Ausfallsicheres Webhosting

Werner Illsinger

Sicherlich ist bekannt, dass man 100 Prozent Ausfallsicherheit auch mit riesigem Aufwand nicht erreichen kann. Man kann nur danach streben, einen möglichst hohen Grad zu erreichen.

Was tun wir derzeit schon alles, um eine möglichst hohe Sicherheit zu erreichen?

Internet Anbindung

Am Standort Rennweg gibt es drei Internet Anbindungen von zwei unterschiedlichen Providern (Silver Server und Inode).

Stromversorgung

Alle Server werden über eine große unterbrechungsfreie Stromversorgung von APC mit Strom versorgt. Sollte es zu Stromproblemen kommen, wird der Betrieb dadurch eine gewisse Zeit aufrechterhalten. Da die Stromversorgung aber in Wien relativ stabil ist, gab es hier noch nie wirkliche Probleme.

Virtualisierung und Clusterung

Früher war jedes Service auf einem eigenen physischen Server installiert. Das heißt, wenn es Hardwareprobleme gab, dass das Service auf diesem Rechner nicht mehr erreichbar war. Mittlerweile haben wir fast alle Server virtualisiert. Diese laufen auf einem Cluster mit der Virtualisierungssoftware Hyper-V (beim Microsoft Windows Server inkludiert). Wenn es zum Ausfall eines der Virtuellen Hosts kommt, dann wird die Aufgabe dieses Hosts vollautomatisch von einem anderen *Cluster Node* übernommen.

Die *Cluster Nodes* sind über (mindestens) drei Netzwerke miteinander verbunden. **(Bild 1)**

Über das erste Netzwerk (Kundennetzwerk) wird auf die Virtuellen Server aus dem Internet zugegriffen.

Mit dem *Heartbeat Netzwerk* überprüfen die Clusternodes, ob die anderen Rechner im Cluster noch ordnungsgemäß funktionieren.

Mit dem dritten Netzwerk (SAN) wird auf die externe Platte, die sich die Cluster Nodes teilen, zugegriffen. Am SAN liegt auch das sogenannte Cluster Shared Volume (CSV). Auf diesem Shared Volume liegen dann auch die virtuellen Server, die auf den Hosts laufen.

Als SAN kann auch ein Windows Rechner verwendet werden. Wir verwenden hier das iSCSI *(Internet Small Computers System Interface)* Protokoll. iSCSI erlaubt normale IP-Netzwerke dazu zu verwenden, Platten an einen Rechner anzubinden. Das senkt die Kosten dramatisch, denn herkömmliche SAN Netzwerkkomponenten sind sehr teuer.

Microsoft stellt seit einiger Zeit die iSCSI-Target Software (sozusagen der iSCSI-Server) für Windows gratis zur Verfügung:
http://www.microsoft.com/download/en/details.aspx?id=19867

Die Client Software ist sowohl in den Server als auch Client Varianten von Windows seit einiger Zeit standardmäßig enthalten. Wem die Funktionen nicht ausreichend sind, der sei auf das Produkt der Firma Starwind Software verwiesen, die ebenfalls ein iSCSI-Target für Windows zur Verfügung stellt, das auch z.B. geclustert werden kann, um die Ausfallsicherheit noch weiter zu erhöhen.

Die beiden Server werden in einem Microsoft Failover Cluster installiert. Als Rolle wird auf den Servern Hyper-V installiert. Die beiden Rechner können auch in der sogenannten Server Core Installation aufgesetzt werden – wobei die Server dann kein Benutzerinterface mehr haben und nur noch über Scripts administriert werden können. Das hat den Vorteil, dass die Server dann auch weniger Angriffsfläche bieten, und auch weniger Patches benötigen.

Als Netzwerk verwenden wir für alle Netzwerke geswitchtes Gigabit Ethernet über Kupferkabel.

Durch die Virtualisierung aller Rechner sind wir gegen Ausfall der Hardware der Server sehr gut geschützt. Beim Ausfall eines der Rechner übernimmt der andere Clusternode binnen kürzester Zeit – und für den Anwender sollte ein Ausfall nicht zu merken sein. Auch für die Wartung der Clusternodes können die virtuellen Server im laufenden Betrieb von einem auf den anderen Server verschoben werden *(Live Migration)*. Damit können die Virtual Hosts gepatcht und auch neu gebootet werden, und der Anwender merkt nichts davon.

Ausfallsicherung der virtuellen Server

Die oben beschriebenen Funktionen helfen noch nicht, um die die wirklichen, nun nur noch virtuellen Server ausfallsicher zu machen. Wenn z.B. der Webserver der nun virtualisiert auf einem der Clusternodes läuft, sich nicht mehr starten lässt oder ein anderes Problem hat, dann läuft zwar die Hardware perfekt, aber der Web Server selbst leider nicht. Wir sind daher gerade dabei, eine Web Farm aufzubauen. D.h. Es wird nicht nur ein Webserver laufen, sondern mindestens zwei.

