Einige allgemeine SysAdmin-Prinzipien

Documentation

- Dokumentieren Sie Ihre Arbeit.
  - Führen Sie ein Tagebuch.
    * Verwenden Sie mindestens eine klar Text Datei.
    * Jeden Eintag datieren.
    * Wenn Sie einen Chef haben, an den Sie Ihr Tagebuch senden, prüfen Sie die Rechtschreibung Ihres Tagebuchs.
    * Das Tagebuch ist nicht nur für Ihren Chef, es ist für Sie.
    * Es ist Ihre eigene FAQ.
    * Es ist Ihre eigene Sammlung von HOWTOs, die Ihnen und anderen dabei helfen, die Arbeit in Zukunft auf anderen Systemen zu reproduzieren.
      · Wenn Sie einen Eintrag in Ihr Tagebuch machen, fragen Sie sich: „Reichen diese Informationen aus, um es mir und vielleicht anderen zu ermöglichen, diese Arbeit zu reproduzieren, an der ich gerade Stunden gearbeitet habe?
    * Es kann mit der Zeit sehr groß werden, weshalb möglicherweise ein besseres System der Selbstdokumentation als eine klar Textdatei erforderlich ist.
      · Möglicherweise etwas Blogähnliches, wo Sie Tags zu jedem Tagebucheintrag hinzufügen können.
    * Das Journal muss gesichert und von überall aus zugänglich sein.
      · Aus diesem Grund führen einige Administratoren Protokolle in Notizbüchern (Notizbüchern aus Papier), obwohl dies mehrere Nachteile hat.
      · Wenn sich Ihr Tagebuch auf einem Firmenserver oder Ihrer Büroarbeitsstation befindet und das Netzwerk ausgefallen ist und Sie 30 Meilen entfernt zu Hause sind und einige wichtige Informationen aus dem Tagebuch benötigen . . . was nun?
  - Verwenden Sie Kommentare in /etc/config-Dateien, um Ihre Änderungen zu dokumentieren.
    * Unterzeichnen und datieren Sie Ihre Kommentare für Ihre zukünftige Referenz und für andere Administratoren.
- Seien Sie im Allgemeinen gut organisiert.
  - sei es die Verzeichnisstruktur unter Ihrem Home-Verzeichnis oder Ihr schriftliches Tagebuch.
- Verwenden Sie Technologie in der Dokumentation.
  - Richten Sie eine Webseite oder FAQ ein.
  - Verwenden Sie Video- oder Digitalfotografie.
  - Manchmal sagt ein Bild buchstäblich mehr als tausend Worte.

Die harten Sachen (Sicherheit und Backups)

- Kümmere dich zuerst um die harten (schwirigen) Sachen.
  - Die schlimmsten Gefühle für einen SysAdmin (macht Angst, gefeuert zu werden):
    * Das System wurde gehackt.
    * Etwas Wichtiges wurde gelöscht und es gibt kein Backup.
  - Backups, Sicherheitshärtung, Notfallwiederherstellungsplan.
  - Wie gut ist die Sicherung?
    * Haben Sie ein System und planen Sie eine Bare-Metal-Wiederherstellung?
    * Überprüfen Sie, ob Sie tatsächlich aus der Sicherung wiederherstellen können.
  - Führen Sie eine Dateisystemintegritätsprüfung (File System Integrity “FSI”) aus.
    * Befindet sich Ihre FSI-Datenbank und Konfigurationsdatei auf einem schreibgeschützten Medium?
    * Von schreibgeschütztem Medium oder NFS-Mount.
  - Führen Sie einen Rootkit-Scanner aus.
    * Von einem schreibgeschützten Medium oder NFS-Mount
  - Achten Sie auf kürzlich entdeckte Sicherheitsprobleme, Exploits und Vorfälle.
- Abonnieren Sie Newsgroups und Mailinglisten, die Ihnen diese Informationen liefern könnten?
- Führen Sie logwatch Logwatchoder ein anderes Programm aus, das Sie auf Unregelmäßigkeiten in Ihren Systemprotokollen hinweist.
  - Führen Sie ein Intrusion Detection System aus.
  - Verwenden Sie eine Firewall.
    * IP-Tabellen unter Linux
      · Es gibt nützliche Front-Ends und vorgefertigte Firewall-Regeln, die Sie verwenden können.

