
Internetzugang überwachen mit Bussines Intelligence (BI)

Autor:
Stefan KANIA

Ort:
St. Michaelisdomm

18. November 2020

Inhalt

| | | |
|----------|---|----------|
| 1 | Einleitung | 2 |
| 2 | Verwalten des Ordners | 2 |
| 2.1 | Anlegen des Ordners | 2 |
| 2.2 | Deaktivierung der Hostbenachrichtigung | 2 |
| 2.3 | Deaktivierender Servicebenachrichtigungen | 3 |
| 2.4 | Dynmische Namensauflösung der Hosts | 3 |
| 3 | Anlegen der Hosts | 4 |
| 4 | Verbinden der Hosts in Bussines Inteligence | 4 |
| 5 | Dummyhost anlegen | 6 |
| 5.1 | Host und Aggregation verbinden | 7 |
| 5.2 | Regel zur Überwachung | 8 |
| | Stichwortverzeichnis | 9 |

1 Einleitung

Der Zugang zum Internet ist in den meisten Firmen ein wichtiger Dienst. Beim Ausfall der Internetverbindung wollen Sie auf jeden Fall im Monitoring eine Meldung erhalten.

In dieser Anleitung sehen Sie eine etwas komplexere Lösung für die Überwachung der Internetverbindung in Ihrem Unternehmen. Dieses Beispiel zeigt Ihnen wie Sie das Modul *Bussines Intelligence* für eine komplexere Überwachung nutzen können. Für die Überwachung des Internetzugangs werden verschiedene Hosts im Internet genutzt die über ein `ping` erreichbar sind.

2 Verwalten des Ordners

Um mehrere Hosts im Internet für die Prüfung des Internetzugangs zu verwenden, ist es am einfachsten eine Ordner anzulegen bei dem Sie bestimmte Voreinstellungen schon eintragen, die dann auf alle Hosts innerhalb des Ordners vererbt werden.

2.1 Anlegen des Ordners

Legen Sie sich einen neuen Ordner mit dem Namen `Internet` an. In den Eigenschaften des Ordners deaktivieren Sie den Agent, `snmp` und `piggyback`. Die Hosts im Internet sollen lediglich über `Ping` auf Erreichbarkeit geprüft werden. Wichtig sind die Einstellung im Abschnitt `DATA SOURCES`. Die Einstellungen dort sehen Sie in der Abbildung 2.1.

| ▼ DATA SOURCES | |
|------------------------|--|
| Check_MK Agent | <input checked="" type="checkbox"/> Normal Checkmk agent, or special agent if configured ▾ |
| SNMP | <input checked="" type="checkbox"/> No SNMP ▾ |
| SNMP credentials | <input type="checkbox"/> none (Default value) |
| Piggyback | <input checked="" type="checkbox"/> Never use piggyback data ▾ |

Abbildung 2.1: Einrichten des Ordners für die Internet-Hosts

2.2 Deaktivierung der Hostbenachrichtigung

Fällt einer der Hosts im Internet aus, wollen Sie darüber nicht alarmiert werden, solange noch mindestens einer der anderen Hosts erreichbar ist. Erst wenn keiner der von Ihnen ausgewählten Host mehr erreichbar ist, wollen Sie einen Alarm denn nur dann ist der Internetzugang sehr wahrscheinlich ausgefallen.

Für die Deaktivierung der Alarmierung klicken Sie auf `WATO, HOST & SERVICE PARAMETERS` suchen Sie nach `notifications`. Unter der Überschrift *Monitoring Configuration* finden Sie die Regel *Enable/disable notifications for hosts*. Klicken Sie auf die Regel. Wählen Sie den Ordner `Internet` aus und klicken Sie auf `CREATE RULE IN FOLDER:`. Erstellen Sie eine sinnvolle Beschreibung so das Sie auch später noch wissen, warum Sie diese Regel eingerichtet haben. Das gilt nicht nur für diese Regel, sondern für alle Regeln die Sie erstellen. Bei dieser Regel sehen Sie ein Beispiel für eine Beschreibung in der Abbildung 2.2.

