ZFS & Co -
Die Vorteile von Solaris für ausfallsichere Mailsysteme

Thomas Nau
Universität Ulm - kiz
Ulm

Schlüsselworte:

ZFS, Email, COMSTAR, CrossBow, Volume-Manager, Solaris Container, Zonen

Einleitung:

Email zählt heute stärker denn je zu den kritischen Anwendungen im RZ, unabhängig von der Ausrichtung des Unternehmens oder der Hochschule. Gehören redundant ausgelegte Systeme in Form von Clustern zum guten Ton, so hat vor allem die Wahl des Betriebssystems maßgeblichen Einfluss auf die Wartbarkeit, Verfügbarkeit und die Desaster-Recovery-Zeit. An Hand der Evolution des Mail-Systems der Universität Ulm mit einer Größe von ca. 10.000 Nutzern zeigt der Erfahrungsbericht nicht nur die technischen Schwachstellen herkömmlicher Lösungen auf, sondern vermittelt auch das Wissen wie diese mit Solaris Mitteln beseitigt werden können. Im Mittelpunkt stehen hierbei insbesondere Volume-Manager und Filesysteme, jedoch auch Techniken wie COMSTAR oder CrossBow, die mit Solaris 11 Express verfügbar sind.
Die SPAM- und Virenproblematik ist nicht Bestandteil des Vortrages.

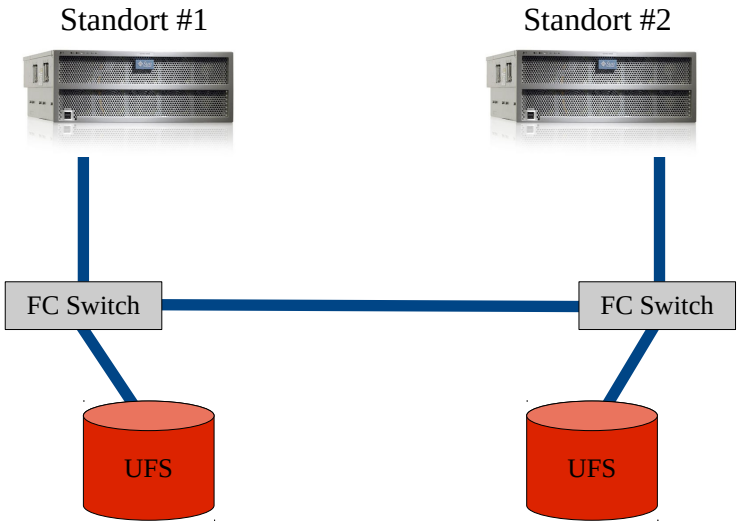
Hintergrund:

Das Kommunikations- und Informationszentrum (kiz) der Universität Ulm trägt unter anderem die Gesamtverantwortung für deren IT-Infrastruktur, inklusive Telefonie, sowie deren Versorgung sowohl mit Elektronischen- als auch mit Print-Medien. Die Kernaufgaben der Abteilung Infrastruktur umfassen hierbei insbesondere Planung, Weiterentwicklung und den Betrieb von

- Cluster basierenden universitätsweiten Mail-, LDAP-, Portal-, Datenbank- und File-Services
- Backup Services für die Universitäten Konstanz und Ulm
- eines HPC Clusters für die Universitäten in Konstanz, Stuttgart und Ulm
- 4 lokale Netzwerke plus flächendeckendes Campus WLAN und MAN im Ulmer Stadtbereich
- Telefonanlage mit ca. 14.000 Anschlüssen unter Einsatz von VoIP und 2-Draht Technik