  - Whitelist eingehende Verbindungen mit tcpd (TCP-Wrapper).
  - Whitelist-Benutzer, die sich per SSH einloggen dürfen.
  - Ist es offensichtlich, welches Betriebssystem Sie ausführen, welche Server Sie ausführen?
    * Machen Sie es weniger offensichtlich.
    * Telnet-Banner, /etc/issue*, Informationen erhalten von Telnet an Port 25 (SMTP).
  - Hüten Sie sich vor der „Das wird hier nicht passieren"- oder „Unsere Benutzer sind nicht so schlauen" Mentalität, die zu Sicherheitsproblemen führt.
- Denken Sie an Redundanz.
  - Gibt es ein Backup des Backups?

Effizienz zählt

- Proxys können die Bandbreitennutzung für Installationen über das Internet und die allgemeine Internetnutzung reduzieren.
- Vermeiden Sie manuelle Masseninstallationen.
  - Versuchen Sie, so viel wie möglich Klonen zu verwenden.

Fernzugriff / Verwaltung

- Sofern nicht jeder Computer, den Sie verwalten, nur von 9 bis 17 Uhr eingeschaltet ist, ist die Systemadministration kein 9-to-5-Job.
- Die Fähigkeit, aus der Ferne zu arbeiten, ist unerlässlich und etwas, das SysAdmins fordern und einrichten sollten.
- Aktivieren Sie Wake-on-LAN und/oder zeitgesteuertes Einschalten im BIOS von Systemen.
  - Wenn Sie Eingaben in die gekauften Systeme gemacht haben, betonen Sie, dass diese Systeme mit diesen Arten von Funktionen ausgestattet sind.
- Erfahren Sie, wie Sie serielle Konsolen und Remote-KVM-Switches verwenden.
- Aktivieren Sie mehr als eine Möglichkeit für den Fernzugriff auf ein System.
  - „# ifdown eth0" beendet den Netzwerkzugriff auf Ihr System.
    * Haben Sie in diesem Fall eine andere Möglichkeit für den Zugriff auf Ihr System aktiviert?
- Lernen Sie, die Befehlszeile zu verwenden.
  - Ja, sogar unter Windows.
  - Die Fernverwaltung erfolgt am besten über die Befehlszeile.
- Erfahren Sie mehr über die SSH-Portweiterleitung.
  - Einer der wenigen Dienste/Protokolle, die vertrauenswürdig genug sind, um Firewalls zuzulassen.

Starten / Herunterfahren

- Führen Sie einige Überprüfungen durch, bevor Sie ein System herunterfahren/neu starten.
  - Ist jemand angemeldet?
  - Wie lange kann es sich leisten, das System herunterzufahren?
  - Gibt es eine Sicherung? Wird ein Backup benötigt?
  - Benötigt das System wirklich einen Neustart?
  - Ist der Bootloader richtig konfiguriert?
  - Gibt es eine alternative Möglichkeit, auf das System zuzugreifen, falls das Booten fehlschlägt?

Automatisierung und Skripterstellung

- Lernen Sie eine Skriptsprache gut und verwenden Sie sie konsequent.
  - Wenn Sie es konsequent anwenden, können Sie es gut lernen.
  - Aber keine Sprache, die so obskur ist, dass nur Sie sie verwenden und verstehen.
- Wenn Sie nicht wirklich gerne tippen, entwickeln Sie eine Reihe von Aliasen und kurzen Skripten, die das Tippen reduzieren.
- Erfahren Sie, wie Sie den Verlauf der Befehlszeile (Shell) verwenden.
  - Erhöhen Sie die Größe des Befehlsverlaufs.
- Periodische Verarbeitung (cron, at usw.)
  - Prozesse müssen nicht interaktiv sein, um geplant zu werden…
    * or learn expect or equivalent system.
  - Testen Sie das Cron-Skript wie jedes andere Skript, das Sie schreiben.
- Schreiben Sie Skripte so, dass sie skalierbar sind.

  - Wird immer noch nützlich sein, wenn mehr Systeme zu Ihrem Admin-Stall hinzugefügt werden.
  - Für jede Administrationslösung gilt: Denken Sie an Skalierbarkeit.

