



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

The screenshot shows the IBM Domino Administration Center interface. The top navigation bar includes 'People & Groups', 'Files', 'Server...', 'Messaging...', 'Replication', and 'Configuration'. Below this, there are tabs for 'Status', 'Analysis', 'Monitoring', 'Statistics', and 'Performance'. The 'Monitoring' tab is active, showing a 'By State' dropdown and a checkbox for 'Show me past error states only'. A table displays server task data for 'Notebook-026/nientit'. A context menu is open over the table, listing options like 'Profile Properties...', 'Monitor New Statistic...', 'Remove Statistic', 'Create Event Generator', 'Show Statistic's Difference', 'Switch to Status Tab', 'Switch to Messaging Tab', 'Switch to Health Reports', 'Switch to DDM', and 'Profiles'. A dialog box titled 'Add Server Task(s) to this Profile' is open, showing a list of tasks to add, including 'Activity Trends Collector', 'Administration Process', 'Agent Manager', 'Billing', 'Calendar Connector', 'Cataloger', 'cc:Mail MTA', 'Certificate Authority (CA) Process', 'Change Manager', 'Chronos', 'Cluster Administration Process (R4/R5 or R6)', 'Cluster Database Directory Manager', and 'Cluster Replicator'. A description for the 'Activity Trends Collector' task is visible at the bottom of the dialog.

Hea	17:06:25 - 17:06:25	Adm	Age	Dat	Eve	Ind	Rep	Rou	Sta	Users	Dead	Hold	Waiting	AvailabilityIndex	ElapsedTime
-	Notebook-026/nientit									1	0	0	0	4	00:01:13



Holschuld - Monitor-Tab – Traveler Task

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

The screenshot shows the Domino Designer interface. On the left is a tree view of applications, including Task\ldap, Task\maps, Task\mtc, Task\nntp, Task\object, Task\pop3, Task\queryset, Task\rdebug, Task\reflect, Task\replica, Task\report, Task\rmeval, Task\rnmgr, Task\router, Task\runjava, Task\sched, Task\smtp, and Task\smtpmta. The main window displays the 'Task\traveler - Form' configuration. At the top, there are two tabs: 'Parse_Load T' and 'Parse_Tell T'. Below them is a 'Basics' table with the following rows:

Basics		
Task name:	<input type="text" value="Task_name T"/>	
Task filename:	<input type="text" value="Task_filename T"/>	
Task Monitor Name:	<input type="text" value="Task_monitorname T"/>	
Description:	<input type="text" value="Task_description T"/>	
Has "LOAD" UI:	<input type="radio"/> Task_hasLoadUI	<input type="text" value="\$Task_LoadCmd T"/>
Has "TELL" UI:	<input type="radio"/> Task_hasTellUI	<input type="text" value="\$Task_TellCmd T"/>

Below the table, there are two panels. The 'Objects' panel shows a tree view for 'Task_filename (Field)' with sub-items: Default Value, Input Translation, and Input Validation. The 'Reference' panel shows the 'Task_filename (Field) : Default Value' configuration. It has a 'Run' dropdown set to 'Client' and a 'Formula' field containing the text "traveler" in pink.



Holschuld - DDM

The screenshot shows the DDM interface with the following elements:

- DDM Header:** Open Events, Recent Events, All Events. Sub-header: All open events, sorted by date.
- Toolbar:** Refresh, Assign..., Change State, Add Comments...
- Table:** Columns: #, Time, Server, By Date, Assigned To. Row 1: 7, So 10.09.2017.
- Assign Event(s) Dialog:** Assign selected event(s) to: Administrator (empty), Myself: Manuel Nientit/assono. Add comments for the selected event(s): Programmierfehler - an Entwicklerübergaben.
- Event List:**

#	Time	Server	By Date	Assigned To
7	So 10.09.2017			
ook-026/nientit	Security: Configuration	?	Security Best Practices Probe: Potential security risks have been found in 4 Person Document(s) ...	
ook-026/nientit	Security: Configuration	?	Security Best Practices Probe: Server Configuration Documents have been analyzed, and 66 percent of the configuration does not match recommended best practices.	
Servers]	Security: Configuration	?	Security Best Practices Probe: Server Configuration Documents have been analyzed, and 55 percent of the configuration does not match recommended best practices.	
ook-026/nientit	Security: Configuration	?	Security Best Practices Probe: Server Documents have been analyzed, and 37 percent of the configuration does not match recommended best practices.	
ook-026/nientit	Security: Access	?	Database review for 'mail\' has completed.	
ook-026/nientit	Server	!	Unable to run program td_grab.EXE: Unable to locate	admin admin