Durch die vor einigen Jahren durch das Präsidium der Universität im Rahmen einer Corporate-Identity-Initiative beschlossene Zentralisierung aller Email-Dienstleistungen, stellt deren Betrieb und Weiterentwicklung eine besondere Herausforderung in Bezug auf Skalierung und Ausfallsicherheit dar und muss als unternehmenskritisch eingestuft werden.
Dabei fällt auf, dass sich Email in den vergangenen Jahren von einem reinen asynchronen Kommunikationsmedium hin zu einer Art universeller Ablage entwickelt hat. Dieses Nutzerverhalten wird durch die immer leistungsfähigeren Volltext Indizier-Mechanismen moderner Email Clients noch gefördert. Darüber hinaus erwarten heute die meisten Email Nutzer ein Zeitverhalten wie es eigentlich im Instant Messaging Bereich angesiedelt ist, d.h. Verzögerungen werden selbst im Minuten Bereich in aller Regel nicht mehr toleriert.

Historie:



Bis Anfang 2006 entsprach die Konfiguration des zentralen Mail Systems weitgehend dem üblichen Design aus redundanten Servern mit RAID-5 Speicher-Systemen an zwei Standorten. Betriebssystemseitig kam der *Solaris Volume Manager* und *logging UFS* auf Basis von Solaris 10 zum Einsatz. Für den Desaster-Recovery Fall wurden auch damals schon off-site Spiegel der Backup Daten an der Universität Karlsruhe gesichert.

"Freeing free inode" und eine Panik des Solaris Kernels führten im Februar 2006 letztendlich zu einem nahezu kompletten Ausfall des Systems von knapp 4 Tagen, wenngleich dieser teilweise durch ein Wochenende abgemildert wurde. Es zeigte sich im Nachhinein, dass keine Datenverluste zu beklagen waren sofern hier Aussagen in Form einer post-mortem Überprüfung überhaupt möglich sind.

Analyse und erste Konsequenzen:

Die anschließende Analyse legte einige grundlegende, designbedingte und daher nicht behebbare Schwachstellen offen, die das Standard HA-System plötzlich in ein "highly unavailable system" verwandelt haben.
So zeigte sich später bei einem der verwendeten Fiber-Channel Ports, vermutlich auf Grund eines vorausgegangenen partiellen Stromausfalls, eine stark erhöhte Fehlerrate. Diese Fehler wurden zum Zeitpunkt des Ausfalls teilweise weder von der Firmware der Switches noch vom Betriebssystem erfasst, sondern zeigten sich erst nach der Umstellung auf ZFS in Form von Prüfsummenfehlern. Daher liegt der Schluss nahe, dass insbesondere auch Metadaten des UFS Filesystems in Mitleidenschaft gezogen wurden. Dies macht einen Filesystem-Check, auch beim Einsatz von UFS-logging, unumgänglich. Nach dessen Laufzeit von über 10 Stunden (auf Grund vieler kleiner Dateien) und anschließender Reaktivierung des Mail-Systems kam es innerhalb weniger Sekunden erneut zu einer Kernel Panik.
Betrachtet man an dieser Stelle die Arbeitsweise des *Solaris Volume Managers (SVM)* näher, so wird zumindest im Nachhinein sofort klar, dass *fsck(1m)* aus statistischer Sicht keinen Erfolg garantieren kann. Zwar werden Schreibzugriffe parallel auf beide Hälften des Spiegels ausgeführt, Lesezugriffe verwenden jedoch aus Performance Gründen als Voreinstellung eine *round-robin* Strategie. Dies gilt daher insbesondere auch für das Lesen von Daten im Rahmen des Filesystem-Checks da *SVM* unterhalb der Ebene der Filesysteme auf dem Block-Layer arbeitet. Hieraus folgt sofort, dass für jeden Block-Zugriff, auch auf die Metadaten des Filesystems, lediglich eine 50:50 Chance besteht, defekte Einträge zu erkennen und ggf. zu korrigieren. Dieses grundsätzliche, von Solaris unabhängige und nicht behebbare Designproblem haftet allen Volumen Managern an, die ohne Prüfsummen allein auf dem Block-Layer arbeiten.