Softwareinstallation/-verwaltung, Systemwartung

- Workflow für die Softwareinstallation:
  - Suchen Sie nach offiziellen (z. B. Debian, Microsoft) Quellen für Software, die Sie installieren möchten.
    * Im Fall von Debian Software, die mit „apt-get, aptitude, . . . “ installiert werden kann, ohne Quellen/Spiegel von Drittanbietern hinzuzufügen.
  - Wenn keine offiziellen Quellen verfügbar sind, verwenden Sie eine empfohlene inoffizielle Quelle oder einen Mirror.
    * Stellen Sie sicher, dass Sie die „Schlüssel“ der Quelle oder des Mirrors erhalten, um sicherzustellen, dass die Software, die Sie erhalten, „signiert“ ist.
      · Installierte Pakete sollten weiterhin mit offiziellen Paketverwaltungsbefehlen (apt-get, aptitude, yum usw.) aktualisierbar/wartbar sein.
  - Wenn keine empfohlenen inoffiziellen Quellen oder Spiegel vorhanden sind, besorgen Sie sich den Quellcode, falls verfügbar, und versuchen Sie, ihn selbst zu erstellen und zu installieren.
    * Hier können Sie entweder versuchen, Ihre eigenen Installationspakete zu erstellen, oder mit Paket-„Sandboxing“-Tools wie stow/xstow installieren.
- Mehrere Paketverwaltungsschemata auf demselben System.
  - Apple, Fink und MacPorts auf MacOSX-Situation.
  - Fummeln mit $PATH und Bibliothekssuchpfaden erforderlich (Linux:/etc/ld.so.conf*).
- Nur weil ein Paket „offiziell“ ist, ist es nicht auf dem neuesten Stand (in Bezug auf Aktualität und Fehler-/Sicherheitskorrekturen).
  - Diese werden von Menschen mit echtem Leben gepflegt, und die Menschen sind oft Freiwillige, die dies in ihrer Freizeit tun.
  - Für zeitnahe Korrekturen müssen Sie möglicherweise regelmäßig manuell kompilieren/installieren/warten, anstatt sich auf das „offizielle“ Paketverwaltungssystem zu verlassen.
- Automatische Updates
  - Klingt nett, aber ein Administrator sollte wissen, was tatsächlich installiert oder aktualisiert wird.
  - Softwareinstallationen/-aktualisierungen sollten eine interaktive Aktivität sein.
    * Aber das Herunterladen (aber nicht das Installieren) von Upgrades über Nacht per Planung sollte in Ordnung sein.
- Aktualisieren Sie das Betriebssystem/den Kernel/die Software sorgfältig.
  - (oder Sicherheitspatches, Service Packs usw. anwenden)
  - Muss es jetzt gemacht werden?
    * Wird das System genutzt? Sind Benutzer angemeldet?
    * Kann es bis zum Ende des Quartals/Semesters warten?
  - Hast du das System vorher gesichert?
  - Werden Sie in der Lage sein, zu einem früheren Systemzustand zurückzukehren, wenn Ihr Upgrade katastrophal ist?
  - Haben Sie das Upgrade auf einem oder mehreren Testsystemen ausreichend getestet?
  - Haben Sie das Upgrade getestet, nachdem Sie es angewendet haben?
  - Nur die Sicherheitspatches oder -pakete mit hoher Priorität können anstelle des gesamten Pakets von Upgrades/Patches angewendet/installiert werden.
- Installieren Sie nur Software, die tatsächlich verwendet wird.
  - Unnötige Software kann Schwachstellen enthalten.
  - Aber den Benutzern Software vorzuenthalten, die sie wirklich brauchen, kann sie dazu motivieren, sie selbst in ihren Home-Verzeichnissen zu installieren.
- Nicht jede Software ist schön verpackt.
  - wie kommerzielle oder „unfreie“ Software.
    * Java von Sun, icc (Intel-Compiler), Eclipse-IDE, Netbeans-IDE, VMware.
  - Möglicherweise müssen Sie es selbst kompilieren.
    * und Installation in /usr/local oder /opt
    * Denken Sie vor der Installation über die Möglichkeit der Deinstallation nach.
      · Kompilieren und Installieren nach /usr/local bedeutet Dateien, die nach /usr/local/bin, /usr/local/lib, /usr/local/share, /usr/local/etc, /usr/local/sbin verstreut sind.
      · Hat das Makefile der Software ein funktionierendes Deinstallationsziel?

