

Zielstellung und Rahmenbedingungen

Diese Dokumentation beschäftigt sich mit dem Thema „Angriffe auf AMQP-Messagebroker“. Begleitend zur Vorlesung „Betriebliche Informationssysteme“ galt es von uns in einem Praktikum zu identifizieren, welche potenziellen Angriffsvektoren existieren. Eingeschlossen ist hier auch das System „RabbitMQ“ welches das zu untersuchende Protokoll einschließt.

Ziel ist es bestimmt Angriffsvektoren aufzuspüren und zu bewerten. Durch Implementierung von einzelnen Clients auf Basis der RabbitMQ Java-Bibliothek sollen die Angriffe veranschaulicht werden. Mit veränderten Parametern richtet sich die Suche gezielt nach Faktoren die das System negativ beeinflussen und so die Verfügbarkeit stören, fokussiert auf „Denial of Service“. DoS kann dabei auf verschiedene Ressourcen bezogen sein (wie CPU, Arbeitsspeicher, Netzwerkbandbreite etc.).

Um die Begrenzungen ausfindig zu machen, gehört es zu Beginn zu unsere Aufgabe angemessene Werkzeuge zur Beobachtung der Ressourcen zu finden. Nur dann ist es möglich die Angriffe zu bewerten und ihre tiefere Auswirkung zu untersuchen.

Ferner sollen Vorschläge zur Schadensbegrenzung gegeben werden. Dazu gehört die Angabe auf welcher Ebene (Netzwerkebene, Protokollebene etc.) sich die Gefahren beseitigen lassen.

Testumgebung

Als Betriebssystem für die Bereitstellung des RabbitMQ-Servers wurde ein Ubuntu Server 14.04.2 LTS mit Kernel 3.16.0-30 verwendet. Das Testsystem wurde dabei als Virtuelle Maschine (VM) in der Virtualisierungslösung „Virtualbox“ der Firma Oracle betrieben, um eine einfache Skalierung der Hardware, eine einfache Portabilität des Testsystem und einen reproduzierbaren Systemzustand, über die integrierte Snapshot-Funktion, bereitzustellen. Für die Konfiguration wurden die in Tabelle 1 dargestellten Einstellungen gewählt.

<i>Host</i>	rabbitmqserver (192.168.178.153)
<i>Anz. CPU</i>	2
<i>RAM</i>	2048 MB
<i>Grafikspeicher</i>	12 MB
<i>HDD</i>	8,00 GB
<i>Netzwerk</i>	1GB über Bridging durch lokales Netzwerk-Interface

Tabelle 1: Konfiguration der Test-VM

Für die reproduzierbare Einrichtung der Testumgebung wurde ein BASH-Skript erstellt, welches sich im Repository des zugehörigen GitHub-Projektes befindet. Es setzt eine frische Installation des Ubuntu Server voraus - ohne eine Vorauswahl an Softwarepaketen (z. B. LAMP). Vor der Ausführung des Skriptes sollte ein Snapshot erstellt werden. Anschließend kann es in der VM über:

```
$> wget https://raw.githubusercontent.com/philippsied/amqp-stress-test/master/utilities/setupTestEnv.sh
```

aus dem Git-Repository heruntergeladen werden. Da das Skript für die Einstellung des Netzwerkinterface Root-Rechte benötigt (Sudo-Rechte genügen nicht), muss der Root-User zuvor aktiviert werden. Abschließend kann das Skript mit Sudo-Rechten ausgeführt werden:

```
$> sudo passwd root
$> sudo bash setupTestEnv.sh
```

Nach Abschluss der Einrichtung erfolgt eine übersichtliche Ausgabe aller Informationen, einschließlich RabbitMQ-Benutzerdaten und Adressen.

Verwendete bzw. Erstellte Programme

RabbitMQ bietet einige Anwendungen, mit denen sich die Leistungsfähigkeit der Server messen lässt. Alle Hilfsprogramme sind innerhalb der *rabbitmq-client-tests.jar* vorzufinden. Diese JAR-Datei enthält weiterhin zahlreiche kleine Beispielpprogramme für das Testen der Funktionalität des eigenen Servers.

