PRTG – Failover Cluster mit Citrix ADC

Bei meinem aktuellen Arbeitgeber steht die Migration in zwei neue Rechenzentren an. Eines der Ziele dieser Migration ist die Erhöhung der Ausfallsicherheit. Dies habe ich zum Anlass genommen mir den PRTG Failover Cluster mit einem vorgeschalteten Citrix ADC einmal anzuschauen.

Die Installation und Konfiguration ist eigentlich recht einfach und das Vorgehen möchte ich in diesem Artikel nochmals erläutern.

PRTG Failover Cluster konfigurieren

Um den Core-Server von PRTG als Failover-Cluster zu konfigurieren gibt es seitens PAESSLER zwei gute Artikel:
– Failover Cluster Configuration
– Failover Cluster Step by Step

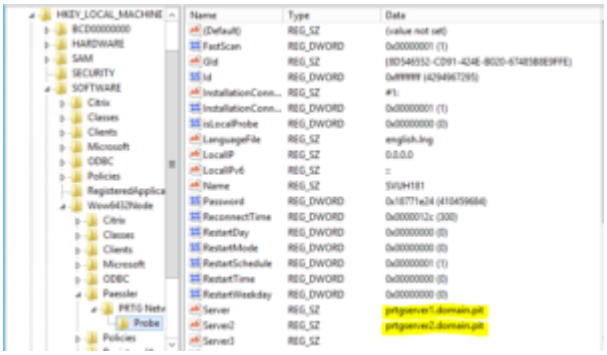
Wenn man sich an diese hält, läuft der Cluster in kürzester Zeit. Was gibt es zu beachten?

- Der zweite Cluster-Node ist immer Read-Only, d.h. selbst bei einem Ausfall des Master-Servers kann auf dem Failover-Server nur überwacht, jedoch nicht konfiguriert

werden.

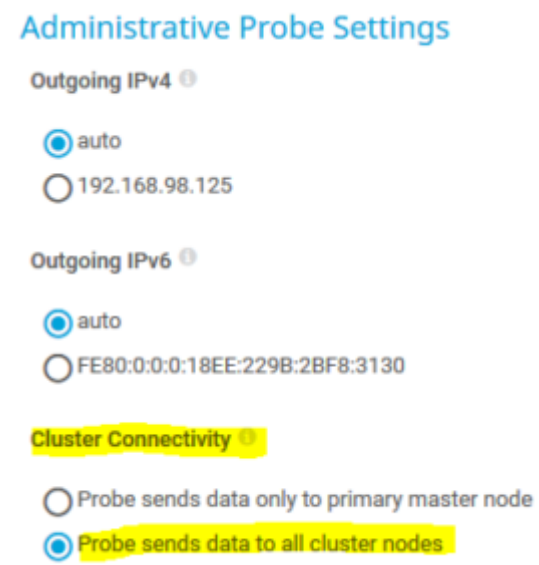
- Remote Probes müssen so (um-)konfiguriert werden, dass sie ihre Daten an alle Cluster Nodes senden und nicht nur dem Master.
- Die Remote Probes werden vom PRTG Cluster selbst konfiguriert. Eine allfällige Registry Anpassung (manuell oder via GPP) wird wieder überschrieben.
- Remote Probes müssen jeden Cluster Node einzeln erreichen können. Bei einer NAT Konfiguration bedeutet dies ein eigener FQDN und NAT Zugang pro Core Server.
- Der erste Administrator (prtgadmin) ist autonom pro Node. Um spätere Probleme zu vermeiden sollte das Passwort auf beiden Servern identisch gesetzt und mit der AD Authentifizierung gearbeitet werden.
- Nur der Master-Server sieht sich selbst noch als „Local Probe“. Auf den Failover-Servern ist nur der „Cluster Probe“ und alle anderen Remote Probe Server ersichtlich.
- Die Probe Dienste der PRTG Core Server senden ihre Daten nur lokal (127.0.0.1).

In den Cluster Einstellungen sollte man die „Node Namen“ passend setzen und die IP Adressen durch FQDN ersetzen.
Dies macht es einerseits übersichtlicher für alle PRTG Benutzer und andererseits ist man unabhängiger bei einer allfälligen Änderung der IP Adressierung.



Kontrolle in der Registry auf einem Remote Probe Server

Kontrolle im Cluster Status



Cluster-Konfiguration der Remote Probes

Hinweise:

– Man kann zwar im GUI dem Master Server einen DNS Alias setzen, die Remote Probes erhalten jedoch immer den originalen Hostname übermittelt.

– Die Änderung wird sofort an die Remote Probes übermittelt.

Bei einer frischen Installation kann nun die Konfiguration direkt in der Cluster Probe gestartet werden. Wurde ein Solo PRTG Core Server in einen Cluster umgewandelt, so müssen die konfigurierten Gruppen, Geräte und Sensoren vomr „Local Probe“ in den „Cluster Probe“ verschoben werden:

Konfiguration Citrix ADC

Nachdem nun der PRTG Failover Cluster soweit konfiguriert ist, bauen wir nun den Zugriff auf diesen. Ohne ADC würde man nun entweder mittels DNS Round-Robin einen FQDN konfigurieren, wobei man hier nicht steuern kann auf welchem Node man landet, oder man arbeitet mit zwei verschiedenen FQDN, was wiederum nicht Anwenderfreundlich ist.

