Ist mein Server gesund?

jenseits von Monitoring…

Motivation und Format

Ist Monitoring nicht genug?

- Exchange ist ein Überlebenskünstler und hat seit 2013 erhebliche Selbstheilungskräfte
- Service-Monitoring ist essentiell wichtig für den Betrieb
  - Verlässt man sich aber nur auf diese, können sich Fehler einschleichen, die irgendwann zu katastrophischen Ereignissen führen oder beispielsweise ein CU-Update verhindern
- Ein kompletter Health Check ist oft aufwendig und daher für den Monitoring-Turnus schlecht geeignet
  - Daher muss er in einem weniger dichten Turnus durchgeführt warden
- … was macht ihr so dafür?

...was schon mal klar wäre...

- Einen Health Check bei Exchange sollte man nur durchführen, wenn die Service-Gesundheit optimal ist
  - Am besten ein paar Wochen nach einem CU – dann hat sich genügend forensisches Material angesammelt, und bis zum nächsten CU ist noch genügend Zeit
  - Und wenn die Service-Gesundheit nicht optimal ist, hat man andere Probleme

Was liefert das “normale” Monitoring?

- Dinge, die wir nicht extra prüfen müssen:
  - CPU, RAM, Swap
  - Virtualsierung *
  - Disk-Füllgrad und –Warteschlangenlängen *
  - Status der Datenbanken *
  - Backup-Status
  - Länge der aktiven Queues *
  - Status der Webdienste (inkl. SMTP Receive, IMAP + POP3)
  - Ablauf der Zertifikate
  - Quota-Ausschöpfung
  - ???

Was müssen wir prüfen

Wo können sich Fehler einschleichen, ohne dass es auffällt?

- Die Basics
- Konfiguration
- Managed Availability-Informationen
- Store
- Transport
- Access

Die Basics

Auch die Schichten darunter nicht vergessen!

- Mal die “klassischen” Event Logs lessen
- Was machen die Storage Volumes?
- Bei SAN: Sind alle Pfade noch da?
- Stimmt die Zeit und kommt sie aus der richtigen Quelle?
- Updates und Patches?
- Gerätetreiber??

Konfiguration

- Stimmen die Netzwerk-Einstellungen noch? (z.B. DNS)
- Swap File?
- Mount Points?
- Passt die AD Site-Zuordnung?
- Gibt es überschüssige lokale Admins? ;-)
- Sind alle Third Party-Komponenten auf Stand und operabel?
- Stimmt am HLB, Reverse Proxy, Mail Gateway noch alles?
- Passen die IP-Scopes an Receive Connectors noch?
- Anpassungen an web.config-Dateien? → wie dokumentieren?
- Registry (TCP Keepalive etc .)
- ???

Store

- Database Schema-Version:

```
Get-MailboxDatabase | Get-MailboxDatabaseCopyStatus |

Where-Object {$_.RequestedDatabaseSchemaVersion -ne
$_.MaximumSupportedDatabaseSchemaVersion} |

ft Name, RequestedDatabaseSchemaVersion,
MaximumSupportedDatabaseSchemaVersion –AutoSize
```

- Falls Abweichungen → Update-DatabaseSchema

Transport

- Monitoring liefert bei Queues oft nur die aktiven Nachrichten
  - Checken, ob die Shadow Redundancy hier einbezogen wird!
- Deferred Messages + Retries können ein Hinweis auf Fehler sein
- Check:

```
$queues = Get-Queue -Server $server -Filter {MessageCount -gt 0} |
Where-Object {$_.DeliveryType -ne "ShadowRedundancy"}

$queues | ft Identity, DeliveryType, Status,
MessageCount,DeferredMessageCount -AutoSize

$msgs = @()

foreach ($queue in $queues) {
     $msgs += Get-Message -Queue $queue |
     Select Status, RetryCount, FromAddress, SourceIP, LastError
}

$msgs | Out-GridView
```

Transport

- Größe und Lage der Transport-Datenbank

```
Notepad %ExchangeInstallPath%Bin\EdgeTransport.exe.config
```

  - Das ist eigentlich etwas fürs Monitoring, da nicht die aktuelle Größe wirklich spannend ist, sondern der Trend
  - Auch interessant: Größenunterschiede innerhalb einer DAG ;-)
- An RCs gebundene TLS-Zertifikate, falls mehrere vorhanden

```
openssl s_client -connect mail.example.com:25 -starttls smtp
openssl s_client -connect mail.example.com:465
```

Access

- IIS Logs, falls noch nicht im Monitoring/Maintenance integriert
- Kerberos-ASA-Status innerhalb eines LB-Verbundes
- Konsistenz der OWA-Einstellungen
- Fehler / Erfolg-Verhältnis (falls noch nicht im Monitoring)
  - Empfehlung: LogParser Studio

- ActiveSync-Endgeräte, die abgelaufen sind oder sonst weg müssen (falls noch nicht im Monitoring)

Managed Availability

- Component States
- Health Sets
- Monitors
- Probes
- …WTF?

What next?

- Toolkit vorbereiten
  - Blöderweise ist hier die Testumgebung oft nur von begrenztem Nutzen
- Beispiel-Health Check durchführen, wenn wirklich alles gut ist
  - …und auf Überraschungen vorbereitet sein
- Ergebnisse des vorherigen Health Checks immer parat haben
  - …falls ein Artefakt, das man entschärft zu haben meint, wieder kommen sollte

Vielen Dank!