VirtualBox Der von uns verwendete Server wurde durch die Virtualisierungslösung VirtualBox realisiert. Neben der einfachen Installation neuer Gast-Systeme besteht die Möglichkeit Sicherheitspunkte zu erstellen. Bei einem Ausfall des System kann so der ursprüngliche Sicherungspunkt wiederhergestellt werden. Als Grundlage dient die Servervariante von Ubuntu 14.04 LTS, welche durch die fehlende grafische Oberfläche zum einsparen von Ressourcen dient.

Glances Glances ist ein System-Monitoring-Tool, das zahlreiche Informationen auf engstem Raum präsentiert. Im einfachsten Fall werden die gesammelten System-Informationen auf der Konsole ausgegeben. Ferner ermöglicht ein integriertes Web-Interface eine Fernüberwachung der Umgebung. Zu den gesammelten Informationen gehören unter anderem: CPU-Auslastung, Kernel-Version, Speicherverbrauch (HDD, RAM) und laufende Prozesse. Hierbei werden alle Informationen im Sekundentakt aktualisiert.

Perftest ist ein Performance-Test-Tool, welches beliebig viele Producer und Consumer erstellt und die Sende-/Empfangsrate misst. Zusammen mit der Latenzzeit werden alle Angaben auf der Konsole ausgegeben.

HTML Performance Tools bieten ebenfalls ein breites Spektrum an Funktionalität. Mit einer Reihe von Tools und Unterstützung von perfest lassen sich automatisierte Benchmarks erstellen. Die gelieferten Daten dienen dem Vergleich der Systems vor und während des Angriffs. Alle Ergebnisse werden in einer JSON-Datei gesichert und ansprechend in einer HTML-Seite dargestellt

AMQPstress Um die Auswirkungen der gewählten Angriffsvektoren testen zu können, wurde für jeden Angriff ein eigener Client implementiert. Grundlage bildet die Java-Library von RabbitMQ, die geeignete Funktionen zur Ansprache des Servers bereitstellt. Alle erstellten Clients lassen sich über bestimmte Parameter aufrufen und mit weiteren Einstellungen versehen. Welche Einstellungen zutreffen, lässt sich anhand dieses Dokuments erschließen. Auch zeigt sich, welche Parameter für einen erfolgreichen Angriff nötig sind. Hierzu gehört unter anderem die Anzahl an Producer und Consumer oder auch die gewählte Nachrichtengröße.

Beschreibung des Benchmarking

Für die Beobachtung des Ressourcenverbrauches auf dem RabbitMQ-Server wurde das Kommandozeilenprogramm *glances* verwendet. Der Programmaufruf für jeden Test lautete wie folgt:

```
$> sudo glances -t 5 --disable-process
```

Er veranlasst, die Ansicht alle 5 Sekunden zu erneuern und die Anzeige der aktuell laufenden Prozesse abzuschalten, um den Ressourcenverbrauch durch *glances* selbst zu reduzieren. Vor jeder Messung wurde die VM auf einen Snapshot zurückgesetzt, bei der sich das System in einem Zustand befindet, den es 5 minuten nach dem Hochfahren der VM besitzt.

S1	Leerlauf
<i>Beschreibung</i>	Der RabbitMQ-Server befindet sich im Leerlauf, d. h. ohne irgendeine Form von Last.
<i>Parameter</i>	Keine
<i>Aktion</i>	Keine
<i>Ressourcenbedarf</i>	CPU: ~0.7% RAM: 11.1% (110MB) HDD: 5.01GB/5.78GB NET: IN ~3Kbit/s OUT ~197Kbit/s
<i>Anmerkungen</i>	Keine
S2	Referenzszenario
<i>Beschreibung</i>	Ein Producer erzeugt kontinuierlich Nachrichten, die von einem Consumer kontinuierlich korrekt entnommen werden. Es finden keine weiteren Anfragen bzw. Zugriffe auf den RabbitMQ-Server statt.
<i>Parameter</i>	Messdauer: 600s (10min) 1 Consumer 1 Producer Nachrichtengröße: 1024 Byte Max. 50 Nachrichten/s (Producer)
<i>Aktion</i>	<code>sh startBenchmark.sh testc:testp@192.168.178.153:5672/%2f</code>
<i>Ressourcenbedarf</i>	CPU: ~3.8% RAM: 11.4% (113MB) HDD: 5.01GB/5.78GB NET: IN ~476Kbit/s OUT ~582Kbit/s
<i>Anmerkungen</i>	Die Sender/Empfangsrate sowie die Latenz sind wie erwartet weitgehend konstant (Siehe Abb. 1). Die Latenz liegt bei durchschnittliche 1.0 ms.