Holschuld – DDM Collection Hierarchy

The screenshot shows the IBM Domino Administration Center interface. On the left, the 'Monitoring Configuration' tree is visible, with 'Server Collection Hierarchy' selected. A red arrow points from this menu item to the 'New Server Collection Hierarchy' dialog box. The dialog box has a title bar that also says 'New Server Collection Hierarchy'. Inside the dialog, the question 'How would you like to configure the server collection hierarchy?' is followed by two radio button options: 'One server will collect from all servers in the domain' (which is selected) and 'Define the hierarchy'. Below these options is a section titled 'Choose the collecting server:' with a dropdown menu showing 'Notebook-026/nientit'. Underneath is a text input field with the placeholder 'Please enter a description'. At the bottom of the dialog, there is explanatory text: 'Sets the selected server as the collecting server for all other servers in the domain. All eligible servers are automatically added to the server collection hierarchy.' and two buttons: 'OK' and 'Cancel'.



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:

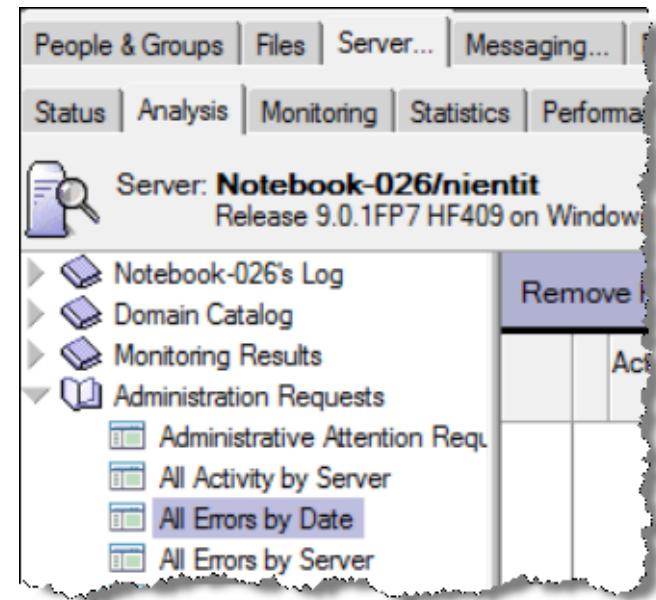
1. Mailrouting/Kommunikation
2. App-Server
3. Web/Traveler



Holschuld – Adminp/4

Ca. wöchentlich (Montags) Admin4.nsf prüfen

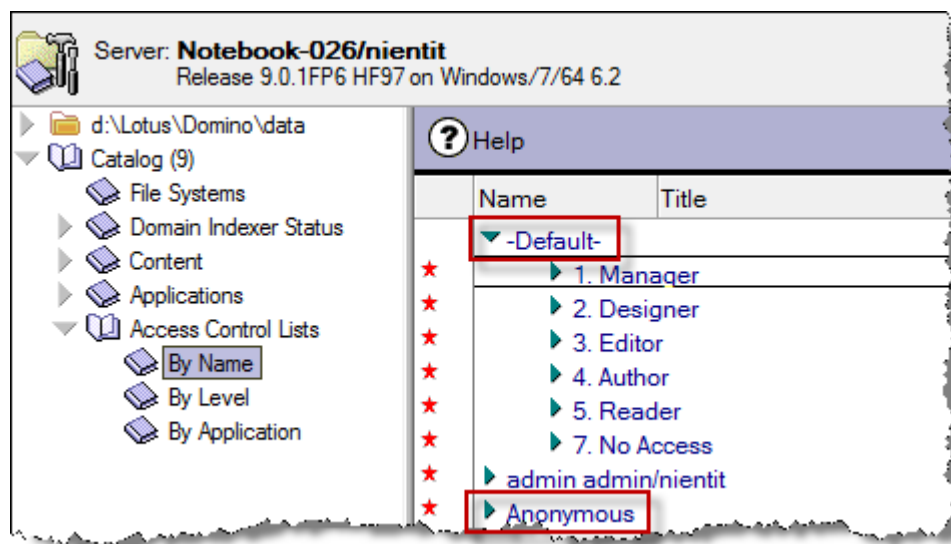
- Fehler bei der Nutzerverwaltung
 - Recert
 - Löschung
 - Umbenennung
- HTTP-Passwortänderungen





