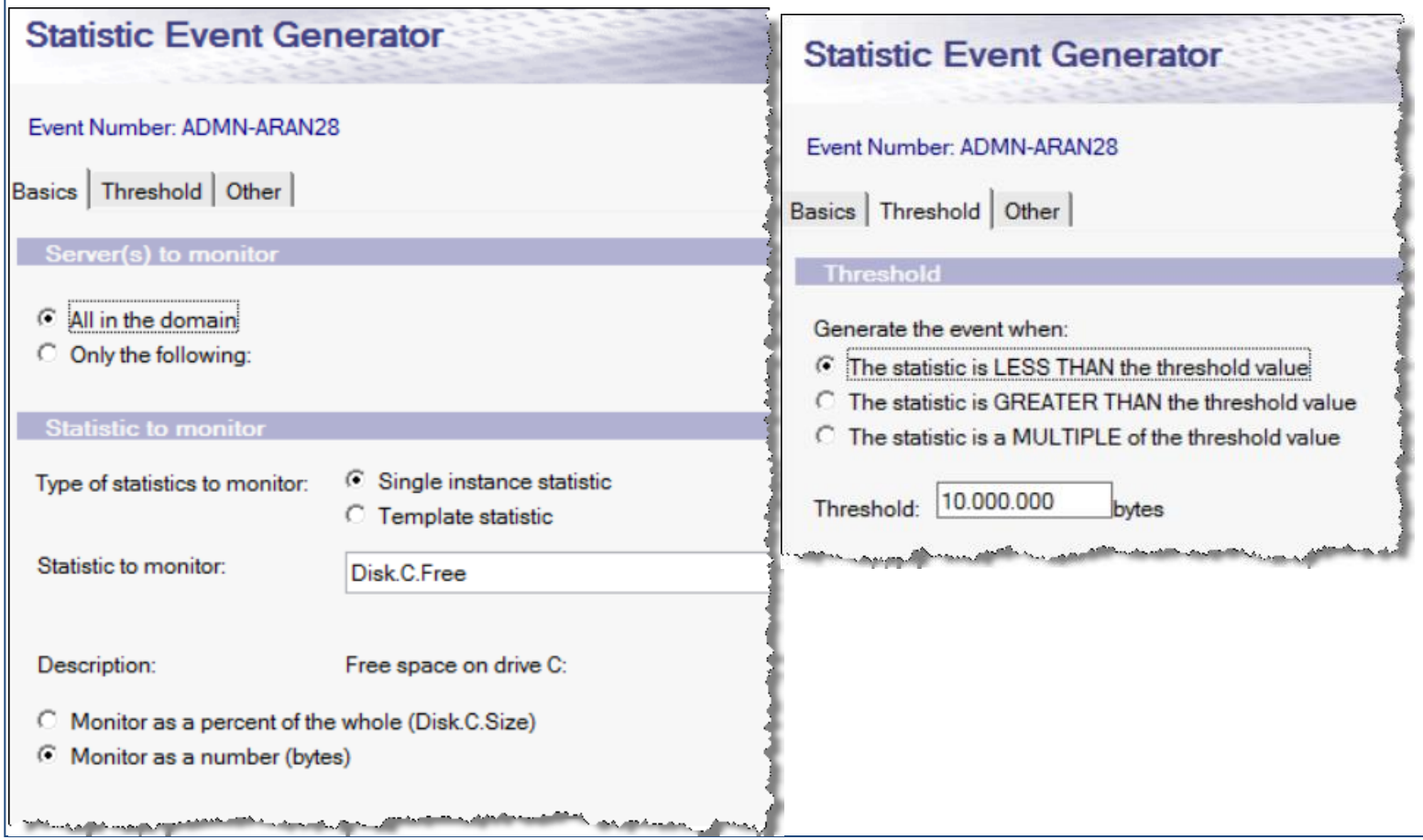
Event Generator – Task Status

Tendenziell eher mit externem Monitoring prüfen



Event Generator – Statistics

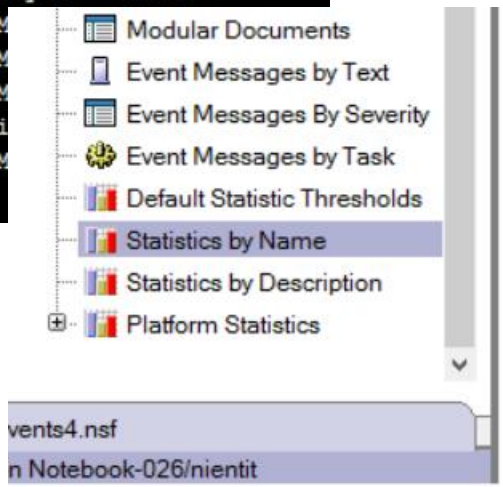
Solche Generators funktionieren nur für Statistiken, die „Threshold enabled“ sind

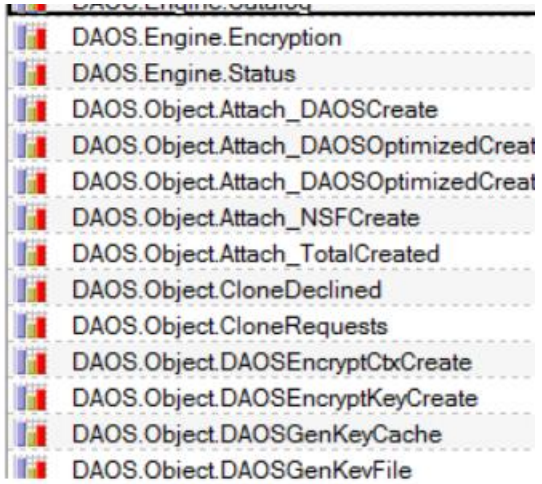


Probes und Events - Statistiken

- Show stat für alle ca. 1200 Statistiken
- Show stat platform für die Platformstatistiken

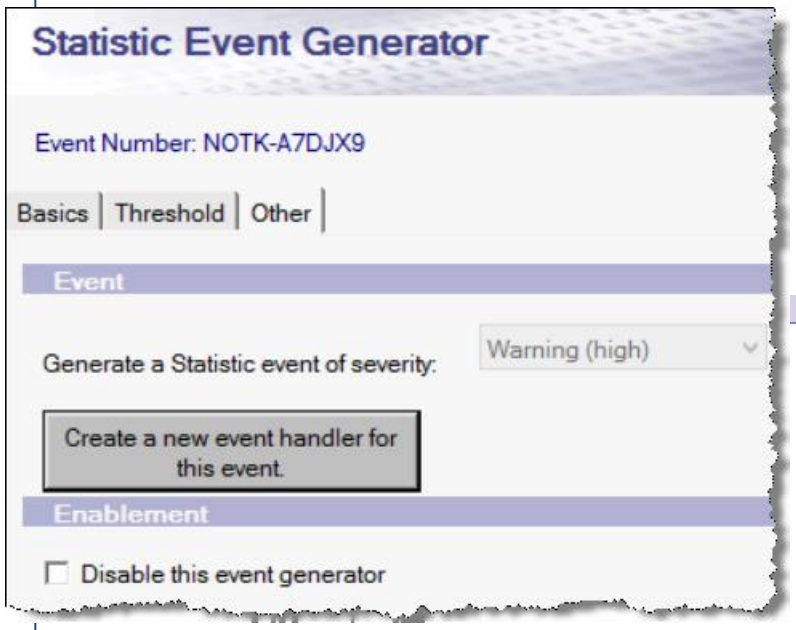
```
show stat platform.mem*
[2D08:000B-3E6C]    Platform.Memory.PageFaultsPerSec = 13.797,15
[2D08:000B-3E6C]    Platform.Memory.PagesPerSec = 399,98
[2D08:000B-3E6C]    Platform.Memory.PagesPerSec.Avg = 70,76
[2D08:000B-3E6C]    Platform.Memory.PagesPerSec.Peak = 1.312,68
[2D08:000B-3E6C]    Platform.Memory.RAM.AvailMBytes = 6.104
[2D08:000B-3E6C]    Platform.Memory.RAM.AvailM
[2D08:000B-3E6C]    Platform.Memory.RAM.AvailM
[2D08:000B-3E6C]    Platform.Memory.RAM.AvailM
[2D08:000B-3E6C]    Platform.Memory.RAM.PctUti
[2D08:000B-3E6C]    Platform.Memory.RAM.TotalM
[2D08:000B-3E6C]    10 statistics found
```





