ITENOS
IT's us.

SERVERBETRIEB LINUX

ANLAGE

VERSION 1.0

Deutsche Telekom Gruppe

ITENOS
IT's us.

Inhaltsverzeichnis **Seite**

1 Einleitung

Dieses Dokument gibt Übersicht über die betrieblichen Anforderungen an ein Management durch ITENOS. Änderungen sind – wenn überhaupt – nur in enger Abstimmung mit ITENOS möglich.

Die Rahmenbedingungen können sich jederzeit durch neue Erkentnisse, Prozesse oder Vorgaben verändern.

Das Dokument beschreibt stets eine Momentaufnahme. Es gilt die jeweils letzte Version!

2 Allgemein

Bedingt durch die große Anzahl an Systemen kann ein Serverbetrieb nur unter konsequenter Nutzung einer automatisierten Infrastruktur erfüllt werden. Für den Bereich Linux gehört dazu sowohl die initiale Bereitstellung neuer Maschinen als auch der Betrieb und die Betreuung von laufenden Systemen.

In beiden Fällen führt dies zu Rahmenbedingen, die durch den Auftraggeber einzuhalten sind. Ein Betrieb durch ITENOS ist ansonsten nicht möglich.

Um einen gesicherten Systembetrieb zu ermöglichen, werden insbesondere sicherheitsrelevante Einstellungen zentral verwaltet.

3 Bereitstellung

Die Bereitstellung eines virtualisierten Linux-Servers erfolgt durch ein automatisches Installationsverfahren.

Im Allgemeinen können durch ITENOS keine Systeme bereitgestellt werden, die von den hier dokumentierten Einstellungen abweichen, da dies nur durch eine zeitaufwändige manuelle Installation erreicht werden kann.

Individualisierbare Parameter sind beschrieben.

3.1 Partitionierung

Während der Installation wird eine Partitionierung nach den für die ITENOS relevanten Sicherheitsvorgaben gemacht. Ohne weitere Anforderungen wird eine einzelne virtuelle Festplatte mit einer Größe von 20GB angelegt. Dies ist auch die minimale Größe, mit der wir Linux-Server betreiben können.

Alle Filesysteme des Betriebssystems werden mit dem Filesystem *ext4* erzeugt. Abgesehen von der `/boot` Partition werden alle Partitionen mit dem Logical Volume Manager (LVM) erstellt. So lassen sich im Betrieb einzelne Mountpoints vergrößern, ohne dass dafür ein Wartungsfenster erforderlich ist.

Die Installation erzeugt folgende Filesysteme:

LVM	Mountpoint	Größe	Filesystem	Mount-Parameter
vg00-root	/	3GiB	ext4	defaults
vg00-swap	swap	1GiB	swap	
vg00-tmp	/tmp	1GiB	ext4	defaults,nosuid,nodev
vg00-opt	/opt	1GiB	ext4	defaults
vg00-srv	/srv	1GiB	ext4	defaults
vg00-var	/var	5GiB	ext4	defaults
vg00-var_log	/var/log	1GiB	ext4	defaults
vg00-home	/home	1GiB	ext4	defaults,nodev

Wird in einzelnen Partitionen mehr Speicherplatz benötigt oder sollen zusätzliche Mountpoints für Anwendungsdaten genutzt werden, so sind diese Anforderungen mit der Beauftragung anzufordern.

Generell ist es aus Gründen der Abschottung zwischen Betriebssystem und Anwendung nicht zulässig, dass die Systempartitionen `/`, `/opt` und `/var` für dynamische Anwendungsdaten genutzt werden. Soll beispielsweise das DBMS MySQL in der Standardkonfiguration auf einem System laufen, so muss für die Datenspeicherung unter `/var/lib/mysql` ein eigener Mountpoint konfiguriert werden. Diese Festlegung wird durch das SDSK Req 33 begründet.

Die Vorgaben für den benötigten Festplattenspeicher verantwortet der Kunde.