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

The screenshot shows the 'Monitoring Configuration' window. On the left is a tree view under 'DDM Configuration' with 'By Type' selected. On the right is a table with the following data:

Total	Enabled	Type	Probe Description
11	0	Administration	
7	0	Application Code	
4	0	Database	
10	0	Directory	
12	2	Messaging	
4	0	Operating System	
2	1	Replication	
5	3	Security	
1	0	Server	
2	0	Web	
58	6		



Probes and Events - Filters

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

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

Domino Domain Monitor Filter

Description:
DDM Default Filter to allow reporting of all simple events with fatal or failure severity.

Event Filter:

Apply filter to enhanced and simple events
 Only apply filter to simple events

Event Types and Severities to Log:

Log All Event Types Log Selected Event Types

Fatal Failure Warning(High) Warning(Low) Normal

Servers on which the filter will be applied:
All servers in the domain



Probes & Events - Automatic Report Closing

Basics | Schedule

Basics

Probe Type: Administration

Probe Subtype: Automatic Report Closing

Probe Description: Default Administration/Automatic Report Closing - database and view

This probe periodically closes Event Reports that have remained open for the specified period of time, but have been in an issue. Any report closed by this probe will be reopened should the error reoccur.

Target

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

Specifics

Errors to periodically close: B-tree structure is invalid [[0x028E]]
Database is corrupt -- Cannot allocate space [[0x0238]]
Entry not found in index [[0x0404]]
This database cannot be read due to an invalid on disk structure [[0x0601]]

Number of days to remain open: 14



Probes and Events – Application Code

Agenten:

- Lang laufend
- verspätet
- Hohe CPU-Last

Application Code Probe: SOKE-62FUX6

Basics

Probe Type:	Application Code
Probe Subtype:	Agents behind schedule
Probe Description:	Default Application Code/Agents Behind Schedule Probe

This probe detects when the start of agent execution falls behind the scheduled time for agents run by the Agent Scheduler. This is 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 agent is running behind schedule by more than:	Generate an event of severity:
<input checked="" type="checkbox"/> Enabled	60 minutes	Fatal
<input checked="" type="checkbox"/> Enabled	45 minutes	Failure



Probes und Events - Database Probes

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

Database Probe: SOKE-62FUZY

Basics

Basics

Probe Type: Database

Probe Subtype: Error Monitoring

Probe Description: [Default Database/Error Monitoring Probe]

This probe monitors key locations in the database software layer (NSF/NIF) and generates events. This probe is not configurable.

Target

Which servers should run this probe?

All Servers in the domain

Special Target Servers

Only the following servers:

Specifics

Severity: Warning (high) [v]

Errors to ignore: [Add Error Codes To List] [Remove Error Codes from List]

File does not exist [[0X0103]]
File object is truncated - file may have been damaged [[0X024F]]
Memory allocation request exceeded 65,000 bytes [[0X013B]]



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 standard LDAP search response times. 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?	<input checked="" type="radio"/> All Servers in the domain
	<input type="radio"/> Special Target Servers
	<input type="radio"/> Only the following servers:

Specifics

Event generation status:	If the Name Lookup response exceeds:	Generate an event of severity:
<input checked="" type="checkbox"/> Enabled	2000 milliseconds	Fatal
<input checked="" type="checkbox"/> Enabled	1500 milliseconds	Failure
<input checked="" type="checkbox"/> Enabled	1200 milliseconds	Warning High
<input type="checkbox"/> Enabled	800 milliseconds	Warning Low

- Directory
 - Directory Availability
 - Directory Catalog Aggregation Schedule
 - Directory Catalog Creation
 - Directory Indexer Process State
 - LDAP Process State
 - LDAP Search Response
 - LDAP TCP Port Health
 - LDAP View Update Algorithm
 - Name Lookup Search Response
 - Secondary LDAP Search Response



