Netzwerk Vorraussetzungen (Firewall)

Beschreibung:

Der Server und die Agents kommunizieren über mehrere Ports. Diese müssen eingehend erreichbar sein

Firewall Ports

Überwachung von Hosts (Agent, SNMP)

Die folgenden Ports auf überwachten Hosts müssen vom Checkmk-Server aus erreichbar sein.

Port	Protokoll	Bezeichnung	Ergänzende Informationen
161	UDP	Simple Network Management Protocol (SNMP)	Via SNMP überwachte Hosts erhalten über diesen Port die Anforderung `GET-REQUEST`.
6556	TCP	Agent	Via Checkmk-Agent überwachte Hosts werden über diesen Port abgefragt. Die Kommunikation erfolgt TLS verschlüsselt oder im Klartext (wie beim Linux-Agenten im Legacy-Modus).

Port	Protokoll	Bezeichnung	Ergänzende Informationen
—	ICMP	Ping	Checkmk überwacht die Erreichbarkeit von Hosts per Ping. Ist dies nicht möglich, muss die Ermittlung des Host-Zustands mit der Regel Host Check Command festgelegt werden.

Aktive Checks greifen direkt auf die Ports der überwachten Dienste zu, die daher auch vom Checkmk-Server aus erreichbar sein müssen. Die Überwachung mit Spezialagenten kann erfordern, andere/weitere Ports zu öffnen. So benötigt der Spezialagent für VMware ESXi (auch NetApp und viele weitere) die Öffnung des Ports 443 auf dem ESXi Server.

Checkmk-Server

Die folgenden Ports auf dem Checkmk-Server müssen für die Hosts im Monitoring erreichbar sein.

Port	Protokoll	Bezeichnung	Ergänzende Informationen
80	TCP	Hypertext Transfer Protocol (HTTP)	Agent Updater (Agentenbäckerei), Discovery des Agent Controller Ports
162	UDP	Simple Network Management Protocol Trap (SNMPTRAP) EC	Empfang von SNMP-Traps über die Event Console *(optional aktivierbar)*
443	TCP	Hypertext Transfer Protocol over SSL/TLS (HTTPS)	Agent Updater (Agentenbäckerei), Discovery des Agent Controller Ports, mit Transportverschlüsselung
514	TCP und UDP	Syslog (EC)	Empfang von Syslog-Nachrichten über die Event Console *(optional aktivierbar)*

Port	Protokoll	Bezeichnung	Ergänzende Informationen
6559	UDP	Echtzeitprüfungen	Empfang von UDP-Paketen für die Echtzeitprüfungen einzelner Dienste (selten verwendet, *optional aktivierbar*)
8000	TCP	Agent Controller TLS-Registrierung	Wenn mehrere Instanzen auf dem Checkmk-Server laufen, sind eventuell weitere Ports (8001, 8002…) nötig.

Die TLS-Registrierung von Agenten nutzt die REST-API auf Port 80/443 zur Discovery des Ports zur Registrierung (meist 8000 TCP). Sind beide nicht erreichbar, kann der Port per Kommandozeilenoption angegeben werden. Falls Port 8000 nicht erreichbar ist, kann auf anderen Hosts im Monitoring eine Registrierung im Auftrag erfolgen.

Verteiltes Monitoring

Remoteinstanz

Die folgenden Ports auf Remote-Instanzen müssen vom als Zentralinstanz arbeitenden Checkmk-Server erreichbar sein.

Port	Protokoll	Bezeichnung	Ergänzende Informationen
80	TCP	HTTPS (Hypertext Transfer Protocol)	Synchronisierung im verteilten Monitoring
443	TCP	Hypertext Transfer Protocol over SSL/TLS (HTTPS)	Synchronisierung im verteilten Monitoring, mit Transportverschlüsselung
6555	TCP	Benachrichtigungs-Spooler (*notification spooler*)	Der Benachrichtigungs-Spooler dient dem zentralen Versand von Benachrichtigungen, hier beim Verbindungsaufbau durch die Zentralinstanz *(optional aktivierbar)*

Port	Protokoll	Bezeichnung	Ergänzende Informationen
6557	TCP	Livestatus	Wenn mehrere Instanzen auf dem Checkmk-Server laufen, sind eventuell weitere Ports nötig *(optional aktivierbar)*
6558	TCP		Statusanschluss der Event Console *(optional aktivierbar)*

Zentralinstanz

Prinzipiell ist verteiltes Monitoring ohne weitere Hilfsmittel wie Tunneling bereits möglich, wenn die Zentralinstanz eine Verbindung zu den Remote-Instanzen herstellen kann. Die Erreichbarkeit der Zentralinstanz durch Remote-Instanzen ist nur für optionale Funktionalitäten (z.B. Agentenbäckerei) erforderlich.