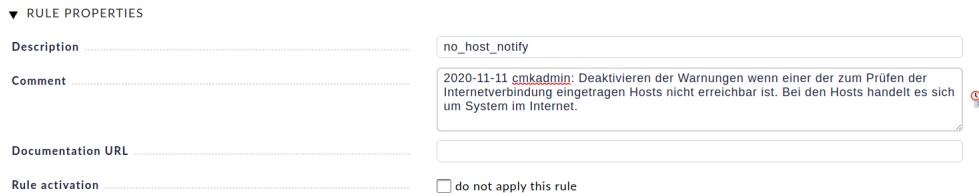


Abbildung 2.2: Kommentar zur Regel

Im Abschnitt `ENABLE/DISABLE NOTIFICATIONS FOR HOSTS` deaktivieren Sie die Benachrichtigungen wie in Abbildung 2.3.

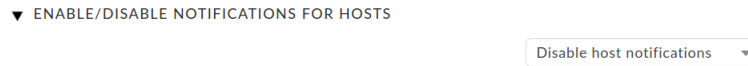


Abbildung 2.3: Deaktivierung der Benachrichtigung für Hosts

Damit haben Sie alle notwendigen Einstellungen vorgenommen und können die Regel speichern.

2.3 Deaktivierender Servicebenachrichtigungen

Für die Hosts die Sie für die Überwachung des Internetzugangs verwenden, wollen und können Sie auch keinen Service Überwachen, denn es geht Ihnen dabei nur um die reine Erreichbarkeit. Aus diesem Grund können Sie auch alle Servicebenachrichtigungen deaktivieren. Suchen Sie unter `WATO, HOST & SERVICE PARAMETERS` erneut nach `notification`. Im Abschnitt *Monitoring Configuration* finden Sie auch noch die Regel `ENABLE/DISABLE NOTIFICATIONS FOR SERVICES`. Klicken Sie auf die Regel und wählen auch hier wieder den Ordner `internet` aus. Nach der Auswahl des Ordners deaktivieren Sie die Benachrichtigung für Services wie schon zuvor die Hostbenachrichtigungen. In Abbildung 2.4 sehen Sie die Einstellung.

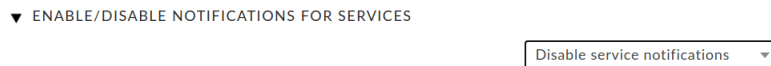


Abbildung 2.4: Deaktivierung der Benachrichtigung für Services

2.4 Dynmische Namensauflösung der Hosts


Um eine Problematik müssen Sie sich jetzt noch kümmern, `checkmk` verwaltet einen eigenen DNS-Cache um die Namen der Hosts nicht bei jeder Abfrage auflösen zu müssen, und das das Monitoring auch noch funktioniert wenn der DNS-Dienst ausgefallen ist. Bei den externen Hosts die Sie für die Überprüfung der Internetverbindung nutzen wollen, können Sie aber nicht sicherstellen, dass sich die IP-Adresse nicht irgendwann ändert. Aus diesem Grund muss der Name der Hosts im Ordner `Internet` bei jeder Prüfung neu aufgelöst werden. Dazu benötigen Sie eine weitere Regel in der für die Hosts in dem Ordner die Namensauflösung bei jeder Anfrage durchführt wird.

Um die Regel zu erstellen klicken Sie auf `WATO, HOST & SERVICE PARAMETERS`. Suchen Sie nach dem Muster *dynamic*. Sie werden eine Regel mit dem Namen `HOSTS WITH DYNAMIC DNS LOOKUP DURING MONITORING` finden. Klicken Sie auf die Regel. Wählen Sie dort den Ordner `Internet` aus und klicken Sie auf `CREATE RULE IN FOLDER:`. Erstellen Sie eine Beschreibung mit dem Grund für die Aktivierung dieser Regel damit Sie auch hier später wissen warum die Hosts immer aufgelöst werden sollen.

Im Abschnitt `CONDITIONS` wählen Sie den Ordner `Internet` und speichern sie die Regel.

3 Anlegen der Hosts

Jetzt ist es soweit, im nächsten Schritt legen Sie die Hosts an, über die Sie die Internetverbindung testen wollen. Zur Überprüfung des Internet suchen Sie sich dafür mindestens drei Server im Internet die Sie mit einem Ping testen können, wie zum Beispiel *www.google.de*. Testen Sie vorher, ob die Hosts auch auf ein Ping reagieren. Beim Anlegen der Hosts benötigen Sie lediglich den Namen, alle anderen wichtigen Einstellungen haben Sie bereits auf dem Ordner vergeben. Da Alle Hosts in dem Ordner diese Eigenschaften erben, brauchen Sie bei den einzelnen Hosts nichts zusätzlich konfigurieren.