Probes und Events - Mail Flow Statistic

- [-] Messaging
 - [+] Mail DSN
 - [+] Mail Flow Statistic Check
 - [+] Mail Reflector
 - [+] Message Retrieval Process State
 - [+] Message Retrieval TCP Port Health
 - [+] NRPC Routing Status
 - [+] Router Process State
 - [+] SMTP Process State
 - [+] SMTP TCP Port Health
 - [+] Transfer Queue

Messaging Probe: SOKE-62FV6H - DISABLED

Basics			
Probe Type:	Messaging		
Probe Subtype:	Mail Flow Statistic Check		
Probe Description:	Default Messaging/Mail Flow Statistic Check Probe		
<p>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 exceed a specified limit (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 percentage is the percentage of the pending message limit that is allowed to be exceeded before an event is generated.</p>			
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:
<input checked="" type="checkbox"/> Enable	Not Applicable	20	Fatal
<input type="checkbox"/> Enable	100	Not Applicable	Failure
<input type="checkbox"/> Enable	50	Not Applicable	Warning (High)
<input type="checkbox"/> Enable	25	Not Applicable	Warning (Low)



Probes und Events – Mail Reflector Probe

Mail an Echomailer – Antwortzeit wird gemessen

Messaging Probe: SOKE-62FV7E - DISABLED

Basics | Schedule

Basics

Probe Type: Messaging

Probe Subtype: Mail Reflector

Probe Description: Default Messaging/Mail Reflector Probe

This probe will test the mail flow to any mail system. To test mail flow to the destination mail domain, you will need to ensure that the subject of the original message must be contained in the subject of the returned message. One way to configure this is to use the Mail Recipient field. The subject of the message delivered by this probe to the mail recipient will not be automatically deleted from the mail file. You may want to set the Mail Recipient field to a specific email address.

Target

Which servers should run this probe?

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

Specifics

Mail Recipient: echo@tu-berlin.de

If the following timeout occurs: Generate an event of severity:

<input checked="" type="checkbox"/> Enable	600 seconds	Failure
<input type="checkbox"/> Enable	300 seconds	Minor (High)



Probes und Events – Operating System Probe

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

Operating System Probe: SOKE-62FVAY - DISABLED

Basics

Basics

Probe Type: Operating System

Probe Subtype: CPU

Probe Description: Default Operating System/CPU Probe

This probe monitors and analyzes processor utilization for the configured Domino server(s) and operating s

Target

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

Specifics

Which Operating Systems should be monitored?

AIX

Linux / zLinux

OS400

z/OS

Solaris

Windows

AIX | Linux / zLinux | OS400 | z/OS | Solaris | Windows

%Processor Utilization

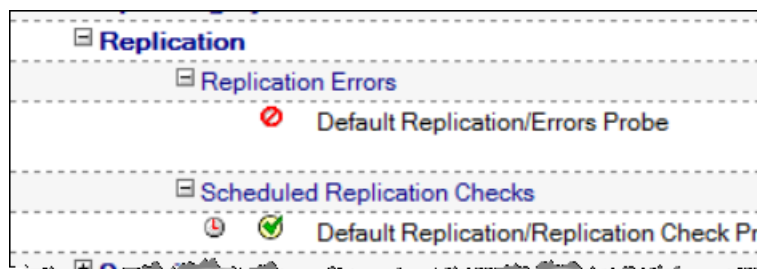
Greater Severity Threshold: 85 %

Lesser Severity Threshold: 75 %

The statistic used for %Processor Utilization is Platform.System.PctCombinedCpuUtil



Probes and Events - Replication



Replication Probe: SOKE-62FVCF

Basics | Schedule

Basics

Probe Type:	Replication
Probe Subtype:	Scheduled Replication Checks
Probe Description:	Default Replication/Replication Check Probe

This probe monitors configured database(s) to ensure that replication on Monitor database. **NOTE:** this probe takes into account replication atte

Target

Which servers should run this probe?	All servers in the domain
Server(s) with which the specified database(s) must replicate:	All servers in the domain
Select one or more databases to probe:	mail*



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)

Security Probe: SOKE-62FVD4

Basics | Specifics | Schedule

Specifics

Which server should be used as the guideline server? Notebook-026/nientit

Which server settings should be compared to the guideline server's settings?