Der Internet Information Server (IIS 7.5) bietet seit dem Windows Server 2008 ein tolles neues Feature – nämlich *Shared Configuration*. Mittels *Shared Configuration* kann man zwei oder mehrere Web Server so einrichten, dass die Webserver auf die exakt gleiche Konfiguration zugreifen und so auch exakt gleich reagieren. Wenn man die Konfiguration auf einem Server ändert, dann wird sie automatisch auch am anderen Server geändert, da ja beide Web Server auf die gleiche Konfiguration zugreifen. **(Bild 2)**

Problem dabei ist, dass jeder Web Server ja eine eigene IP Adresse hat, und diese auch im Name Server eingetragen werden muss. Daher ist das alleine noch nicht die Lösung. Um dieses Problem auch noch zu lösen, benötigt man entweder einen *Hardware Load Balancer* (z.B. BigIP von F5 Netwoks oder Barracuda, etc.) – oder man verwendet eine Funktion, die im Windows Server ebenfalls gratis verfügbar ist: *Application Request Routing* (ARR). ARR ist ein *IP Load Balancer* auf *Application Level*, der aus dem Internet kommende Http-Requests auf die vorhandenen Web Server weiterroutet – und so gewünscht auch cacht. Das Setup inklusive der Firewalls würde dann in etwa so aussehen: **(Bild 3)**

Zwei Stück *Application Request Router* – um auch hier ausfallsicher zu sein – vor den zwei Web Servern. Bliebt nur noch das Problem, wie man die beiden ARR Server durch eine gemeinsame IP-Adresse aus dem Internet erreichbar macht. Dies geschieht mittels *Network Load Balancing*

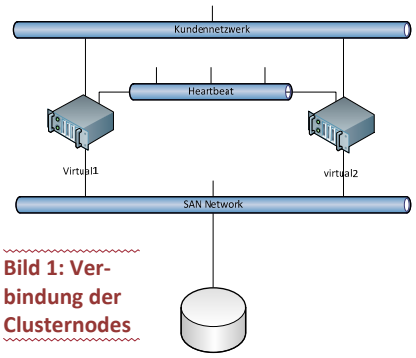

Bild 1: Verbindung der Clusternodes

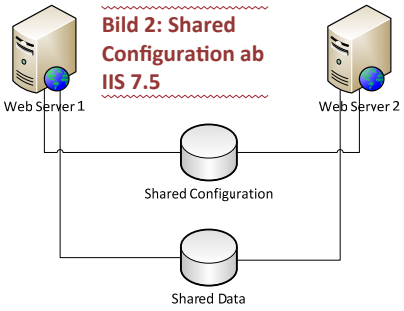

Bild 2: Shared Configuration ab IIS 7.5

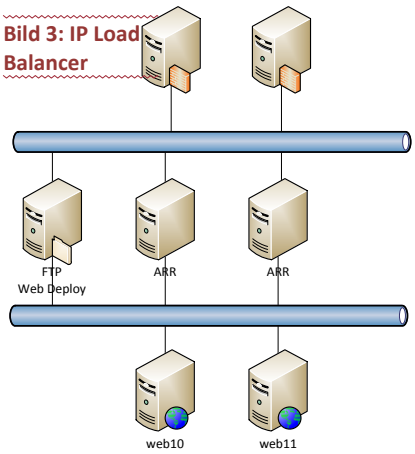

Bild 3: IP Load Balancer

Funktion (NLBS Service im Windows Server ebenfalls gratis dabei). Durch NLBS werden die beiden ARR Server dann beide über die gleiche IP Adresse erreichbar – die dann auch im DNS Server als Web Server Adresse eingetragen wird.

Es kann jetzt sowohl einer der beiden ARR Server ausfallen als auch einer der beiden Web Server – die Website bleibt in jedem Fall weiterhin erreichbar. Auch zu Wartungszwecken können einzelne Server „offline" genommen werden, um z.B. Software zu installieren, sie zu rebooten, etc.

Weitere Informationen

IIS Shard Configuration:
http://learn.iis.net/page.aspx/264/shared-configuration/

IIS Application Request Routing
http://learn.iis.net/page.aspx/489/using-the-application-request-routing-module/

Sicherung von E-Mail und Datenbank

Mit diesen Schritten haben wir unser Ziel, die Hosting Infrastruktur möglichst ausfallsicher zu machen, fast erreicht. Es fehlen uns jetzt lediglich noch die Datenbank und der Mailserver. Mehr über diese Dienste werden wir in einer der nächsten Ausgaben berichten.