3.2 Systemhärtung

Für Systeme und Anwendungen im Konzern der Deutschen Telekom ist ein Härtung entsprechend der von der GIS festgelegten Vorgaben vorgeschrieben. Für die Systeme kann dies in großen Teilen zentral über das Konfigurationsmanagement vorgenommen werden. So wird auch sichergestellt dass die Einstellungen dauerhaft erhalten bleiben, da die Automatisierung dies in regelmäßigen Abständen prüft und gegebenenfalls korrigiert.

Teilweise werden Sicherheitseinstellungen durch das Einspielen von Updates wieder zurückgenommen. Auch aus diesem Grund ist ein durchgängiger Betrieb der Automatisierung erforderlich, da nur dann gewährleistet wird, dass die Einstellungen nach Updates und Neustart wieder auf den vorgegebenen Standard geändert werden.

Die Aktivierung der Parameter gemäß den Vorgaben ist offensichtlich nur vor einer Installation und Inbetriebnahme der Anwendung sinnvoll. Auf den durch ITENOS bereitgestellten Systemen wird die Härtung daher direkt nach der Installation vorgenommen. Wurden die Systeme nicht durch ITENOS installiert und/oder die Härtung soll trotzdem später während des Wirkbetriebs durchgeführt werden, so ist mit Beeinträchtigungen zu rechnen.

4 Betrieb

Für den Betrieb durch ITENOS ist der Einsatz der Automatisierungs- und Management-Software Puppet zwingend Voraussetzung. Eine Deaktivierung von Puppet ist nicht zulässig. Die Betriebsverantwortung durch ITENOS erlischt, falls Puppet dennoch deaktiviert wird.

Generell läuft die Management-Software in regelmäßigen Intervallen (meist 30 Minuten). Die Software erkennt Unterschiede zum definierten Soll-Zustand und korrigiert diese. Unautorisierte Änderungen an den von der Software verwalteten Einstellungen werden ohne weitere Prüfung automatisch wieder auf den dokumentierten Wert zurückgesetzt. Alle Ressourcen, die von einem Kunden eigenverantwortlich kontrolliert werden sollen, können daher **nicht** durch die Automatisierung verwaltet werden, da dies früher oder später zu Problemen führt, wenn der Kunde eine Änderung durchführt. ITENOS verwaltet daher auch keine anwendungsspezifischen Konfigurationen. Ausnahmen sind die Parameter, die durch die Security vorgegeben werden und nur in Ausnahmenfällen durch Anwendungsanforderungen geändert werden dürfen. In diesen Fällen sind die Einstellungen der ITENOS anzuzeigen, diese werden dann in der Automatisierung hinterlegt.

In den meisten Fällen enthalten die zentral verwalteten Dateien einen entsprechenden Kommentar, dass diese Datei durch Puppet verwaltet wird und nicht verändert werden darf.

Als Benutzer root kann aber auch das Skript `puppet-managed-resources` aufgerufen werden, um die durch die Automatisierung verwalteten Ressourcen anzuzeigen. Die Ausgabe wird dabei konkret für das jeweilige System erstellt und enthält daher möglicherweise auch Ressourcen, die über die hier angegebene Aufstellung hinaus geht.

4.1 Hostname/FQDN

Jeder in der Automatisierung verwaltetet Server muss zwingend einen Fully Qualified Domainname (FQDN) haben. Dabei ist die Dokumentation des Kommandos hostname maßgeblich, d.h. das Kommando `hostname` muss den kurzen Hostnamen ausgeben und das Kommando `hostname -f` muss den FQDN anzeigen. Der für den lokalen Host relevante Eintrag in der Datei `/etc/hosts` darf in Bezug auf die Reihenfolge der Einträge daher nicht verändert werden. Der FQDN ist komplett in Kleinschrift anzugeben und diese Schreibweise darf nachträglich nicht verändert werden, da andere Komponenten das System über diesen Namen referenzieren. So kann bei einer unbefugten Änderung beispielsweise das Monitoring keine Messwerte/Alarme mehr ausgeben oder die unterbrochene Kerberos-Anbindung eine Benutzeranmeldung verhindern.