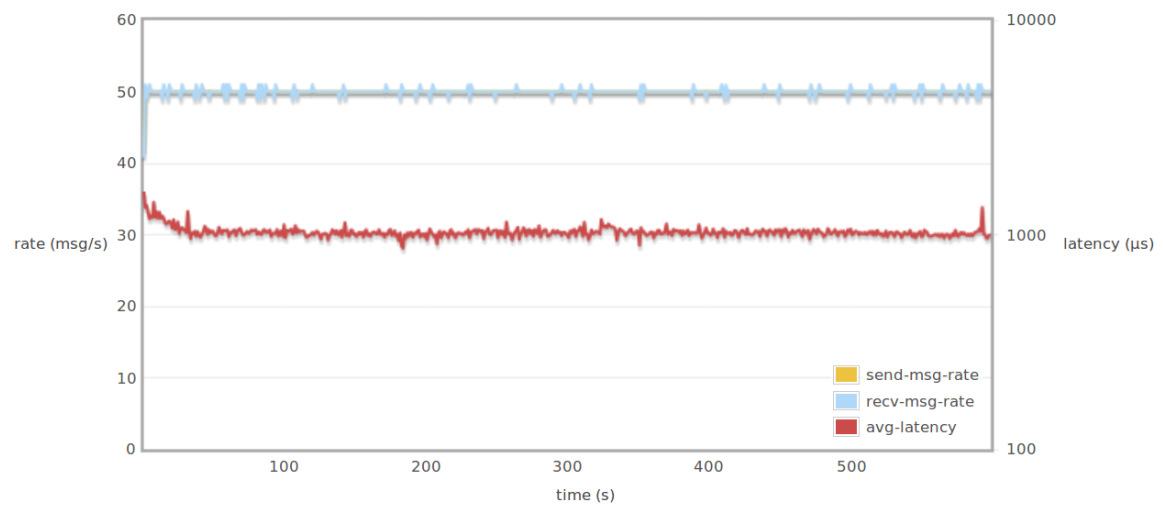


Abbildung 1: Ohne Angriff - Verlauf der Sende-/Empfangsrate und der Latenz im Referenzszenario

Beschreibung der Angriffe

A1	Referenzangriff - Kooperativer Client
<i>Beschreibung</i>	Ein Producer erzeugt kontinuierlich Nachrichten die über einen „fanout“-Exchange an 5 Consumer verteilt werden. Die Consumer quittieren dem RabbitMQ-Server dabei den Erhalt der Nachricht.
<i>Testparameter</i>	-dm ACK (Aufrufparameter für Angriff) -c 5 (5 Consumer) -i 10 (10ms Pause zwischen 2 Consumer/Producer-Anfragen) -ms 10240 (Messagegröße: 10KB) -u <uri> (URI für Verbindung mit Server) 1 Producer (Standard) Nicht-Persistente Nachrichten (Standard)
<i>Befehlszeile</i>	<pre>Amqpstress -dm ACK -c 5 -i 10 -ms 10240 -u amqp://testc:testp@192.168.178.153:5672/%2f</pre>
<i>Ressourcenbedarf</i>	CPU: ~10.1% - 13.0% RAM: 11.9% - 12.0% (118MB - 119MB) HDD: 5.01GB/5.78GB NET: IN ~8.51Mbit/s OUT ~66.67Mbit/s
<i>Beobachtungen</i>	Der Ressourcenverbrauch ist wie erwartet weitgehend konstant. Die Latenz liegt bei durchschnittliche 1.0 ms. In Bezug auf das Referenzszenario ist keine Beeinträchtigung erkennbar (Siehe Abb. 2).