- Directory Profile Note
- Security settings in the Server Configuration Document
- Server Document (All Sections)
- 'Admins' section
- 'P...



Probes and Events – Administration Probe

Server Probe: SOKE-62FVE9

Basics | Schedule

Basics

Probe Type:	Server
Probe Subtype:	Administration
Probe Description:	『Default Server/Administration Probe』

This probe monitors errors in processing the selected administration requests on the selected se

Target

Which servers should run this probe?

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

Specifics

Administration Requests:

- Change HTTP Password in Domino Directory
- Change User Password in Domino Directory
- Initiate Rename in Domino Directory
- Initiate Web User Rename in Domino Directory
- Recertify Certificate Authority in Domino Directory
- Recertify Cross Certificate in Domino Directory
- Rename in Person Documents
- Rename Person in Calendar Entries and Profiles in Mail File
- Rename Person in Domino Directory
- Rename Web User in Access Control List
- Set Password Information



Probes und Events - Generators

Es gibt sechs Arten von Generators:

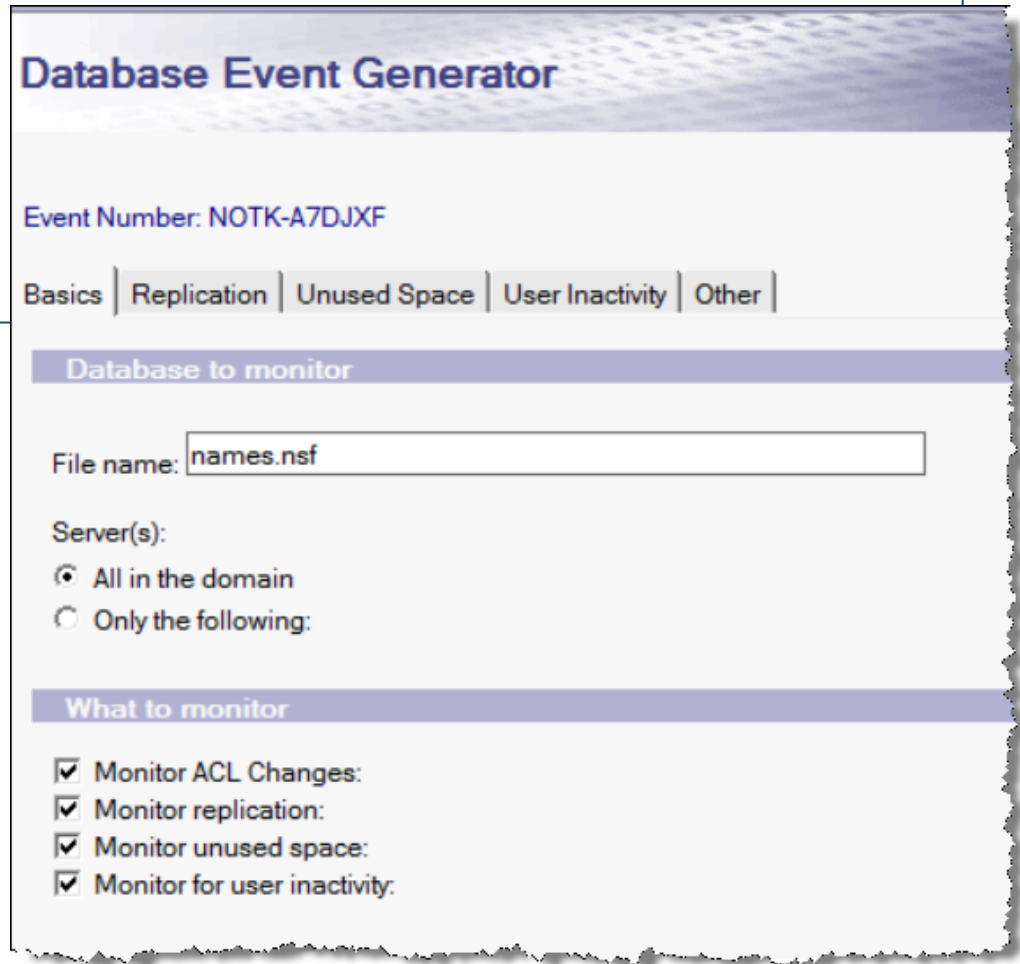
- Database
- Domino Server
- TCP Server
- Mail Routing
- Statistic
- Task Status

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?