Nachdem Sie die Änderungen angewendet haben, sehen Sie die Hosts jetzt im *Tactical overview*. Lassen Sie sich über die Tactical overview alle eingerichteten Hosts anzeigen. Sie sehen dort auch die Host die Sie für die Überwachung des Internetzugangs eingerichtet haben. Bei den Hosts fällt das Icon  auf, das Ihnen zeigt, dass die Benachrichtigung deaktiviert wurde. Abbildung 3.1 zeigt einen der Hosts.




| Local site kania | | | | | | | | |
|------------------|---------------|---|----|----|----|----|----|---|
| STATE | HOST | ICONS | OK | WA | UN | CR | PD | |
| UP | www.amazon.de |    | 1 | 0 | 0 | 0 | 0 | 0 |

Abbildung 3.1: Ausschnitt aus dem Tactical Overview

Tipp!

Wenn Sie schon viele Hosts im checkmk eingetragen haben, können Sie im Eingabefenster zu QUICK-SEARCH das Muster *h:www* eingeben, dann werden Ihnen nur die Hostnamen angezeigt, die mit *www* beginnen.

4 Verbinden der Hosts in Bussines Intelligence

Jetzt verbinden Sie die Hosts, die Sie gerade angelegt haben, noch miteinander. Der Grund ist der, dass Sie durch die Verbindung der Hosts nur eine Benachrichtigung erhalten wenn alle Hosts nicht erreichbar sind. Das geht nicht mit einer einfachen Regel, hierfür müssen Sie ein spezielles Modul von checkmk verwenden, das Modul *Bussines Intelligence(BI)*.

Klicken Sie auf dafür auf WATO, BUSSINES INTELIGENCE, sie gelangen dann in eine Liste von *BI Configuration Packs*. Zu diesem Zeitpunkt sehne Sie dort nur einen Eintrag mit dem Namen *default*. Um eine neues *Configuration Pack* zu erzeugen, klicken Sie auf NEW BI PACK, daraufhin gelangen Sie in die Maske zum erstellen des neuen Configuration Packs. Vergeben Sie dort eine eindeutige ID und einen Titel so wie in Abbildung 4.1

▼ BI PACK PROPERTIES


BI pack ID test-internet

Title test-internet

Permitted Contact Groups Add Contact Group

Public Allow all users to refer to rules contained in this pack

Abbildung 4.1: Erstellen eines neuen configuration pack

Speichern Sie das neue Configuration Pack, Sie kommen dann zurück in die Übersicht. Um eine neue Regel zu erstellen klicken Sie auf das Icon . Daraufhin gelangen Sie in die leere Übersicht der Regeln. Klicken Sie auf NEW RULE. In dem dann erscheinenden Fenster erstellen Sie die Regel. Im ersten Bereich RULE PROPERTIES füllen Sie die Felder wie in der Abbildung 4.2 aus.

▼ RULE PROPERTIES

Rule ID test-internet

Rule Title test-internet

Abbildung 4.2: Eigenschaften der Regel

Im Abschnitt **CHILDE NODE GENERATION** tragen Sie die von Ihnen eingerichteten Hosts für die Überwachung des Internetzugangs ein. Alle Einträge für die hier ausgewählten Hosts finden Sie in der Abbildung 4.3

▼ CHILD NODE GENERATION

Nodes that are aggregated by this rule

- +

State of a host

🗑️

Host: www.google.de

- +

State of a host

🗑️

Host: www.amazon.de

- +

State of a host

🗑️

Host: www.ebay.de

Add child node generator

Abbildung 4.3: Einträge für die Child Nodes

Im letzten Abschnitt **AGGREGTION FUNCTION** legen Sie jetzt fest unter welcher Bedingung die Kombination der externen Hosts auf *CRIT* wechseln soll. Da selbst bei einem erreichbaren Host der Internetzugang noch vorhanden ist, muss der Zustand *CRIT* erst dann gemeldet werden wenn alle drei Hosts nicht mehr erreichbar sind. Sehen Sie hierzu die Abbildung 4.4.

