Lab 10: Monitoring mit Nagios

Der Webserver ist ein öffentlicher Dienst und kann somit i.d.R. von anderen Rechnern direkt überprüft werden. Bei der direkten Überprüfung ist kein Agent wie NRPE notwendig (Siehe „NRPE Konfiguration übernehmen“).

Jedoch kann es Szenarien geben, wo diese Überprüfung indirekt (über einen Agent) erfolgen müsste. Was wären solche Szenarien? Denken Sie dabei auch an Sicherheit.

Intranet, interne Webseiten die nicht öffentlich zugänglich sein sollten.

Der CPU Load wird steigen und Nagios sollte beim nächsten Check einen CIRITICAL Zustand anzeigen.

Ihnen wird vermutlich auffallen, dass mehrere Zonen eine hohe CPU Auslastung aufweisen und nicht nur die Zone des Fileservers. Wieso? Stellen Sie sich dazu das Zonenkonzept vor.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
apache	Apache Webserver	CRITICAL	10-11-2013 11:12:32	0d 0h 47m 29s	2/2	Connection refused
fileserver	Current Load	CRITICAL	10-11-2013 11:12:27	0d 0h 1m 34s	2/2	CRITICAL - load average: 35.43, 18.08, 8.48
	Total Processes	OK	10-11-2013 11:12:14	0d 0h 54m 47s	1/2	PROCS OK: 123 processes
localhost	Current Load	CRITICAL	10-11-2013 11:12:29	0d 0h 0m 32s	1/4	CRITICAL - load average: 35.46, 18.14, 8.51
	Current Users	OK	10-11-2013 11:12:07	514d 1h 24m 14s	1/4	USERS OK - 1 users currently logged in
	HTTP	OK	10-11-2013 11:11:05	514d 1h 23m 37s	1/4	HTTP OK HTTP/1.1 200 OK - 340 bytes in 0.002 seconds
	PING	OK	10-11-2013 11:09:45	514d 1h 22m 59s	1/4	PING OK - Packet loss = 0%, RTA = 0.06 ms
	Root Partition	OK	10-11-2013 11:12:20	514d 1h 22m 22s	1/4	DISK OK - free space: / 9191 MB (95% inode=99%):
	SSH	OK	10-11-2013 11:10:58	3d 1h 12m 3s	1/4	SSH OK - Sun_SSH_1.1.4 (protocol 2.0)
	Swap Usage	OK	10-11-2013 11:08:35	514d 1h 21m 7s	1/4	SWAP OK - 100% free (639 MB out of 639 MB)
	Total Processes	OK	10-11-2013 11:11:13	514d 1h 20m 29s	1/4	PROCS OK: 45 processes with STATE = RSZDT

Linux Servers (linux-servers)

Host	Status	Services	Actions
localhost	UP	7 OK 1 CRITICAL	

Unix Services (unix-services)

Host	Status	Services	Actions
apache	UP	1 CRITICAL	
fileserver	UP	1 OK 1 CRITICAL	
mysql	UP	No matching services	

Der Fileserver wird von „localhost“ aus überwacht. Entsprechend wir der Status nach „oben“ propagiert.

Wenig Plattenspeicher

Definieren Sie in der NRPE Konfiguration ein Kommando, welches den freien Festplattenspeicher (vom Root Verzeichnis /) überprüft. Bei weniger als 20% freier Speicherplatz soll eine WARNING und bei weniger als 10% ein CRITICAL zurückgegeben werden.

```
# 'check_local_disk' command definition
define command{
        command_name    check_local_disk
        command_line    $USER1$/check_disk -w $ARG1$ -c $ARG2$ -p $ARG3$
        }
```

Definieren Sie in der Nagios Konfiguration den entsprechenden Service:

```
define service{
        use                             remote-service          ; Name of service template to use
        host_name                       fileserver
        service_description             HDD.root
        check_command                   check_local_disk!20%!10%!/
}
```

fileserver	Current Load	OK	10-18-2013 08:43:17	6d 20h 46m 50s	1/2	OK - load average: 0.01, 0.01, 0.01
	HDD.root	OK	10-18-2013 08:43:17	6d 20h 45m 36s	1/2	DISK OK - free space: / 7805 MB (94% inode=99%):
	Total Processes	OK	10-18-2013 08:43:17	6d 22h 25m 28s	1/2	PROCS OK: 35 processes

Nagios sollte nun einen CRITICAL Zustand ausgeben, da zu wenig freier Speicherplatz vorhanden ist.

Ihnen wird eventuell auffallen, dass mehrere Zonen eine hohe Festplatten Auslastung aufweisen und nicht nur die Zone des Fileservers. Wieso? Stellen Sie sich dazu das Zonenkonzept vor.

fileserver	Current Load	OK	10-18-2013 08:55:17	6d 20h 58m 49s	1/2	OK - load average: 0.02, 0.04, 0.03
	HDD.root	CRITICAL	10-18-2013 08:55:17	0d 0h 0m 24s	1/2	DISK CRITICAL - free space: / 50 MB (10% inode=80%):
	Total Processes	OK	10-18-2013 08:55:18	6d 22h 37m 27s	1/2	PROCS OK: 38 processes

Da alle „Server" auf einem Node laufen, wird das Filesystem für alle Server beeinflusst.

Zu viele Prozesse

Es werden eine grosse Anzahl Prozesse auf der Zone erstellt. Überschreitet die Prozessanzahl 200, so soll eine WARNING ausgegeben werden. Über 250 Prozesse soll ein CRITICAL ausgegeben werden.