Database Event Generator

Event Number: NOTK-A7DJXF

Basics | Replication | Unused Space | User Inactivity | Other

Database to monitor

File name:

Server(s):

All in the domain

Only the following:

What to monitor

Monitor ACL Changes:

Monitor replication:

Monitor unused space:

Monitor for user inactivity:



Event Generator - Server

Domino Server Event Generator

Event Number: ADMN-ARAMSE

Basics | Probe | Other

Target server(s)

Server(s):

▼

Probing server (source)

Server:

▼

Access

Interval: Minutes

Check just the ability to access the destination server

Check the ability to access the destination server and open this database:

File name:

Domino Server Event Generator

Event Number: ADMN-ARAMSE

Basics | Probe | Other

Ports

Perform probe using any available port

Time

Timeout threshold: Msecs

Resulting statistic

SERVER.<Probing Server>.<Destination Server>



Event Generator – TCP Probes

TCP Server Event Generator

Event Number: NOTK-A7DJXH

Basics | Probe | DNS | HTTP | IMAP | LDAP | NNTP | POP3 | SMTP | Other

All Domino servers in the domain will probe their own configured ports

Target Server(s)

All in the domain

Only the following:

▼

Probing server(s) (source)

▼



Event Generator – TCP Probes

TCP Server Event Generator

Event Number: NOTK-A7DJXH

Basics | Probe | DNS | HTTP | IMAP | LDAP | NNTP | POP3 | SMTP | Other

Resulting statistic: QOS.HTTP.<Destination Server>.[NOTK-A7DJXH].ResponseTime

Resulting statistic: QOS.HTTPSSL.<Destination Server>.[NOTK-A7DJXH].ResponseTime

Probe just the port

Fetch this URL:

http://<ServerAddress>/lotustraveler.nsf



Event Generator – Mail Routing

Mail Routing Event Generator

Event Number: ADMN-ARAMWW

Basics | Probe | Other

All Domino servers in the domain will probe themselves

Target mail address (destination)

Recipient:

▼

Note: Only one mail address should be listed as the recipient. Do not use group names or multiple a

Probing servers (source)

Server(s):

▼

Show intermediate hop times QOS. Mail. from.<ServerName>.to<ServerName>.ResponseTime
Show intermediate hop response times



Event Generator – Task Status

Tendenziell eher mit externem Monitoring prüfen

Task Status Event Generator
Event Number: ADMN-ARAMYH

Basics | Other

Tasks to monitor

Task name:

- Admin Process
- Agent Manager
- Billing
- Calendar Connector
- Cataloger

Server(s):

- All in the domain
- Only the following:

What to monitor

- Monitor task down
- Monitor task up
- Monitor task stalled
- Monitor task unstalled



Event Generator – Statistics

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

Statistic Event Generator

Event Number: ADMN-ARAN28

Basics | **Threshold** | Other

Server(s) to monitor

All in the domain
 Only the following:

Statistic to monitor

Type of statistics to monitor: Single instance statistic
 Template statistic

Statistic to monitor:

Description: Free space on drive C:

Monitor as a percent of the whole (Disk.C.Size)
 Monitor as a number (bytes)

Statistic Event Generator

Event Number: ADMN-ARAN28

Basics | Threshold | **Other**

Threshold

Generate the event when:

The statistic is LESS THAN the threshold value
 The statistic is GREATER THAN the threshold value
 The statistic is a MULTIPLE of the threshold value