Probes und Events - Handler

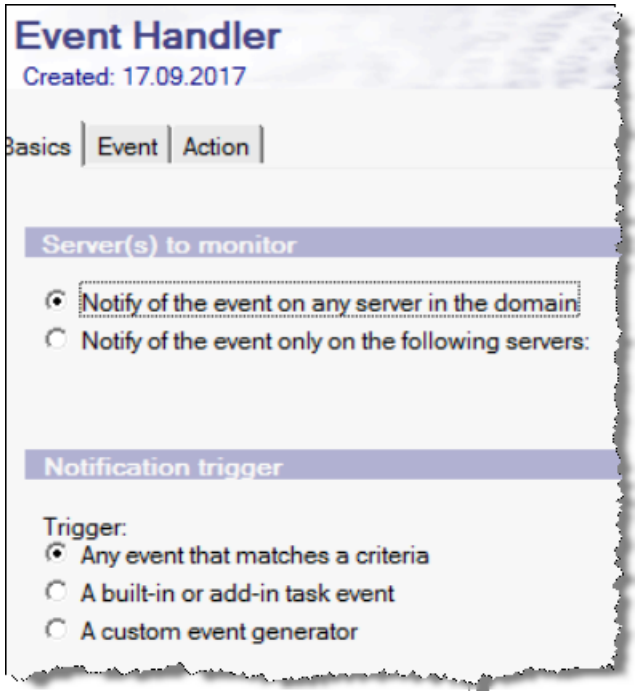
Die vermutlich interessantesten: Mail, Log, Trap