In diesem Abschnitt wird die Konfiguration eines LB vServer mit Failover Funktion erläutert.

Hierzu werden alle (normalerweise zwei) Cluster Nodes im ADC erfasst:

```
add server prtgserver1 prtgserver1.domain.pit
add server prtgserver2 prtgserver2.domain.pit
```

Für jeden Server erstellen wir einen Service. Nach best practice sind die PRTG Server SSL verschlüsselt, somit bauen wir passende Services dazu:

```
add service svc-https-prtgserver1 prtgserver1 SSL 443
add service svc-https-prtgserver2 prtgserver2 SSL 443
```

Im Gegensatz zu einem normalen Loadbalancing wird im Failover nicht ein einzelner sondern zwei vServer benötigt, um den zweiten als Backup zu konfigurieren. Dem vServer mit einer IP wird der Service des PRTG Master Servers angefügt. Der zweite vServer (ohne Adressierung) steuert den PRTG Failover Server an. Beide LB vServer benötigen auch das dazu passende SSL Zertifikat:

```
add lb vserver lb-vsrv-prtg.domain.pit SSL 192.168.200.222 443
add lb vserver lb-vsrv-prtg-backup.domain.pit SSL 0.0.0.0 0

bind lb vserver lb-vsrv-prtg.domain.pit svc-https-prtgserver1
bind lb vserver lb-vsrv-prtg-backup.domain.pit svc-https-prtgserver2

bind ssl vserver lb-vsrv-prtg.domain.pit -certkeyName wildcard.domain.pit
bind ssl vserver lb-vsrv-prtg-backup.domain.pit -certkeyName wildcard.domain.pit

set lb vserver lb-vsrv-prtg.domain.pit -backupVServer lb-vsrv-prtg-backup.domain.pit
```

Dem Service Monitoring habe ich am meisten Zeit gewidmet. Die PRTG Server bieten eine Status-Seite (/api/public/testlogin.htm), welche jedoch bereits bei einem Problem mit dem Mailserver ein „NOTOK“ zurück meldet.
Nur diese Status-Seite alleine konnte ich also nicht nutzen.

Daher baute ich ein Monitoring basierend auf dieser plus zusätzlichen zwei Standard-Monitoren (TCP und HTTP). Da sich der TCP-Default Monitor nicht anfügen lässt wenn bereits ein anderer Monitor in Benutzung ist, habe ich einen eigenen erstellt.
Wegen der Benutzung von HTTPS muss dem HTTP Monitor der Response Code 302 hinzugefügt werden.

```
add lb monitor mon-prtg-TCP TCP
add lb monitor mon-prtg-http HTTP -respCode 200 302 -httpRequest "HEAD /" -secure YES
```

Das Monitoring der Status-Seite bat mir ein erstes Mal die Nutzung des „Reverse“ Monitorings. Würde man nämlich nur die Antwort „OK“ prüfen, so wäre der Monitor auch bei einem „NOTOK“ zufrieden, da „OK“ ein Bestandteil der Antwort ist. Daher prüfen wir auf ein „NOTOK“ und geben mit dem Monitor grünes Licht, falls diese Antwort nicht vorhanden ist – Reverse eben. ;-)

```
add lb monitor MON-PRTG-Core-Status HTTP-ECV -send "GET /api/public/testlogin.htm" -recv NOTOK -reverse YES -secure YES
```

Zu guter Letzt müssen die neu gebauten Monitore in den Services konfiguriert werden. Dazu fügen wir pro Service die drei hinzu und definieren den Monitoring Schwellwert 2. So bleibt der Service verfügbar, solange zwei Monitore grünes Licht geben:

```
bind service svc-https-prtgserver1 -monitorName mon-prtg-http
bind service svc-https-prtgserver1 -monitorName mon-prtg-TCP
bind service svc-https-prtgserver1 -monitorName mon-prtg-Core-
```

```
Status
bind service svc-https-prtgserver2 -monitorName mon-prtg-http
bind service svc-https-prtgserver2 -monitorName mon-prtg-TCP
bind service svc-https-prtgserver2 -monitorName mon-prtg-Core-
Status

set service svc-https-prtgserver1 -monThreshold 2
set service svc-https-prtgserver2 -monThreshold 2
```

Mit dieser Konfiguration kann nun ein Benutzer über eine FQDN (z.B. prtgcluster.domain.pit) auf die PRTG Oberfläche zugreifen. Der LB vServer vom ADC schaltet erst auf den Failover Server um, sobald der Master Server nicht mehr verfügbar ist (z.B. Neustart). Ist der Master Server wieder online, schaltet der ADC wieder auf diesen zurück.

Viel Spass beim Nachbauen. :-)

ADC-PRTGHerunterladen