Tragen Sie in der NRPE Konfiguration das entsprechende Kommando ein:

```
command[check_total_procs]=/opt/csw/libexec/nagios-plugins/check_procs -w 200 -c 250
```

Definieren Sie in der Nagios Konfiguration den Service:

```
define service{
        use remote-service
        host_name fileserver
        service_description Total Processes
        check_command check_nrpe!check_total_procs
}
```

Es werden ca. 200 Zombieprozesse im System herumgeistern. Nagios wird diesem Umstand mit einem CRITICAL Zustand signalisieren. Was ist genau ein Zombieprozess?

fileserver	Current Load	OK	10-18-2013 09:14:17	6d 21h 17m 57s	1/2	OK - load average: 0.14, 0.07, 0.04
	HDD.root	OK	10-18-2013 09:14:17	0d 0h 17m 32s	1/2	DISK OK - free space: / 9181 MB (95% inode=99%):
	Total Processes	CRITICAL	10-18-2013 09:14:18	0d 0h 1m 31s	2/2	PROCS CRITICAL: 288 processes

Ein Zombie ist vor allem in Unix-ähnlichen Betriebssystemen (wie beispielsweise Linux) ein Prozess, der beendet ist, aber trotzdem noch in der Prozesstabelle auftaucht und geringfügig Systemressourcen belegt.

Wie können Sie Zombieprozesse erkennen? Schauen Sie in die Manpages vom Befehl ps

```
Mit dem Befehl: ps -el
     -e                 Lists information  about  every  process
                        now running.
     -l                 Generates a long listing. (See below.)
```

Welche Auswirkungen hat ein Zombieprozess auf ein System?

Ein Zombie richtet selbst keinen Schaden an, kann aber auf einen Fehler hinweisen. Die Ressourcen werden unnötig belastet (z.B. RAM).

MySQL

Konfigurieren Sie den NRPE Agent so, dass eine WARNING bei 4080 Einträgen und ein CRITICAL bei 4081 Einträgen ausgegeben werden.

```
command[check_mysql_query]=/opt/csw/libexec/nagios-plugins/check_mysql_query -q "SELECT COUNT(*) FROM City"
-d world -w 4079 -c 4080 -u root
```

Definieren Sie in der Nagios Konfiguration den Service:

```
define service{
        use remote-service
        host_name mysql
        service_description MySQL RowCount
        check_command check_nrpe!check_mysql_query
}
```

RowCount	OK	10-18-2013 09:46:54	0d 0h 2m 28s	1/2	QUERY OK: 'SELECT COUNT(*) FROM City' returned 4079.

Gehen Sie in den MySQL Kommandomodus und wählen die world Datenbank aus. Fügen Sie anschliessend einen neuen Eintrag in die City Tabelle.

```
mysql -u root
mysql> USE world;
INSERT INTO City (Name, CountryCode, District, Population) VALUES ('Horw', 'CH', 'Lucerne', 13000);
```

Das Web Interface von Nagios soll nun eine WARNING ausgeben.

RowCount	WARNING	10-18-2013 10:04:54	0d 0h 14m 45s	2/2	QUERY WARNING: 'SELECT COUNT(*) FROM City' returned 4080

Fügen Sie nun einen weiteren Eintrag hinzu.

```
INSERT INTO City (Name, CountryCode, District, Population) VALUES ('Horw', 'CH', 'Lucerne', 13000);
```

Nun sollte Nagios einen CRITICAL ausgeben.

RowCount	CRITICAL	10-18-2013 10:07:54	0d 0h 1m 22s	2/2	QUERY CRITICAL: 'SELECT COUNT(*) FROM City' returned 4081.

Sie können anschliessend die erstellten Einträge wieder löschen

```
delete from city where name = 'Horw'
```

Überprüfung des Datenbankdienstes

Hier wollen wir überprüfen ob der Datenbankdienst erreichbar und funktionstüchtig ist.

Definieren sie das entsprechende Kommando in der Konfiguration des NRPE Agents:

```
command[check_mysql]=/opt/csw/libexec/nagios-plugins/check_mysql -u root -d world
```

In der Nagios Konfiguration müssen Sie den Service definieren:

```
define service{
        use remote-service
        host_name mysql
        service_description MySQL Status
        check_command check_nrpe!check_mysql
}
```

mysql	MySQL Status	OK	10-18-2013 10:08:45	0d 0h 24m 1s	1/2	Uptime: 863570 Threads: 2 Questions: 102 Slow queries: 0 Opens: 15 Flush tables: 1 Open tables: 9 Queries per second avg: 0.000

Schalten Sie den Datenbankdienst offline. Welcher Befehl ist dazu notwendig?

```
Mit  svcs -a | grep mysql können die vorhandenen Services angezeigt werden.
svcadm disable svc:/network/cswmysql5:default
```

Nagios wird den nicht zu erreichenden Datenbankdienst mittels eines CRITICAL Zustands signalisieren.

mysql	MySQL Status	CRITICAL	10-18-2013 10:15:45	0d 0h 0m 18s	1/2	Can't connect to local MySQL server through socket '/tmp/mysql.sock' (2)
	RowCount	CRITICAL	10-18-2013 10:15:54	0d 0h 0m 9s	1/2	QUERY CRITICAL: Can't connect to local MySQL server through socket '/tmp/mysql.sock' (2)