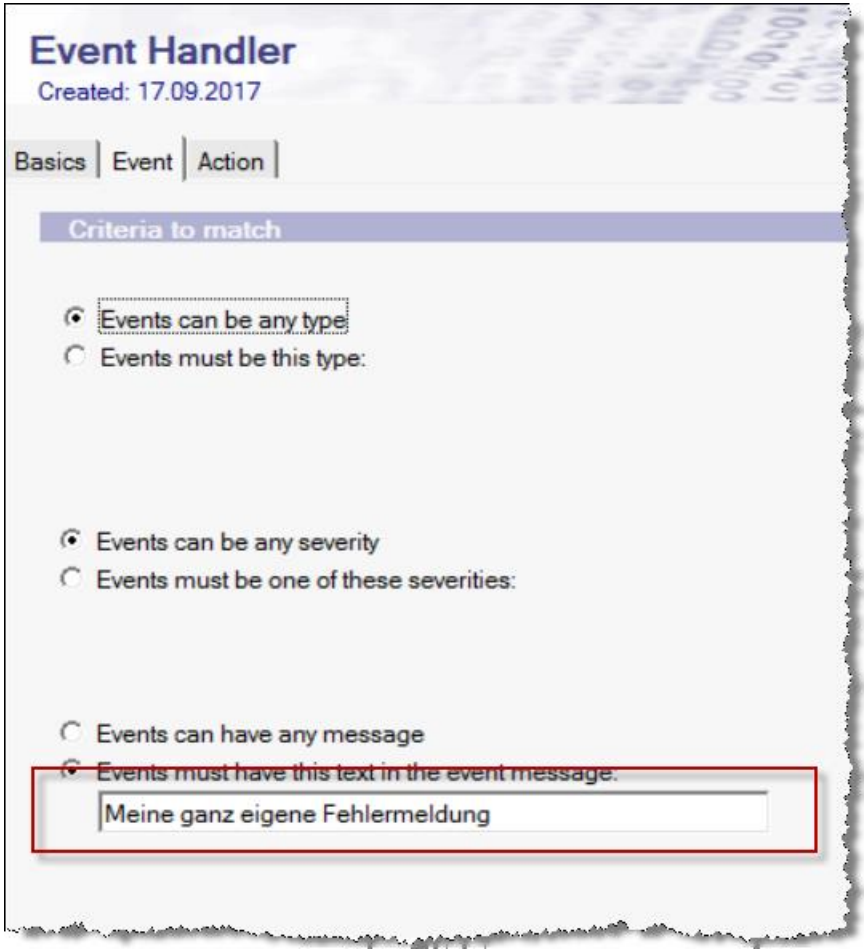


	Method	Description
	Broadcast	Broadcast
	EventAgent	Run an agent
	EventControler	Send Java Controller Command
	EventRemCon	Send a console command to the server
	Log	Log to a database
	Mail	Mail
	NTLog	Log to Event Viewer
	Pager	Pager
	Prog	Run Program
	Relay	Relay to other server
	SOUND	Sound
	TEC	Forward event to Tivoli Enterprise Console
	Trap	SNMP Trap
	UNIXLog	Log to Unix System Log

Probes und Events - Handler

Handler für spezielle Aufgaben:





Probes und Events – Vorschläge für Handler

Type	Event	Notication method (R/N/P)	Stakeholder
Built-In-Event	Router: Unable to failover to another cluster member for <name> <database name>	N	Domino-Administratoren
Built-In-Event	Unable to failover replica ID (<id>) from server <name> to any other cluster member	N	Domino-Administratoren
Built-In-Event	Unable to redirect failover from <name> for replica id <id>	N	Domino-Administratoren
Custom Event	Lookup Search	N	Domino-Administratoren
Custom Event	Mail Flow Statistic	P	Domino-Administratoren Mailsender
Custom Event	Mail Reflector	P	Domino Administratoren, Mailsender

Probes & Events – Vorschläge für Generator

Typ	Name	Alarmwert	Alarmtyp	Stakeholder
Statistic	Server.Availability.Index	0	R	Domino-Administratoren
Statistic	Replica.Cluster.SecondsOnQueue	30	R	Domino-Administratoren
Statistic	Replica.Cluster.WorkQueueDepth	10	R	Domino Administratoren
Statistic	DAOS.Engine.Catalog	!= Synchronized	N	Domino-Administratoren

Externes Monitoring – Warum?

Weil:

- Domino sich nicht überwachen kann, wenn es ausgefallen ist
- bereits externe Werkzeuge da sind, die Ereignisse in Beziehung setzen können
- Man in Domino nichts sagen, dass mich ein Zustand erst interessiert, wenn er eine Häufigkeit oder Dauer hatte
- möglicherweise auch schon Kommunikations- und Eskalationswege fertig definiert sind
- Security Intelligence-Werkzeuge daran angebunden sind/werden können
- Es bequem ist die Detailkonfiguration anderen zu überlassen

Externes Monitoring

- OS-Ebene
  - Verfügbarkeit von Diensten
  - Hardware-Status
- Agentless
  - SNMP - Domino-Statistiken mit standardisierter Schnittstelle
  - Textbasiert – 3rd Party wertet die Logs auf bestimmte Schlüsselbegriffe aus
- Agentbased
  - Zugriff über NRPC
  - Komplexe Anfragen möglich
  - Abfragen auf die versteckteren Infos (z.B. domlog.nsf) möglich