Als letztes und zeitaufwändigstes Problem in der Kette von Ereignissen, ist die Wahl der falschen Tools zu nennen. Der Einsatz von *rsync(1),* um die Daten des read-only gemounteten (hier hatten wir Glück) UFS Filesytems auf ZFS zu übertragen, trug mit über 40 Stunden Laufzeit erheblich zur Gesamtdauer des Ausfalls bei. Zu diesem Zeitpunkt konnten jedoch bereits wenige Dutzend Nutzer mit zeitkritischen Aufgaben wieder auf essentielle Email Daten zugreifen. Auch konnten wieder neue Emails verschickt und empfangen werden. Nachfolgende Tests und darauf basierende Schätzungen führten zu dem Schluss, dass das Einspielen des letzten Backups und eine nachfolgende Synchronisation mittels *rsync(1)* etwa 24 Stunden eingespart hätte.
Als wichtigste Konsequenz neben dem technisch unabdingbaren Wechsel hin zu ZFS finden seither zwei mal pro Jahr Desaster-Recovery Tests statt, bei denen eine komplette Wiederherstellung aller Email Daten innerhalb eines Arbeitstages erfolgen muss.

Die derzeit einzige Lösung: ZFS

Bei der Entwicklung von ZFS wurden insbesondere auch die Design bedingten Schwachstellen herkömmlicher Lösungen korrigiert. Für das oben geschilderte Szenario sind besonders die folgenden Eigenschaften von ZFS relevant:

- "Starke" 256-bit Prüfsummen wie *fletcher4* oder *sha256* erlauben es, Fehler auf dem gesamten Daten-Weg zu erkennen und bei entsprechender redundanter Auslegung diese auch zu korrigieren. Diese Prüfsummen werden nicht zusammen mit den Daten, sondern im sogenannten Pointer-Bereich abgelegt.
- Gültige Daten werden niemals überschrieben (copy on write, COW).
- ZFS integriert den Volume Manager und hat damit kein "*round-robin* Problem".
- ZFS legt für besonders wichtige Daten, etwa Metadaten des Filesystems, Kopien in sogenannten ditto-blocks ab. Diese sind von der übergeordneten Redundanz unabhängig und ermöglichen im Fehlerfall eine weitgehende Navigation im Filesystem (*cd*, *ls*, …)
- ZFS ist von der Prozessor Architektur unabhängig, was eine Datenmigration auf die binär-Daten der Anwendungen beschränkt.

Darüber hinaus bietet ZFS eine Vielzahl betriebsrelevanter Vorteile, etwa snapshots und clones. Diese kommen vermehrt als Ergänzung bzw. als Ersatz üblicher Backup-Lösungen zum Einsatz. Letztere erlauben es, bei Filesystemen mit mehreren 10 Millionen Dateien, häufig nicht mehr, ein oder mehrere, Backups pro Tag anzufertigen. Darüber hinaus ist auf Grund der langen Laufzeiten eine Konsistenz der Metadaten des Email Systems, vorgehalten in einzelnen Dateien, nicht zu gewährleisten.
Unerkannte Fehler, die sich erst zu einem späteren Zeitpunkt zu einem Problem auswachsen, lassen sich mittels scrubbing frühzeitig aufspüren und, bei entsprechender Konfiguration, auch beheben. Hierbei werden alle verwendeten Blöcke des zpools gelesen und an Hand der Prüfsummen kontrolliert. Sollten Diskrepanzen auftreten, können diese, sofern zumindest eine Kopie in Ordnung ist, korrigiert werden. In den frühen ZFS Version hatte das scrubbing einen gravierenden negativen Einfluss auf die IO-Performance der Systeme, dies wurde jedoch im aktuellen Solaris 11 Express Release behoben. In den allermeisten Fällen empfiehlt es sich daher alle zpools oft und regelmäßig zu überprüfen.