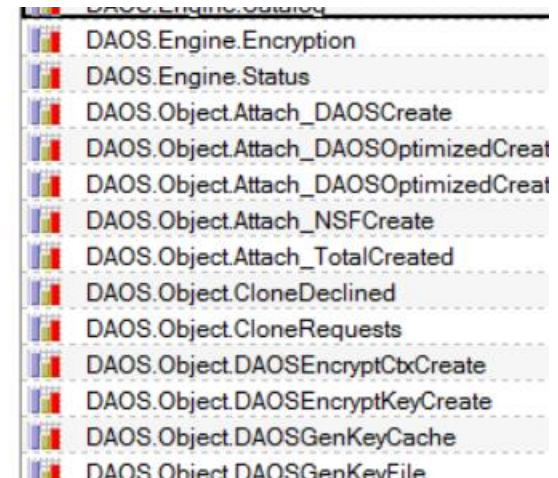
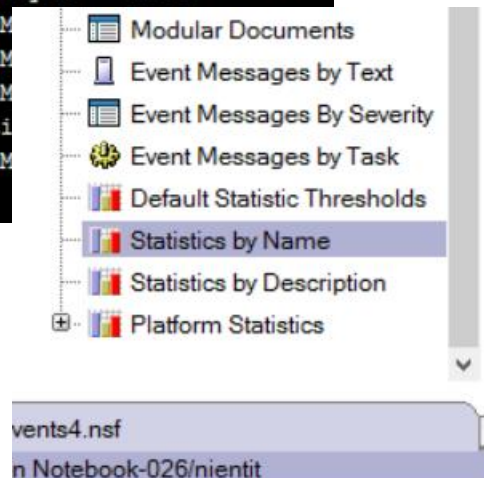
Threshold: bytes



Probes und Events - Statistiken

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

```
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

Statistic Event Generator

Event Number: NOTK-A7DJX9

Basics | Threshold | Other

Event

Generate a Statistic event of severity: Warning (high) ▾

Enablement

Disable this event generator

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



Probes und Events - Handler

Handler für spezielle Aufgaben:

Event Handler

Created: 17.09.2017

Basics | Event | Action

Server(s) to monitor

- Notify of the event on any server in the domain
- Notify of the event only on the following servers:

Notification trigger

Trigger:

- Any event that matches a criteria
- A built-in or add-in task event
- A custom event generator

Event Handler

Created: 17.09.2017

Basics | Event | Action

Criteria to match

- Events can be any type
- Events must be this type:
- Events can be any severity
- Events must be one of these severities:
- Events can have any message
- Events must have this text in the event message.



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

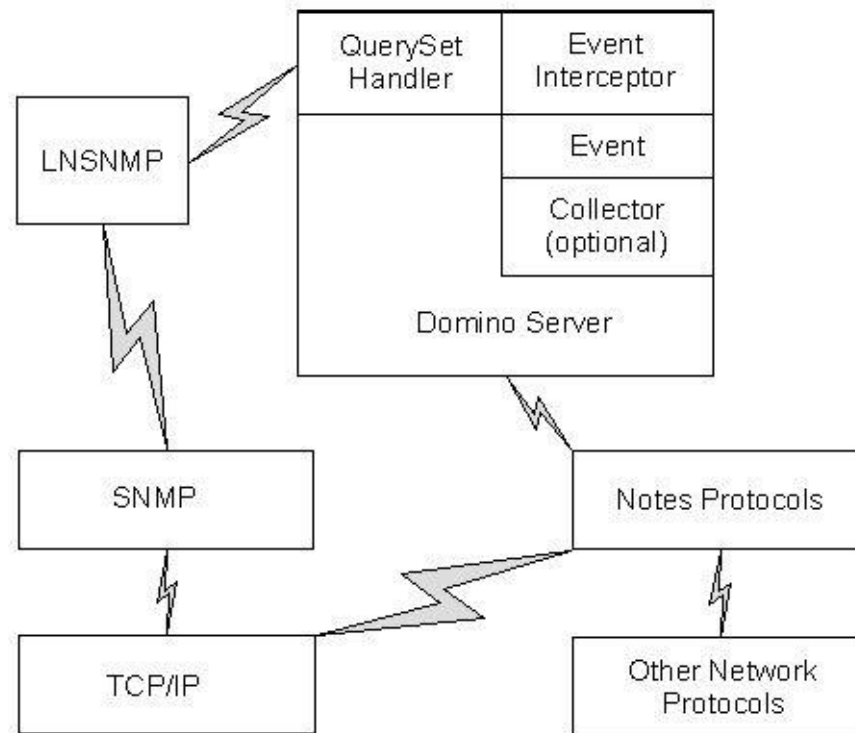
Simple Network Monitoring Protokoll

- Weltweit eindeutige 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/S POF)	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/SP OF)	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 Anmeldefehler (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>