▼ AGGREGATION FUNCTION

Aggregation Function Count the number of nodes in state OK

Required number of OK-nodes for a total state of OK: Explicit number ▼

Number of OK-nodes

Required number of OK-nodes for a total state of WARN: Explicit number ▼

Number of OK-nodes

Abbildung 4.4: Festlegung des Zustands CRIT

Speichern Sie die Einstellungen. im nächsten Schritt erstellen Sie aus der Regel noch eine Aggregation. Klicken Sie dazu auf **NEW AGGREGATIONS**. In dem folgenden Fenster verbinden Sie jetzt das *Configuration Pack* mit der Regel. Die Abbildung 4.5 zeigt Ihnen die Einstellungen.

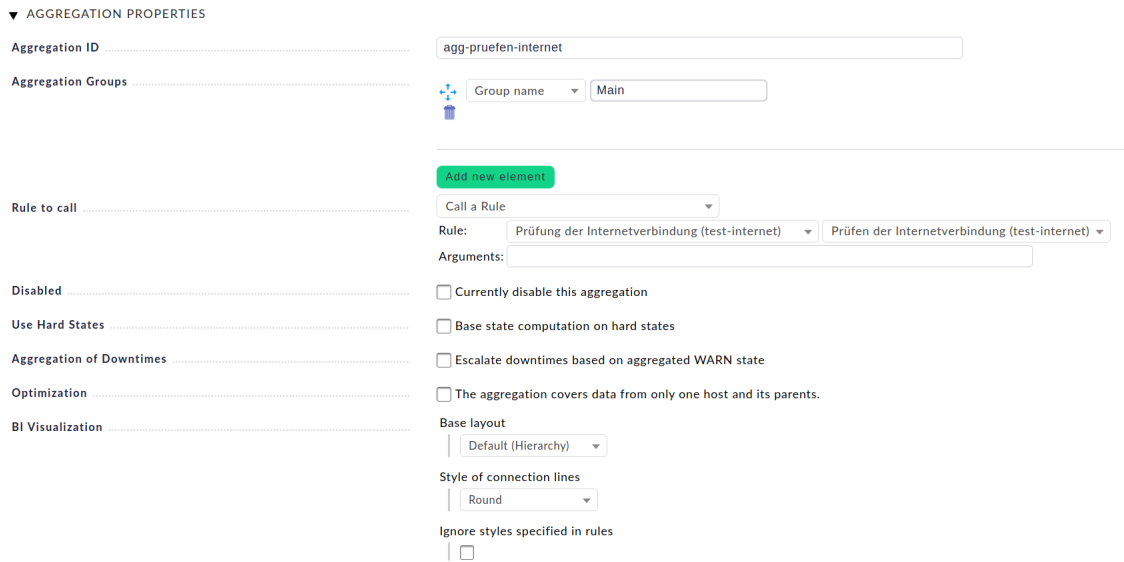


Abbildung 4.5: Verknüpfung von Regel und Configuration pack

Damit haben Sie den Status der externen Hosts zusammengefasst. Vergessen Sie auch hier nicht die Änderungen anzuwenden. Klicken Sie anschließend in der Seitenleiste im Plugin VIEWS auf BUSSINES INTELIGENCE, ALL AGGREGATIONS. Dort sehen Sie jetzt alle Aggregationen.

Hinweis!

Wenn Sie das erste Mal auf die Aggregations klicken sehen Sie die Übersicht und für die Prüfung des Internets wird nur ein *OK* für alle Hosts angezeigt. Um die Baumansicht zu sehen klicken Sie auf den Pfeil neben dem *OK* für den Tree. Dann klappt der Baum auf und Sie sehen alle Hosts

In Abbildung 4.6 sehne Sie jetzt alle drei Hosts, den Status jedes einzelnen Hosts und den gesamt Status der Internetverbindung.