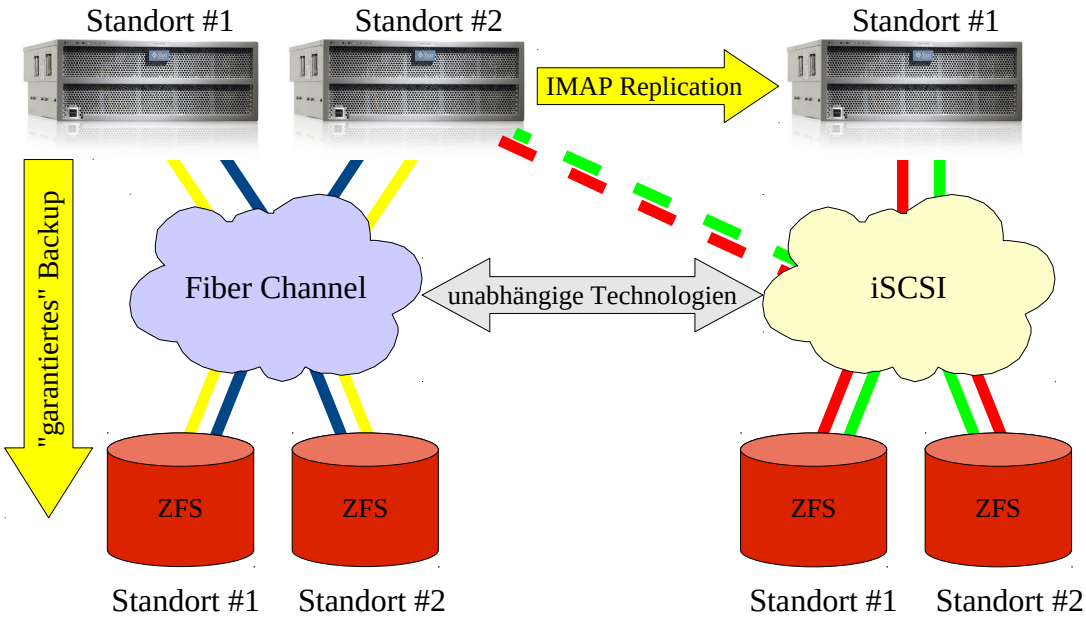
Das nachfolgende Beispiel verdeutlicht die Erkennung von Fehlern:

```
obi-wan# zpool scrub testpool; sleep 15; zpool status -v

  pool: testpool
 state: ONLINE
status: One or more devices has experienced an unrecoverable error. An
        attempt was made to correct the error.  Applications are
        unaffected.
action: Determine if the device needs to be replaced, and clear the errors
        using 'zpool online' or replace the device with 'zpool replace'.
   see: http://www.sun.com/msg/ZFS-8000-9P
 scrub: scrub in progress, 26.21% done, 0h1m to go
config:

        NAME                STATE     READ WRITE CKSUM
        pool                ONLINE       0     0     0
          mirror            ONLINE       0     0     0
            /var/tmp/vdev1  ONLINE       0     0     0
            /var/tmp/vdev2  ONLINE       0     0    58  228.5 repaired
```

Evolution:

Entscheidend für zentrale IT-Dienstleistungen am kiz der Universität Ulm ist eine kontinuierliche Weiterentwicklung, sowohl was Verfügbarkeit und Performance, aber insbesondere auch Desaster-Recovery Szenarien angeht. Eine konsequente Nutzung neuer und neuester Technologien im Solaris Umfeld, etwa auch Solaris 11 Express, erlaubten es uns, in den vergangenen 5 Jahren, in allen genannten Bereichen entscheidende Verbesserungen zu erreichen.