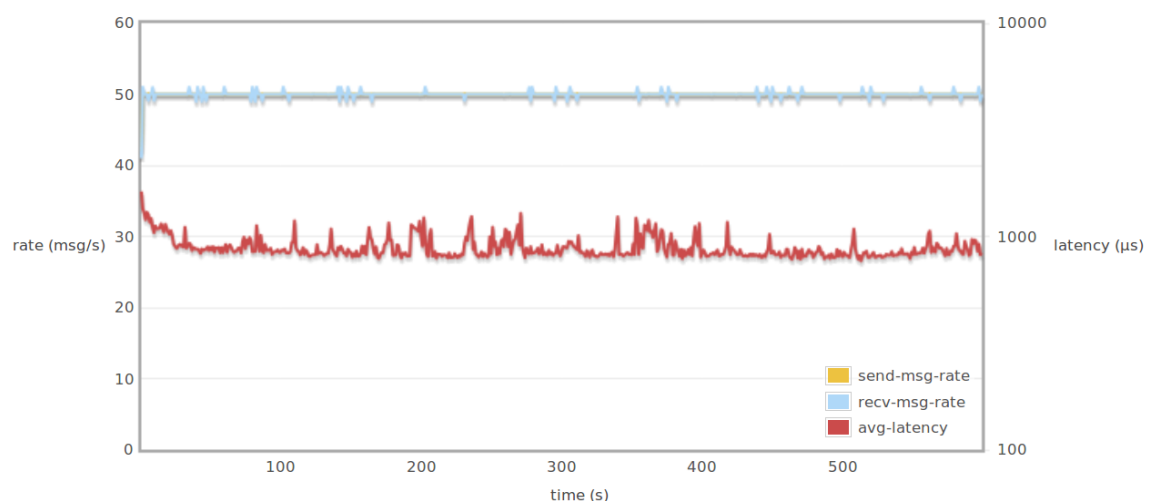
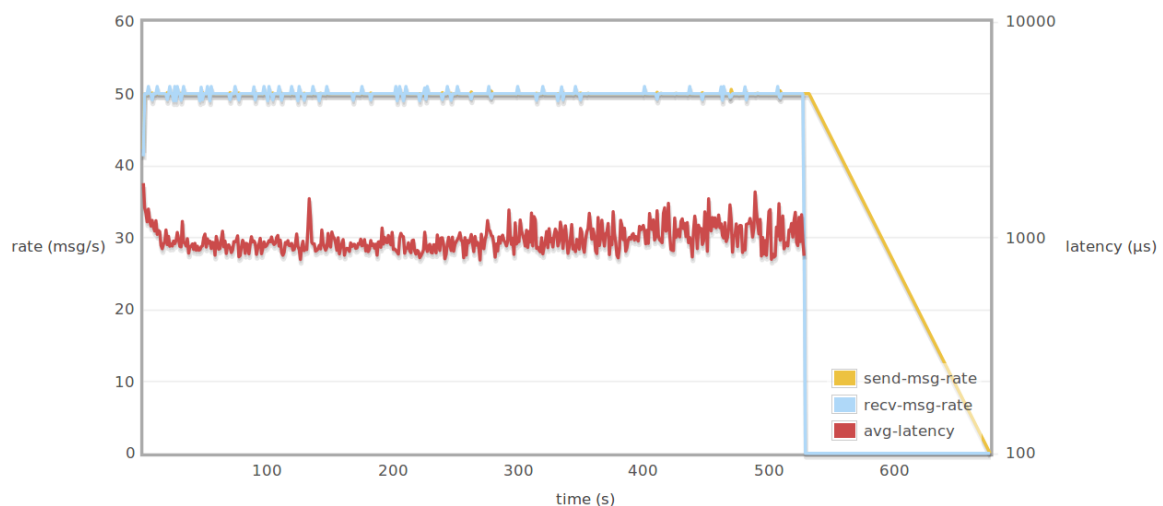
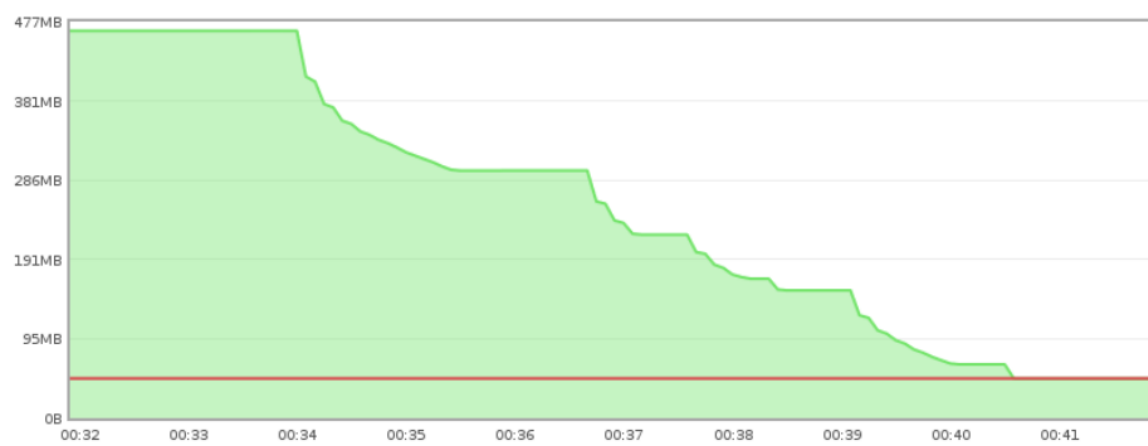
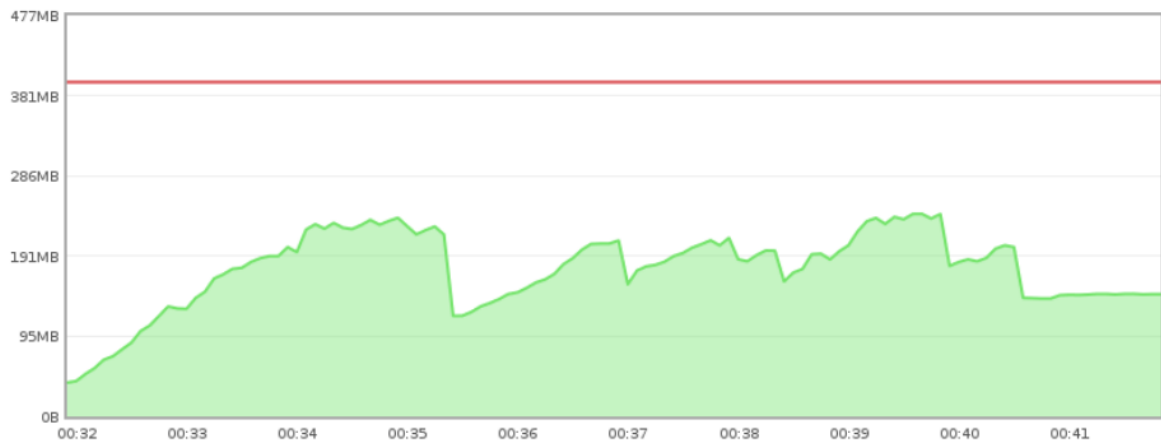