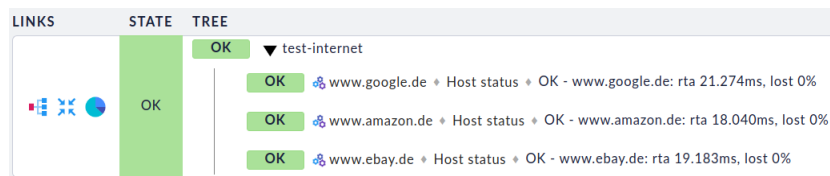


Abbildung 4.6: Übersicht über die Aggration

Können alle Hosts über ein Ping erreicht werden, haben alle Hosts den Status (OK) auch der Gesamtstatus ist (OK). Das Icon hinter dem Status *OK* aller drei Hosts zeigt an, dass regelmäßig geprüft wird ob die Hosts erreichbar sind. Klicken Sie auf das Icon können Sie den Status der Hosts ändern. Ändern Sie den Status von zwei Hosts auf (CRIT), in dem Sie zwei mal auf das Symbol klicken. Anschließend übernehmen Sie den Status noch über das Icon links neben dem Gesamtstatus für die Aggragation. Sie werden feststellen, solange noch ein Host erreichbar ist, bleibt der Status auf *OK*. Erst wenn keiner der Hosts auf Anfragen antwortet, wechselt der Status Ihrer Internetverbindung auf *CRIT*. Nachdem Sie auch den dritten Host auf *Crit* gestellt haben, ändert sich der Gesamtstatus. Schalten Sie alle Hosts wieder auf automatische Prüfung (die drei Zahnräder) und übernehmen Sie den Status.

5 Dummyhost anlegen

Bis zu diesem Zeitpunkt würde zwar eine Anzeige in checkmk erscheine wenn die Internetverbindung nicht mehr besteht, aber eine Meldung würde noch nicht generiert. Denn BI dient nur zur

Darstellung von Zusammenhängen. Jetzt ist es an der Zeit, dass Sie aus der Aggregation eine Regel erzeugen. Diese Regel verbinden Sie mit einem Host, damit dieser Host dann den Fehler melden kann. Sie können dabei jeden beliebigen Host verwenden, auch ein Switch wäre möglich. Nur welchen Sinn macht es, wenn der Internetzugang ausfällt und ein Switch auf den Status (CRIT) wechselt? Genau! Keinen. Aus diesem Grund können Sie für die Überprüfung der Aggregation einen Dummyhost anlegen. Der Dummyhost muss nicht existent sein und braucht somit auch keine IP-Adresse, er muss lediglich vorhanden sein. Einen solchen Dummyhost legen Sie am besten direkt im Main directory an, denn diesen Host können Sie später auch noch für weitere Aggregations verwenden. In der Abbildung 5.1 sehen Sie die Eigenschaften des Dummyhosts.

▼ BASIC SETTINGS

Hostname my-dummy

Alias empty (Default value)

Monitored on site kania - Local site kania (Default value)

Permissions empty (Default value)

Parents empty (Default value)

▼ NETWORK ADDRESS

IP Address Family No IP

▼ DATA SOURCES

Check_MK Agent No agent

SNMP No SNMP (Default value)

Piggyback Never use piggyback data

Abbildung 5.1: Eigenschaften des Dummy-Hosts

Wie Sie sehen, hat der Host weder einen Agent, noch wird er über SNMP angesprochen, auch hat der Host keine IP-Adresse.

5.1 Host und Aggregation verbinden

Über diesen Host können Sie jetzt den Zustand der BI-Aggregation prüfen. Klicken Sie dafür wieder auf WATO, HOST & SERVICE PARAMETERS und klicken dann auf der rechten Seite auf ACTIVE CHECKS. Sie gelangen dann in die Übersicht aller aktiven Checks. Klicken Sie dort auf den Check CHECK STATE OF BI AGGREGATION. Dort erstellen Sie eine neue Regel im Main directory.

Im Abschnitt CHECK STATE OF BI AGGREGATION tragen Sie im Feld *Base URL (OMD Site)* die komplette URL Ihrer Site ein.

Wichtig!

Wenn Ihr checkmk-Host nur über HTTPS erreichbar ist, müssen Sie dafür sorgen, dass das Zertifikat auf Gültigkeit überprüft werden kann.

Im Feld *Aggregation Name* wird der Name der Aggregation eingetragen, den Sie im BI-Modul vergeben haben. Hier im Beispiel war das der Name *test-internet*.