Der derzeitige Entwicklungsstand lässt sich also wie folgt zusammenfassen:



In einem ersten Schritt wurden alle beteiligten Systeme mittels MPxIO (IO Multipathing) redundant über unabhängige Kabeltrassen miteinander verbunden. Weiterhin erlaubt der Einsatz von COMSTAR

(Common Multiprotocol SCSI Target) den Betrieb einer iSCSI Infrastruktur, deren Komponenten vollständig unabhängig vom primären Fiber Channel Netzwerk sind, jedoch gleichzeitig den Zugriff durch alle Server im Bedarfsfall ermöglichen. Dies kommt insbesondere dem Desaster-Recovery System zu Gute, bei dem auf Ebene des Cyrus IMAP-Servers eine asynchrone, und vom Filesystem unabhängige, Replikation in einen zweiten zpool stattfindet. Die zeitliche Verzögerung liegt hier im Allgemeinen bei wenigen Sekunden.
Zwei weitere Optionen des eingesetzten IMAP Servers, *"delayed expunge"* und *"delayed mailbox delete",* sorgen dafür, dass Löschvorgänge durch Anwender erst verzögert, bei uns nach 24 Stunden, vollzogen werden. Diese Verzögerung ist für den Nutzer nicht sichtbar, stellt jedoch im Zusammenspiel mit der ZFS snapshot Technologie sicher, dass jede Mail auch im Backup System gesichert wird. Für unsere Anwender hat der Einsatz dieser Techniken den erfreulichen Nebeneffekt, dass gelöschte aktuelle Emails sehr schnell restauriert werden können.

Was bringt 2011 und 2012?

Die wesentlichen Weiterentwicklungen unserer Email Services werden sicherlich im Bereich neuer Technologien im Solaris 11 Umfeld stattfinden. Insbesondere der vollständige Ersatz althergebrachter Backup Techniken durch snapshots und deren Replikation via TCP/IP an einen weiteren Standort ist auf Grund der stetig wachsenden Anzahl der Dateien unabdingbar.
Darüber hinaus wird vor allem die Netzwerk Virtualisierung in Solaris 11 (Projekt CrossBow) im Zusammenspiel mit Solaris Containern (Zonen) den Aufbau deutlich einfacherer Testumgebungen erlauben. Mit Hilfe dieser Technologie ist es möglich, komplette Netzwerke inklusive Firewalls, Router und Switches in einer virtuellen Umgebung nachzubilden, wobei, wie bei Solaris Containern üblich, lediglich eine Betriebssystem Instanz zu warten ist.
Die Zielsetzung dieser Test- und Staging Umgebung wird die Vorbereitung einer schrittweisen Trennung der einzelnen Teil-Anwendungen wie IMAP, SMTP, Viren-Scanner usw. auf Basis von Zonen oder, wenn nötig, einzelner Server sein. Auf Grund unserer derzeitigen Performance Daten und Abschätzungen für die Zukunft wird jedoch eine Aufteilung auf mehrere Server und die damit verbundene deutlich höhere Komplexität mittelfristig nicht notwendig sein.
Des weiteren werden wir, auf Grund von Verbesserungen im Bereich des IP-Stacks und der zugehörigen Tools in Solaris 11, auch den Einsatz von IP-Multipathing erneut prüfen. Dies hatte sich in der Vergangenheit im Zusammenspiel mit der von uns eingesetzten HA-Software als zu komplex und fehleranfällig herausgestellt.

Der Lohn, Nagios Availability Report 01.01.2010 – 10.09.2011:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	618d 15h 24m 5s	99.998%	99.998%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	618d 15h 24m 5s	99.998%	99.998%
DOWN	Unscheduled	0d 0h 17m 23s	0.002%	0.002%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 17m 23s	0.002%	0.002%
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	618d 15h 41m 28s	100.000%	100.000%

Eine Ausfallzeit von weniger als 20 Minuten seit dem 1. Januar 2010 unterstreicht die Qualität des Gesamtkonzeptes, sowie insbesondere auch die seiner einzelnen technischen Komponenten mit Solaris/ZFS als Kerntechnologie.

Kontaktadresse:

Thomas Nau
Universität Ulm -kiz
Albert Einstein Allee 11
D-89081 Ulm

Telefon: +49 (0) 731 50-22464
Fax: +49 (0) 731 50-22471
E-Mail Thomas.Nau@uni-ulm.de
Internet: http://www.uni-ulm.de/einrichtungen/kiz