Users

- Beschreibt ihre Probleme selten mit einem Detaillierungsgrad, der zur Lösung ihrer Probleme erforderlich ist.
  - Es sollte vermieden werden, nach ihrem Passwort zu fragen, damit Sie sich als sie anmelden können, um ihre Probleme zu diagnostizieren.
    * Wenn Sie müssen, müssen sie ihr Passwort danach ändern.
  - Kann su - userid oder eine andere Methode verwenden, um einen Prozess als ein anderer Benutzer zu starten.
  - Fordern Sie einen Screenshot an.
    * Manchmal so einfach wie das Drücken der -Taste.
    * Oder mit ihren Handys.
- „Essen Sie Ihr eigenes Hundefutter."
  - Verwenden Sie dieselbe Umgebung wie die Benutzer, dieselben Computer in denselben Netzwerken wie die Benutzer, damit Sie Probleme erkennen können, mit denen sie zu Ihnen kommen.
  - Benutzer sein. Verwenden Sie Benutzertools.
    * Man kann kein UNIX-Administrator sein, ohne zuerst ein UNIX-Benutzer zu sein (gilt auch für Windows)
  - Beschäftigen Sie sich mit der Benutzerfreundlichkeit der Betriebssystemumgebung für Ihre Benutzer.
    * Dies hat den zusätzlichen Vorteil, dass Ihre Support-Kopfschmerzen reduziert werden.
    * Verwenden Sie sinnvolle Einstellungen in Standard-Shell-Profilen in /etc/skel
      · ohne die Sicherheit zu kompromitieren.
        · kein „." in $PATH, umask=077.
      · eine informative Shell-Eingabeaufforderung.
    * Wird die Standardbenutzeroberfläche (Fenstermanager oder Desktop) für CS 175-Studenten vertraut und intuitiv genug sein und auch Beschwerden von Professoren minimieren?
    * Keine Laufwerksbuchstaben und der einfache Zugriff auf USB-Sticks könnten viele Benutzer frustrieren, egal ob sie Linux-Neulinge sind oder nicht.
      · Systeme wie autofs funktionieren für Wechselmedien, obwohl ihre Einrichtung normalerweise keine leichte Aufgabe ist.
      · Balance gegen einfache Verwaltung.
        · Einfache Fenstermanager wie IceWM: schnellerer Start, geringerer Speicherbedarf, einfach zu konfigurieren (für den Administrator), vertraut aussehende Oberfläche.
        · Desktop-Umgebungen wie Gnome/KDE: langsamerer Start, größerer Speicherbedarf, einfach zu konfigurieren (für den Benutzer).
- Benutzerschulung (Training)
  - Eine Support-Webseite mit FAQs?
  - Gelegentliche „UNIX for Dummies"-Seminare?
- Gehen Sie nicht davon aus, dass die Benutzer nicht schlau genug sind oder sich der veröffentlichten Sicherheitslücken nicht bewusst sind.
  - Die „würde hier nie passieren"-Mentalität

Standardisierung vs. Vielfalt

- Auf einer Linux-Distribution standardisieren oder mehrere Distributionen verwenden?
  - Wenn Sie standardisieren, wählen Sie Ihre Standarddistribution mit Bedacht aus.
    * Betrachten Sie die prognostizierte Kontinuität einer Distribution.
      · Debians Kontinuität scheint eine gute Option zu sein.
        · weniger bei vielen Debian-Derivaten.
  - Mehrere Distributionen sind auch eine gute Idee.
    * RedHat ist immer noch die am weitesten verbreitete Distribution und rpm das am weitesten verbreitete Paketformat.
      · Es ist gut, mit RPM-basierten Distributionen und Redhat-ähnlichen Distributionen vertraut zu sein.
  - Mehrere UNIX-Versionen sind ebenfalls eine gute Idee.
    * What if, by some miracle, SCO wins and Linux is lost?
      · FreeBSD waiting in the wings.
      · Solaris x86? (future looks bleak)
      · AIX? (not free; bleh)
      · Mac OS X (see AIX)

Advocacy

- Should a UNIX admin advocate the use of UNIX?
  - Up to a point
    * An admin should advocate the right tool for the job ..
      · .. and learn the right tool for the job, even if that happens to be Windows.

Learning Administration

```
* Learn administration by doing administration.
* More likely to learn if something goes wrong.
```

Keeping up with the Joneses

```
* What technologies are being used ‘‘out there,’’ and are we behind the times?
    * LDAP instead of NIS
    * cfengine instead of my own scripts
    * systemimager instead of my own scripts
```