UNIKLINIK KÖLN

Nachhaltige IT für Spitzenmedizin am UKK

Überwachen der IT Landschaft einer Uniklinik

Ein kurzer Überblick der IT einer Uniklinik und der Versuch diese sinnvoll zu überwachen

13.09.2017 Düsseldorf | Paul Dvoran | Klinikum der Universität zu Köln

UNIKLINIK KÖLN | uk-it

Organisationshierarchie einer Uniklinik

Die Klinikdirektoren entscheiden eigenständig im Rahmen ihrer Klinik.

UNIKLINIK KÖLN | uk-it

Hardware

- VMWare
  - 618 virtuelle ESX Server (Linux, Windows) auf 27 Hosts
- Citrix
  - 126 virtuelle XEN Server auf 25 Hosts mit 80 published Applications
- AIX
  - 80 LPARs auf 10 managed Systems (P6, P7, P8)
- Storage
  - NAS, SAN, Archivierung, SVC, Midrange Storage, Tape Libraries

UNIKLINIK KÖLN | uk-it

Software

- Datenbanken
  - Oracle, MSSQL, DB2, MySQL, Sybase, …
- Betriebswirtschaftliche Applikationen
  - Diverse SAP Systeme, Zeitmanagement, …
- Medizinische Applikationen
  - PACS, Laborsysteme, KIS, PDMS, ePA, …
- „Vagabunden“
  - Alles was sich „oben“ nicht einordnen lässt