Bei den *Login credentials* steht automatisch der Benutzer *automation*. Hierbei handelt es sich um einen Benutzer, der beim Anlegen der Site automatisch erzeugt wird. Im Abschnitt CONDITIONS tragen Sie jetzt noch den Namen Ihres Dummyhosts bei *Explicit hosts* ein, hier im Beispiel ist das der Name *my-dummy*.

Wichtig!

Denken Sie daran, dass Sie hier auf die genaue Schreibweise achten müssen.

In der Abbildung 5.2 sehen Sie alle vergeben Parameter zu der Regel.

New rule: Check State of BI Aggregation

Abort
Predef. conditions

Connect to the local or a remote monitoring host, which uses Check_MK BI to aggregate several states to a single BI aggregation, which you want to show up as a single service.

▼ RULE PROPERTIES

Description aggr_test_init

Comment 2020-11-12 [cmkadmin](#): Diese Regel verbindet sich mit der Webseite der OMD-Site um die Aggregation der Internetverbindung zu prüfen. Geprüft wird hier gegen den Dummyhost "my-dummy"

Documentation URL

Rule activation do not apply this rule

▼ CHECK STATE OF BI AGGREGATION

Base URL (OMD Site)

Aggregation Name

Login credentials

Optional parameters

- Authentication Mode
- Seconds before connection times out
- State, if BI aggregate is in scheduled downtime
- State, if BI aggregate is acknowledged
- Track downtimes

▼ CONDITIONS

Condition type

Folder

Host tags Add tag condition

Host labels Add label condition

Explicit hosts

Negate: make rule apply for all but the above hosts

Abbildung 5.2: Parameter der Aggregation

5.2 Regel zur Überwachung

Damit haben Sie jetzt Ihre Aggregation mit einem Host verbunden. Jetzt fehlt noch die Überwachung des Hosts. Auch dazu benötigen Sie ein Regel. Klicken Sie dazu wieder auf WATO, HOST & SERVICE PARAMETERS und suchen dort nach *Host check*. In dem Suchergebnis finden Sie die Regel HOST CHECK COMMAND, klicken Sie auf die Regel um eine neue Regel im Main directory zu erzeugen.

Im Abschnitt HOST CHECK COMMAND wählen Sie USE THE STATUS OF THE SERVICE... aus. Als Service tragen Sie hier den Namen der Aggregation *test-internet* ein. Tragen Sie jetzt noch den Hostname Ihres Dummyhosts bei *Explicit hosts* ein. Dann können Sie die Regel speichern und Anwenden. In Abbildung 5.3 sehen Sie die komplette Regel.

▼ RULE PROPERTIES

Description internet-dummy

Comment

Documentation URL

Rule activation do not apply this rule

▼ HOST CHECK COMMAND

Use the status of the service... test-internet

▼ CONDITIONS

Condition type Explicit conditions

Folder Main directory

Host tags Add tag condi

Host labels Add label condition

Explicit hosts my-dummy

Negate: make rule apply for all but the above hosts

Abbildung 5.3: Regel für den Dummystatus

Immer wenn in Zukunft die Internetverbindung ausfällt wechselt der Status und Sie können einen Alarm generieren. Zum Testen, ob der Dummyhost auf auf *CRIT* wechselt wenn die Verbindung ausfällt, können Sie nicht einfach in der Aggregation den Status ändern. Sie könnten aber den Resolver des checkmk-Hosts auf einen ungültigen Wert setzen, dann könnten die Namen für dne Test nicht mehr aufgelöst werden und somit wären die Server im Internet nicht mehr erreichbar und sowohl die Aggregation als auch der Dummyhost würden auf den Status *CRIT* wechseln. Ihr Monitoring würde auch weiter funktionieren, da checkmk einen eigenen DNS-Cache pflegt und für Ihre eigenen Host keine Namensauflösung bei jeder Prüfung notwendig ist.

Die Einrichtung der Überprüfung der Internetverbindung ist eine komplexe Einrichtung, aber eine wichtig Prüfung. Denn wenn die Internetverbindung nicht mehr besteht, sind viele Dienste nicht mehr funktionsfähig.

Index

B

Bussines Inteligence 2

D

DNS-Cache 3

N

Namensauflösung 3

notification 2 f.

P

Ping 2, 4