Die folgenden Ports auf dem als Zentralinstanz arbeitenden Checkmk-Server müssen durch die zugeordneten Remote-Instanzen erreichbar sein, um die beschriebene Funktionalität bereitzustellen.

Port	Protokoll	Bezeichnung	Ergänzende Informationen
80	TCP	Hypertext Transfer Protocol (HTTP)	Für Agentenbäckerei und dynamische Host-Konfiguration
443	TCP	Hypertext Transfer Protocol over SSL/TLS (HTTPS)	Für Agentenbäckerei und dynamische Host-Konfiguration, mit Transportverschlüsselung
6555	TCP	Benachrichtigungs-Spooler (*notification spooler*)	Der Benachrichtigungs-Spooler dient dem zentralen Versand von Benachrichtigungen, hier beim Verbindungsaufbau durch eine Remote-Instanz *(optional aktivierbar)*

Checkmk Appliance Cluster

Sie können zwei Checkmk-Appliances ("Knoten") zu einem Cluster zusammenschließen. Dabei werden alle Konfigurationen und Daten zwischen den beiden Geräten abgeglichen.

Die folgenden Ports müssen von beiden Knoten aus ein- und ausgehend freigegeben sein.

Port	Protokoll	Bezeichnung	Ergänzende Informationen
3121	TCP	Pacemaker	Pacemaker Cluster resource manager
4321	UDP	Corosync	Corosync Cluster Engine
4323	UDP	Corosync	Corosync Cluster Engine
7789	TCP	DRBD	Synchronisierung der DRDB (Distributed Replicated Block Device)

Firewall Regeln (wenn eine Firewall Konfiguriert ist, hinzufügen, hier am Beispiel am CheckMK-Server nicht Agent)

FIrewalld

Installation:

```
#Install
yum install firewalld   # für RHEL-basierte Systeme
apt-get install firewalld  # für Debian-basierte Systeme
#Add Systemstart
systemctl start firewalld
systemctl enable firewalld
```

Folgende Regeln hinzufügen, falls die Firewall auch gerade erst installiert wurde habe Ich Port 22 (SSH) einfach mit zugepackt, weil sonst sind wir gleich ausgesperrt. Das Permanent bedeutet das auch nach einem neustart des Servers die Regeln wieder geldaen werden sollen

```
firewall-cmd --zone=public --add-port=8000/tcp --permanent
firewall-cmd --zone=public --add-port=6559/udp --permanent
```

```
firewall-cmd --zone=public --add-port=514/udp --permanent
firewall-cmd --zone=public --add-port=514/tcp --permanent
firewall-cmd --zone=public --add-port=162/udp --permanent
firewall-cmd --zone=public --add-port=80/tcp --permanent
firewall-cmd --zone=public --add-port=443/tcp --permanent
firewall-cmd --zone=public --add-port=22/tcp --permanent
```

Alle Regeln auflisten lassen

```
firewall-cmd --list-all
Output
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: eth0 eth1
  sources:
  services: cockpit dhcpv6-client http https ssh
  ports: 3000/tcp 8005/tcp 5665/tcp 8000/tcp 6559/udp 514/udp 514/tcp 162/udp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Nun ein relaod der Firewall durchführen

```
firewall-cmd --reload
```

ufw Firewall

Install.

```
#Install
apt-get install ufw   # für Debian-basierte Systeme
yum install ufw       # für RHEL-basierte Systeme
#Enable at Systemstart
ufw enable
```

Regeln hinzufügen

```
ufw allow 8000/tcp
ufw allow 6559/udp
ufw allow 514/udp
ufw allow 514/tcp
ufw allow 162/udp
ufw allow 80/tcp
ufw allow 443/tcp
ufw allow 22/tcp
```

Version #6
Erstellt: 9 März 2023 10:06:32 von Admin
Zuletzt aktualisiert: 28 März 2023 10:02:28 von Admin