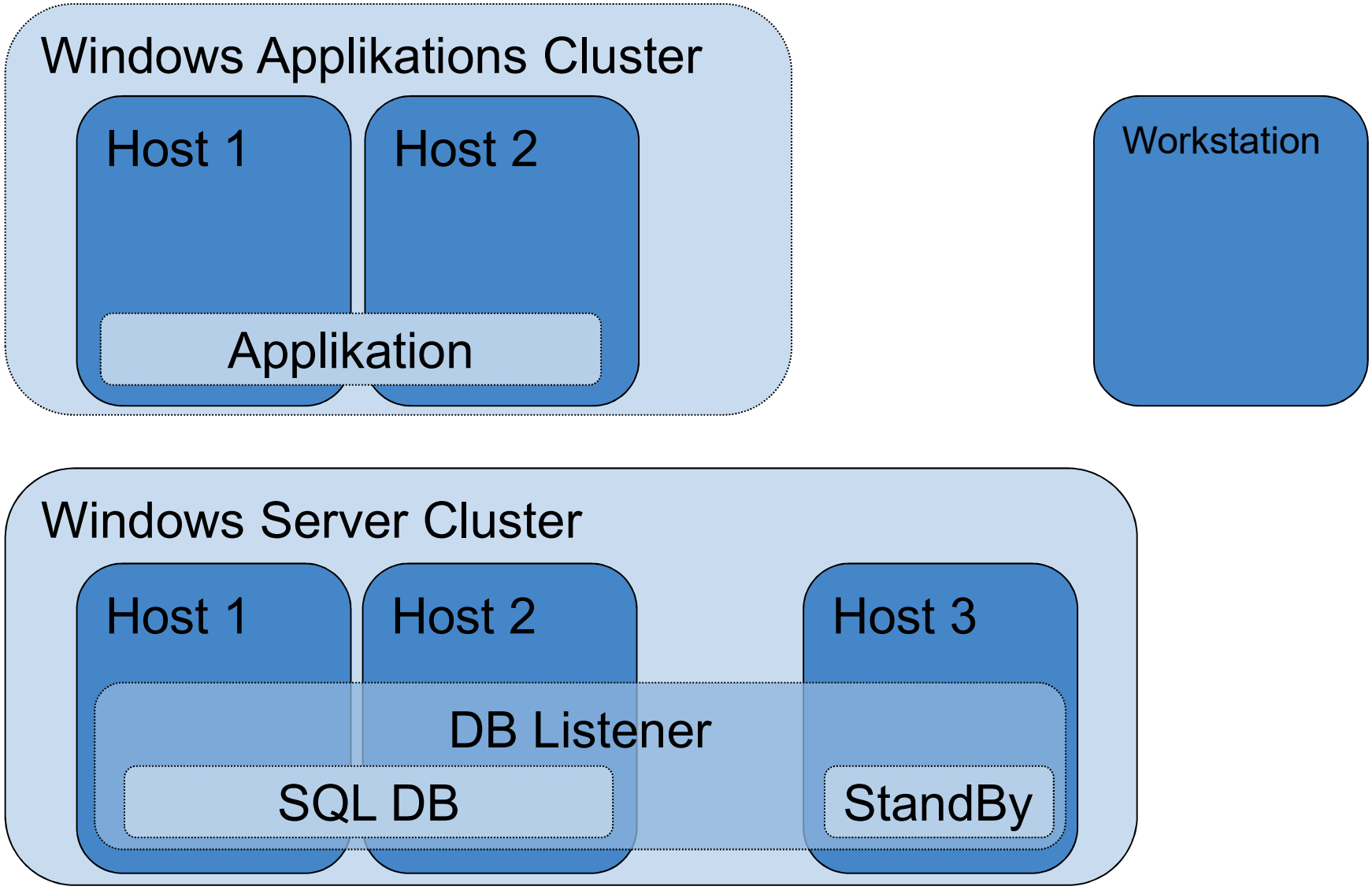
UNIKLINIK KÖLN | uk-it

Monitoring 1

- Aktuell ca. 1000 Hosts mit 16000 Services
- Basisüberwachung => Check_mk
- Datenbanken => check_..._health
- Storage => eigene Checks (Perl, Snmp, …)
- Alle Arten von Logfiles (Windows, Unix) => check_logfiles
- Rest => eigene Checks (Bash, Perl, Powershell, Batch, …)

Monitoring 2

- openITCockpit von itnovum mit Naemon darunter
- Mastersystem geclustert
- Verteiltes System mit mehreren Satelliten in verschiedenen Netzen
- Sehr viele Erweiterungen innerhalb des openITCockpits bereits integriert
- Überwachung von Prozessen mit Event Correlations


Windows Applikations Cluster
Host 1
Host 2
Applikation
Workstation
Windows Server Cluster
Host 1
Host 2
Host 3
DB Listener
SQL DB
StandBy

Monitoring 3 – PDMS Intensiv

- Verzeichnisse, CPU, RAM, Prozesse => check_mk
- MSSQL DB => check_mssql_health
- Clusterelemente => Powershell Scripte
- Replikation => Application Eventlog => check_logfiles
- Cluster => FailoverClustering Eventlog => check_logfiles

UNIKLINIK KÖLN | uk-it

Monitoring 4 – PDMS Intensiv

```
@searches = ({
        tag => 'evt_cluster',
        type => 'wevtutil',
        wevtutil => {
           eventlog => 'Microsoft-Windows-FailoverClustering/Operational',
        },
        options =>
        'sticky,noprotocol,supersmartscript,preferredlevel=critical,eventlogformat="%w
eventid:%i source:%s msg:%m"',
        criticalpatterns => [
           'eventid:1200.*', 'eventid:1201.*', 'eventid:1203.*', 'eventid:1204.*',
           'eventid:1205.*', 'eventid:1641.*,
        ],
        script  => sub {
           print "<a href='https://uk-koeln.de/logfiles/logfiles_nrpe.php?host=".„host.uk-
koeln.de"."&SSL=YES"."&logname=cluster_event.log'
target='_blank'>".$ENV{"CHECK_LOGFILES_SERVICEOUTPUT"}."</a>";
return $ENV{CHECK_LOGFILES_SERVICESTATEID};
        }
});
```

UNIKLINIK KÖLN | uk-it

Monitoring 5 – PDMS Intensiv

Next check in:	in 1 minute
Output:	CRITICAL - (1 errors) - 2017-08-25T14:17:29 eventid:1201 source:Microsoft-Windows-FailoverClustering'_Guid='{BAF908EA-3421-4CA9-9B84-6689B8C6F85F} msg:Der Clusterdienst hat die Clusterrolle "W-CLU-[redacted]-P-CNS" erfolgreich online geschaltet.
Performance data:	'evt_cluster_lines'=0 'evt_cluster_warnings'=0 'evt_cluster_criticals'=1 'evt_cluster_unknowns'=0

Unbestätigte Fehlermeldungen im eventlog_cluster fuer [redacted]-cn02.[redacted]

CRITICAL - (1 errors) - 2017-08-25T14:17:29 eventid:1201 source:Microsoft-Windows-FailoverClustering'_Guid='{BAF908EA-3421-4CA9-9B84-6689B8C6F85F} msg:Der Clusterdienst hat die Clusterrolle "W-CLU-[redacted]-P-CNS" erfolgreich online geschaltet. |'evt_cluster_lines'=0 'evt_cluster_warnings'=0 'evt_cluster_criticals'=1 'evt_cluster_unknowns'=0