Abbildung 2: Kooperativer Client - Verlauf der Sende-/Empfangsrate und der Latenz im Referenzszenario

A2**Ignorieren von Nachrichten**

<i>Beschreibung</i>	Ein Producer erzeugt kontinuierlich Nachrichten gewisser Größe mit zufälligem Inhalt, die von einem oder mehreren Consumern empfangen, aber nicht quittiert werden. Der RabbitMQ-Server ist somit gezwungen, die Nachrichten in der Queue zwischenspeichern.
<i>Testparameter</i>	-dm NO (Aufrufparameter für Angriff) -c 5 (5 Consumer) -i 10 (10ms Pause zwischen 2 Consumer/Producer-Anfragen) -ms 10240 (Messagegröße: 10KB) -u <uri> (URI für Verbindung mit Server) 1 Producer (Standard) Nicht-Persistente Nachrichten (Standard)
<i>Befehlszeile</i>	<pre>Amqpstress -dm NO -c 5 -i 10 -ms 10240 -u amqp://testc:testp@192.168.178.153:5672/%2f</pre>
<i>Ressourcenbedarf</i>	CPU: ~11.1% - 38.7% RAM: 12.0% - 12.0% (120MB - 386MB) HDD: 5.01GB/5.78GB bis 5.42GB/5.78GB NET: IN ~8.33Mbit/s OUT ~68.0Mbit/s
<i>Beobachtungen</i>	Nachrichten werden bis zur Hälfte des eingestellten Limits (hier 200MB) im RAM gehalten, bei überschreiten lagert der RabbitMQ-Server im Hintergrund die Nachrichten auf die Festplatte aus. Durch die Freigabe des RAM-Speichers entsteht ein Sägezahnmuster. Dieser Vorgang wiederholt sich bis die Festplatte voll ist und RabbitMQ alle Verbindungen schließt und in diesem Zustand verweilt. Die CPU-Last und der Netzwerkdurchsatz fallen dabei auf Werte wie im Idle-Zustand