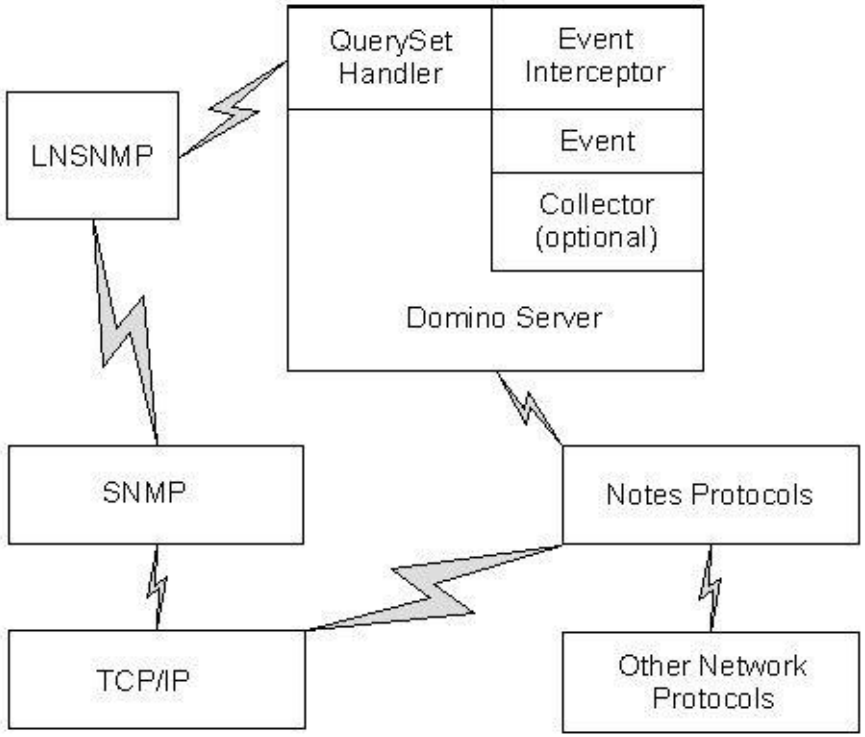
Externe Monitoring – SNMP

Simple Network Monitoring Protokoll

- Weltweit eineindeutige OIDs (MIB)
- Port: UDP 161 (Default)
- Domino MIB liegt im Datenverzeichnis
- OIDs dokumentiert auf diversen Webseiten

Externes Monitoring - SNMP

- Domino Agent
- Domino-Dienst(e)
- OS-Dienst
- SNMPv1 unsicher



Externes Monitoring – SNMP einrichten

- Windows Dienst registrieren:
  - Lnsnmp –Sc
  - Net start snmp
  - Net start lnsnmp
- Domino Dienste starten
  - Quryset (must)
  - intrcpt (für Traps)
  - Collect
- MIBs liegen im Datenverzeichnis

Externes Monitoring – Zusätzliche Hinweise

- Manche Dienste haben keine feste OID
  - Tool sollte dynamische OIDs verwalten können
- Manche Events ergeben nur zusammen (korreliert) einen Sinn
  - Bestimmter Nutzer meldet sich zur ungewöhnlichen Zeit an und versendet ungewöhnlich viel Mail -> Hack?
- Die Abhängigkeiten zwischen Systemen abzubilden, erleichtert die Kommunikation bzw. verringert Fehlalarme

Externes Monitoring – Mail

Bei Mail ist zu berücksichtigen, wie notifications übertragen würden – ggf. muss eine page ausgelöst werden

Name/OID	Alarmwert	Alert (normal/correlation/SPOF)	Stakeholder
Mail.Dead/ 1.3.6.1.4.1.334.72.1.1.4.1	> 10	N/P/P	Gesamt-IT Domino-Administratoren
Mail.Hold/ 1.3.6.1.4.1.334.72.1.1.4.21	> 20	N/P/P	Gesamt-IT Domino-Administratoren
MAIL.TotalFailures/ 1.3.6.1.4.1.334.72.1.1.4.3	> 100	N	Domino-Administratoren