Bestätigen

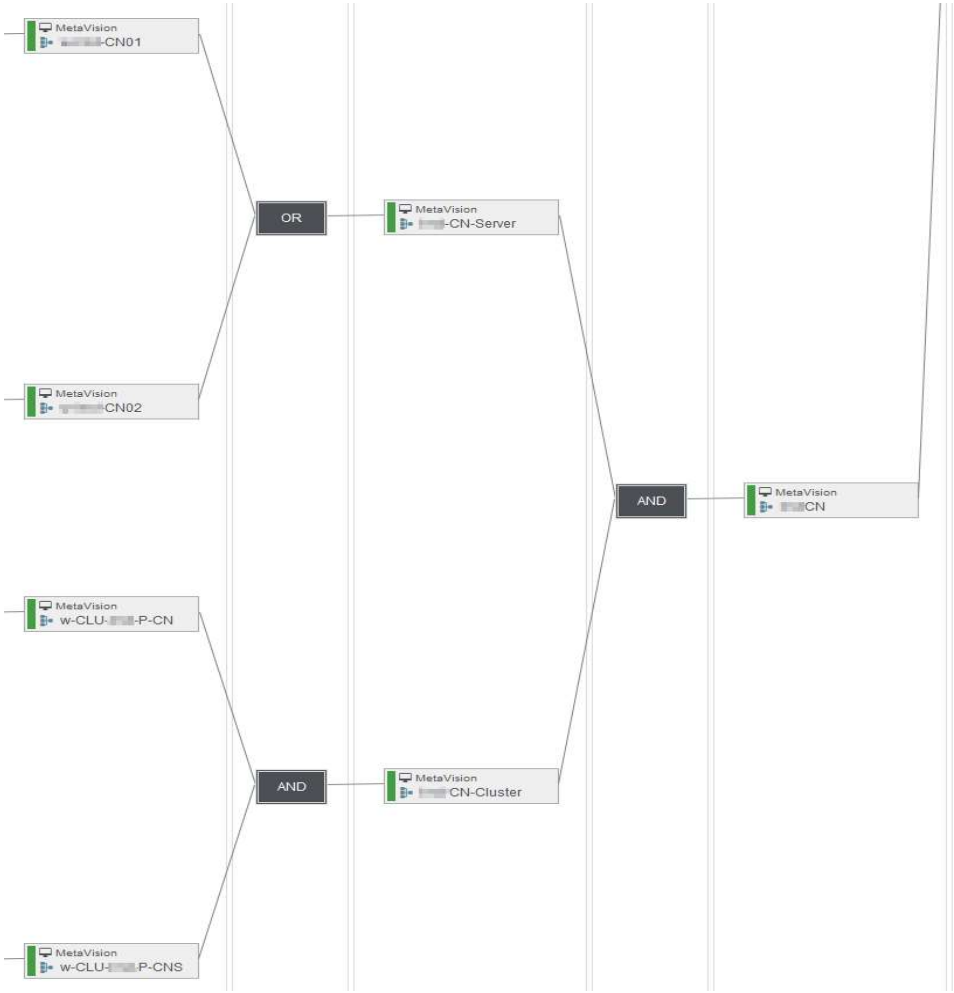
Unbestätigte Fehlermeldungen im eventlog_cluster fuer [redacted]-cn02[redacted]

OK - no errors or warnings|'evt_cluster_lines'=0 'evt_cluster_warnings'=0 'evt_cluster_criticals'=0 'evt_cluster_unknowns'=0