A3	Sofortiges Abweisen von Nachrichten
<i>Beschreibung</i>	Ein Producer erzeugt kontinuierlich Nachrichten gewisser Größe mit zufälligem Inhalt, die von einem oder mehreren Consumern empfangen, aber sofort abgewiesen (basic.Reject) werden. Der RabbitMQ-Server ist somit gezwungen, die Nachrichten in der Queue zwischenspeichern und erneut an den Consumer zu senden.
<i>Testparameter</i>	-dm REJECT (Aufrufparameter für Angriff) -c 5 (5 Consumer) -i 10 (10ms Pause zwischen 2 Consumer/Producer-Anfragen) -ms 10240 (Messagegröße: 10KB) -u <uri> (URI für Verbindung mit Server) 1 Producer (Standard) Nicht-Persistente Nachrichten (Standard)
<i>Befehlszeile</i>	<code>Amqpstress -dm REJECT -c 5 -i 10 -ms 102400 -mp -u amqp://testc:testp@localhost:5672/%2f</code>
<i>Ressourcenbedarf</i>	CPU: ~11.1% - 38.7% RAM: 12.0% - 12.0% (120MB - 386MB) HDD: 5.01GB/5.78GB bis 5.42GB/5.78GB NET: IN ~8.33Mbit/s OUT ~68.0Mbit/s
<i>Beobachtungen</i>	

A4	Gebündeltes Abweisen von Nachrichten
<i>Beschreibung</i>	Ein Producer erzeugt kontinuierlich Nachrichten gewisser Größe mit zufälligem Inhalt, die von einem oder mehreren Consumer empfangen, zunächst ignoriert werden, um sie bei Erreichen eines Schwellwertes gebündelt abzuweisen (basic.NACK). Dadurch ist der RabbitMQ-Server gezwungen alle Nachrichten zwischenspeichern und stoßweise alle Nachrichten bis zu der aktuellen Sequenznummer erneut zuzustellen.
<i>Testparameter</i>	-dm NACK (Aufrufparameter für Angriff) Schwellwert: 1000 Nachrichten (Standard) -c 5 (5 Consumer) -i 10 (10ms Pause zwischen 2 Consumer/Producer-Anfragen) -ms 102400 (Messagegröße: 10KB) -u <uri> (URI für Verbindung mit Server) 1 Producer (Standard) Nicht-Persistente Nachrichten (Standard)
<i>Befehlszeile</i>	<code>Amqpstress -dm NACK -c 5 -i 10 -ms 102400 -u amqp://testc:testp@localhost:5672/%2f</code>
<i>Ressourcenbedarf</i>	
<i>Beobachtungen</i>	

A5	Anlegen und Löschen von Queues
<i>Beschreibung</i>	Ein Client erzeugt bis zu einem Schwellwert Queues und befüllt sie mit einer zufälligen Nachricht gegebener Größe. Wenn der Schwellwert erreicht ist, werden alle Queues ohne zu Warten gelöscht und der Zyklus beginnt erneut. Der RabbitMQ-Server muss die Überreste der Queues im RAM bzw. der Festplatte bereinigen, während neue Queues angelegt und befüllt werden.
<i>Testparameter</i>	<code>-dq</code> (Aufrufparameter für Angriff) <code>-pc 10</code> (Schwellwert: 10 Queues) <code>-i 10</code> (10ms Pause zwischen 2 Consumer/Producer-Anfragen) <code>-ms 0</code> (Keine Nachrichten senden) <code>-u <uri></code> (URI für Verbindung mit Server) 1 Client - Consumer und Producer zugleich (Standard) Nicht-Persistente Nachrichten (Standard)
<i>Befehlszeile</i>	<code>Amqpstress -dq -pc 10 -i 10 -ms 0 -u amqp://testc:testp@localhost:5672/%2f</code>
<i>Ressourcenbedarf</i>	
<i>Beobachtungen</i>	