Externes Monitoring – OS-Ebene

Parameter	Alarmwert	Alert (normal/correlation/ SPOF)	Stakeholder
Domino-Dienst (nserver.exe)	Läuft nicht	N/P/P	Domino-Administratoren 1st Level-Support Ggf. Fremdclients (SMTP, POP3, LDAP)
nsmtp.exe	Läuft nicht	N/P/P	Domino-Administratoren SMTP-Clients
npop3.exe	Läuft nicht	N/P/P	Domino-Administratoren Fremdclients
Nldap.exe	Läuft nicht	R/N/N	Domino-Administratoren LDAP-Clients
Nhttp.exe	Läuft nicht	N/N/N	Domino-Administratoren
Disk frei	< 10%	N	Domino-Administratoren Storage-Betreuer
Disk Queue Length	> 1	R	
Disk Response	> 10ms	R	
CPU percent used	> 10min bei 100%	R	Domino-Administratoren
CPU Queue Length	> 5/Kern	R	Domino-Administratoren
RAM Percent used	> 90%	R	Domino-Administratoren
Pagefile Size (sofern dynamisch)	> 1Gb	R	Domino-Administratoren

Externes Monitoring

Port/Dienst	Alarmwert	Alert (normal/correlation/SPOF)	Stakeholder
NRPC (1352 TCP)	Nicht erreichbar	N/P/P	Domino-Administratoren 1st Level-Support Ggf. Fremdclients (SMTP, POP3, LDAP)
SMTP/s (25 TCP)	Nicht erreichbar Antwort<>200 Maildelivery-Time > 10sec	N/P/P	Domino-Administratoren SMTP Clients
POP3 (110/993 TCP)	Nicht erreichbar Antwort<>200 Total Response Time > 30sec	N/P/P	Gesamt-IT (weil Ticketmgmt ausgefallen)
LDAP (389 TCP)	Nicht erreichbar Antwort<>200 Response Time > 5sec	R/N/N	Domino-Administratoren LDAP-Clients
http (80/443 TCP)	Nicht erreichbar Antwort<>200 Response Time > 10sec	N/P/P	Domino-Administratoren
SNMP (161 UDP)	Nicht erreichbar Response Time > 20ms	N/N/N	Domino-Administratoren „Nagios“-Administratoren

Externes Monitoring - Textbasiert

Es gibt Systeme, die auf die Auswertung von Textdateien nach definierbaren Kriterien spezialisiert sind.

- console.log ist eine Textdatei, die Informationen über den Systemzustand enthält

->

Worauf achten?

- Gehäufte Anmeldungsfehler (Webserver)
- Viele abgewiesene SMTP-Versuche (Rejected for Policy Reason)
- Webzugriff auf .php(??)

Externes Monitoring - agentbasiert

Kann potentiell alle Daten, die Domino sammelt auswerten

Hersteller bringen u.U. bereits sinnvolle Standardkonfigurationen mit

Einer der Hersteller läuft vertreten durch mehrere Personen hier herum

P

Kleine Spinnerei

Wenn auf der einen Seite der „Citizen Developer“ immer mehr Anwendungen ins System schmeißt, aber der Admin gleichzeitig die Kontrolle (Schnittstellen, Sicherheit) haben muss. Wie geht das Zusammen?

Dann müssen wir doch auch jederzeit über Anwendungen informiert und eine idealerweise automatisierte Auswertung durchführen können.

Gibt’s da auch was von Ratiopharm?

Fragen?

Jetzt stellen oder später…

Interessante Quellen

Domino SNMP konfigurieren:

http://www-01.ibm.com/support/docview.wss?uid=swg21169283

SNMP in Windows konfigurieren:

http://www.ibm.com/support/knowledgecenter/SSKTMJ_8.5.3/com.ibm.help.domino.admin85.doc/H_CONFIGURING_THE_DOMINO_SNMP_AGENT_FOR_WINDOWS_OVER.html?lang=de

SNMP in Linux konfigurieren:

http://www.ibm.com/support/knowledgecenter/SSKTMJ_8.5.3/com.ibm.help.domino.admin85.doc/H_CONFIGURING_THE_DOMINO_SNMP_AGENT_FOR_LINUX_OVER.html?lang=de

Übersicht über den MIB-Tree:
http://support.ipmonitor.com/mibs/NOTES-MIB/tree.aspx