Bestätigen

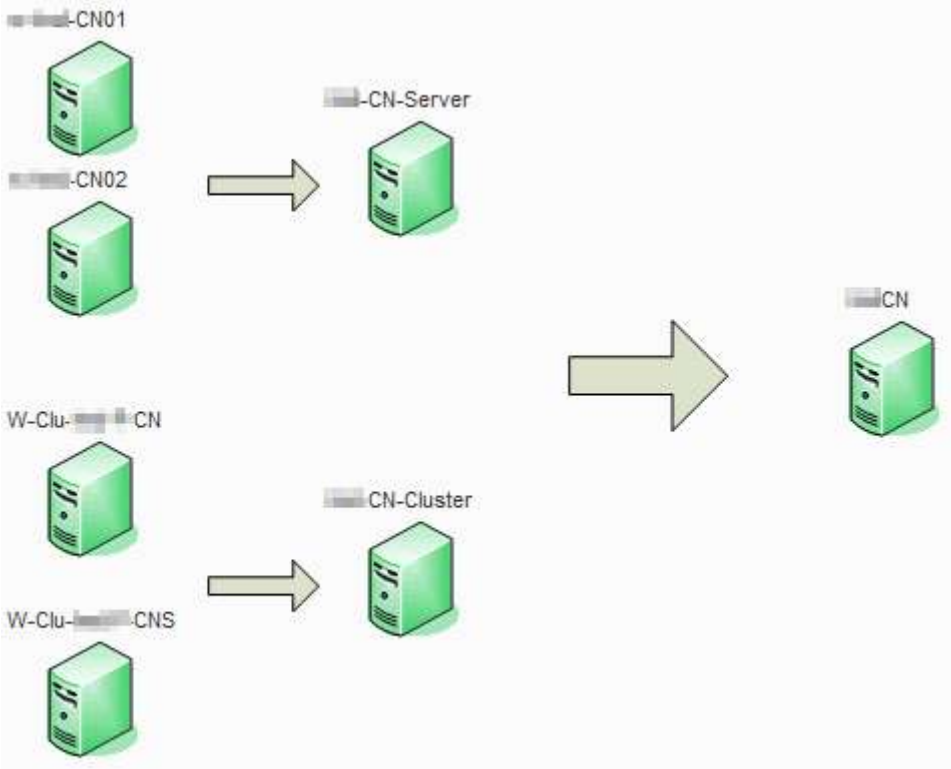
UNIKLINIK KÖLN | uk-it

Monitoring 6 – PDMS Intensiv



UNIKLINIK KÖLN | uk-it

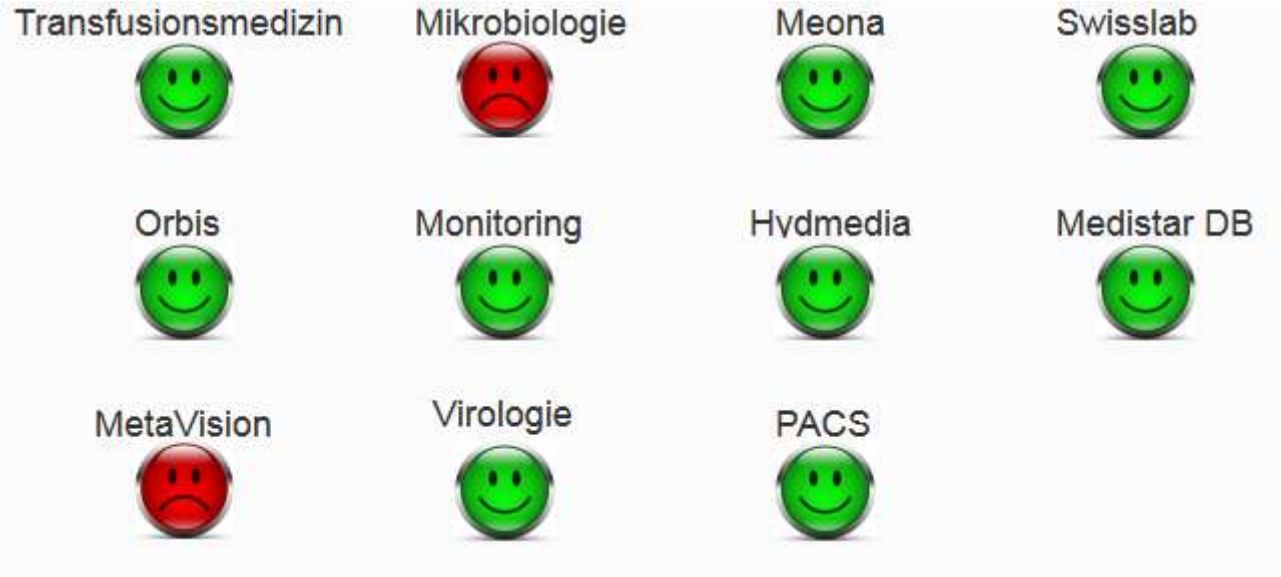
Monitoring 7 – PDMS Intensiv



Virtuelle Service Checks haben auch Nagios konformen Status.

Monitoring 8

Ansicht der wichtigsten Systeme auf dem Dashboard



Noch Fragen?

Gerne auch per Mail:
Paul.dvoran@uk-koeln.de

Vielen Dank für die Aufmerksamkeit .