A6**Versenden von Nachrichten mit großem Header**

<i>Beschreibung</i>	RabbitMQ bietet die Möglichkeit im Header der Nachricht bestimmt Parameter für die Weiterleitung zu deklarieren. Dieser Test beschäftigt sich mit der Auswirkung, wenn der Header unnötig ausgelastet wird. Das System ist gezwungen alle Weiterleitungsoptionen zu Prüfen, auch wenn diese keinem Ziel entsprechen.
<i>Testparameter</i>	-lh (Aufrufparameter für Angriff) -ms 10000 (Messagegröße: 10000 Byte) -hs 2500 (Headergröße - Anzahl Einträge in Map) -u <uri> (URI für Verbindung mit Server)
<i>Befehlszeile</i>	<code>Amqpstress -lh -ms 10000 -hs 2500 -u amqp://testc:testp@localhost:5672</code>
<i>Ressourcenbedarf</i>	Die Anwendung generiert zu Beginn 2500 Weiterleitungsoptionen (Bestehend aus 8 Byte Key und 36 Byte Value = 44 Byte pro Eintrag) und schreibt sie in den Header jeder Nachricht. Hierdurch ist das System stark ausgelastet und der Durchsatz der Nachrichten schrumpft stark auf 10 - 20 Nachrichten pro Sekunde. Es macht keinen Unterschied ob der Key oder Value vergrößert wird, die geringe Übertragungsrate bleibt bestehen. Der Value wird daher nicht ausgewertet. Die CPU Last liegt bei 10 -15%
<i>Beobachtungen</i>	Die Headergröße ist bei etwa 2500 Weiterleitungsoptionen begrenzt. Wird diese überschritten lässt das System die Verbindung fallen, aufgrund einer zu großen Framegröße. Die Framegröße lässt sich beim Aufbau der Verbindung angeben, kann aber die bereits voreingestellten eingestellten 128 Byte nicht überschreiten.

Übertragungsrate nach Nachrichtengröße			Headergröße
10.000 Byte	1.000 Byte	100 Byte	Einträge (Byte)
140m/s	260m/s	350m/s	200 (8.800)
80m/s	120m/s	180m/s	500 (22.000)
30m/s	50m/s	70m/s	1.000 (44.000)
20m/s	30m/s	40m/s	2.000 (88.000)
10m/s	10m/s	20m/s	2.500 (110.000)
270m/s	3.000m/s	10.000m/s	kein Eintrag

A7	Aufbauen mehrerer Channel über eine einzelne Verbindung
<i>Beschreibung</i>	Neben einzelnen Verbindungen können in RabbitMQ auch mehrerer Kanäle aufgebaut werden. Hier stellt sich die Frage, wie das System mit einer Vielzahl von Kanäle zurecht kommt. Auf Basis einer einzelnen Verbindung wird das System so ausgelastet und beobachtet.
<i>Testparameter</i>	-mc (Aufrufparameter für Angriff) -ms 10000 (Messagegröße: 10000 Byte) -u <uri> (URI für Verbindung mit Server) -p 100 (100 Producer) -c 10 (10 Consumer)
<i>Befehlszeile</i>	<code>Amqpstress -mc -p 100 -c 10 -ms 10000 -u amqp://testc:testp@localhost:5672</code>
<i>Ressourcenbedarf</i>	Das System ist stark ausgelastet. Ähneln aber der Auslastung unter der Erstellung mehrerer Verbindungen. Allerdings beansprucht der Aufbau der Channel extrem viel Zeit. Nach Aufbau aller Kanäle bricht die Übertragungsrate stark ein. Dabei liegt die CPU-Last bei etwa 45 - 55%
<i>Beobachtungen</i>	Zeit für Aufbau der Channel hängt stark von der Anzahl von Producer und Consumer ab. Nachfolgend zeigt sich ein Vergleich von mehreren Kanälen sowie mehreren Verbindungen.

Tabelle 2: Mehrere Channel

Übertragungsrate (schreiben)	Producer	Consumer	Nachrichtengröße (Byte)
7.000m/s	100	10	100
800m/s	100	10	1.000
100m/s	100	10	10.000

CPU	51.8%	nice:	0.0%	LOAD	2-core	MEM	39.8%
user:	40.2%	irq:	0.0%	1 min:	0.75	total:	1.95G
system:	8.2%	iowait:	0.6%	5 min:	0.61	belegt:	796M
idle:	48.2%	steal:	0.0%	15 min:	0.41	frei:	1.18G

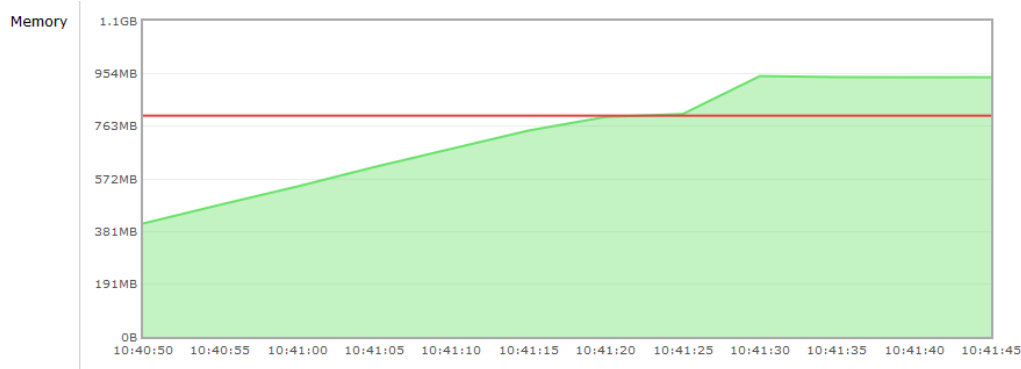
Tabelle 3: Mehrere Verbindungen

Übertragungsrate (schreiben)	Producer	Consumer	Nachrichtengröße (Byte)
24.000m/s	100	10	100
2.000m/s	100	10	1.000
100m/s	100	10	10.000

```
CPU      80.5%  nice:    0.0%  LOAD    2-core  MEM      54.1%
user:    66.1%  irq:     0.0%  1 min:   1.12  total:   1.95G
system:   8.2%  iowait:  0.4%  5 min:   0.50  belegt:  1.06G
idle:    19.5%  steal:   0.0%  15 min:  0.43  frei:    918M
```

A8**Commit mehrerer Nachrichten im Transaktionsmodus**

<i>Beschreibung</i>	Im Transaktionsmodus ist es möglich mehrere Nachrichten als Folge zu übertragen, die aber vergleichbar mit Datenbanken als Einheit betrachtet werden. Nur durch die Commit()-Funktion wird der neue Zustand angenommen und die Nachrichten im System zur Verfügung gestellt. Ferner kann mit der Rollback()-Funktion der ursprüngliche Zustand wiederhergestellt werden. Zu untersuchen wäre die Situation, wenn permanent Nachrichten ohne commit gesendet werden - der Server muss die Nachrichten dann im Speicher belassen.
<i>Testparameter</i>	-tx (Aufrufparameter für Angriff) -p 100 (100 Producer) -ms 10000 (Messagegröße: 10000 Byte) -mct 10000 (Nachrichtenanzahl pro Producer: 10000) -co false (Commit der Transaktion - hier: Auslassen) -u <uri> (URI für Verbindung mit Server)
<i>Befehlszeile</i>	<pre>Amqpstress -tx -p 100 -ms 10000 -mct 10000 -co false -u amqp://testc:testp@localhost:5672</pre>
<i>Ressourcenbedarf</i>	Durch Auslassen des Commits steigt der Speicherverbrauch stark an. Nach wenigen Sekunden ist die Speichergrenze erreicht und keine weiteren Nachrichten werden übertragen. Daraufhin verharren alle Producer bis der Speicher wieder freigegeben wird (Falls Consumer vorhanden)
<i>Beobachtungen</i>	Sporadisch friert der RabbitMQ-Server bei diesem Versuch ein. Ein Aufbau einer neuen Verbindung schlägt fehl und die Weboberfläche ist nicht mehr erreichbar. Nach längerer Zeit (etwa 10 Minuten) baut der Server aber wieder die Verbindungen ab und ein Zugriff ist wieder möglich. Dennoch bleibt der Speicherverbrauch bestehen.



A9	Verzögerung des Verbindungsaufbaues
<i>Beschreibung</i>	.
<i>Testparameter</i>	-u <uri> (URI für Verbindung mit Server)
<i>Befehlszeile</i>	<code>Ampstress -u amqp://testc:testp@localhost:5672</code>
<i>Ressourcenbedarf</i>	
<i>Beobachtungen</i>	

A10	Ausnutzung des Hearthbeats
<i>Beschreibung</i>	.
<i>Testparameter</i>	-u <uri> (URI für Verbindung mit Server)
<i>Befehlszeile</i>	<code>Ampstress -u amqp://testc:testp@localhost:5672</code>
<i>Ressourcenbedarf</i>	
<i>Beobachtungen</i>	

Auswirkungen der Angriffe

Zusammenfassung und Fazit