Die mit dem FQDN verknüpfte IP Adresse kann eine beliebige IP des Systems sein. Das Installationsverfahren nutzt per Default die Management IP, da dieses Interface auf allen Systemen verfügbar ist. Je nach Anforderung der Anwendung kann hier entweder die Management-Adresse oder eine Adresse für den Wirkbetrieb hinterlegt werden.

Zusätzliche Aliases für den FQDN Eintrag können durch den Kunden oder die ITENOS hinzugefügt werden.

4.2 Spracheinstellung über Locale

Die Systeme sind generell für die Nutzung der nachfolgenden Locales konfiguriert:

- `en_US.UTF-8`
- `en_GB.UTF-8`
- `de_DE.UTF-8`

Weitere Locales können auf Anforderung aktiviert werden.

Die Vorgabe für eine Locale (s. /etc/default/locale für Debian/Ubuntu bzw. /etc/locale.conf für RedHat/OracleLinux) ist generell leer, da diese Einstellung durch jeden Benutzer in Form von Umgebungsvariablen nach den persönlichen Wünschen gesetzt werden kann. Soll eine zentrale Einstellung für den kompletten Server genutzt werden, so kann dies angefordert werden.

4.3 Systemverzeichnisse

Von der Automatisierung werden Eigentümer und Berechtigungen diverser Systemverzeichnisse verwaltet. Ohne Anspruch auf Vollständigkeit gehören dazu:

- `/`
- `/boot`
- `/etc`
- `/etc/ssh`
- `/home`
- `/opt`
- `/root`
- `/tmp`
- `/usr`
- `/var`
- `/var/tmp`

Eigentümer, Gruppe und Berechtigungen der Verzeichnisse sind durch Sicherheitsvorgaben festgelegt und können nicht verändert werden. Diese Vorgaben sind so strikt, weil durch fehlende Leseberechtigungen eventuell eine Anmeldung nicht mehr möglich ist, während durch zusätzliche Schreibberechtigungen potentielle Sicherheitslücken entstehen.

4.4 Konfigurationsdateien des Betriebssystems

Für einige Systemdateien wird der Besitzer, die Gruppe und die Zugriffsrechte zur Gewährleistung der Sicherheitsanforderungen zentral verwaltet. So wird verhindert, dass sensible Informationen ausgelesen werden können. Dabei handelt es sich um diese Dateien:

- `/etc/group`
- `/etc/group-`
- `/etc/gshadow`
- `/etc/gshadow-`
- `/etc/passwd`
- `/etc/passwd-`
- `/etc/shadow`
- `/etc/shadow-`

4.5 DNS

Die Namensauflösung in der Datei `/etc/resolv.conf` wird zentral gesteuert. Je nach Anforderung kann neben einer internen DNS-Auflösung auch eine Namensauflösung über das Internet oder das HitNet hinterlegt werden. Dabei können bis zu drei Nameserver hinterlegt werden.

4.6 Sudo

Sudo erlaubt die Ausführung von Befehlen mit erweiterten Berechtigungen durch normale Benutzer. Daher wird auch hier die komplette Konfiguration durch eine zentrale Verwaltung übernommen. Manuelle Änderungen an der Konfiguration sind nicht möglich und zusätzliche Konfigurationseinstellungen werden durch die Automatisierung auch wieder entfernt. Kontrolliert wird der Inhalt der Datei `/etc/sudoers` sowie alle Dateien im `/etc/sudoers.d` Verzeichnis.

4.7 PAM

Über PAM (Pluggable Authentication Modules) werden die bei der Authentifizierung, dem Sessionaufbau und der Passwortänderung zu durchlaufenen Sicherheitsprüfungen konfiguriert. Dies erfolgt über eine Reihe von Dateien im `/etc/pam.d` Verzeichnis. Alle Einstellungen werden zentral verwaltet. Kundenspezifische Änderungen sind nicht vorgesehen.

4.8 Kernel Parameter

Über Kernel Parameter werden Eigenschaften des laufenden Linux-Systems kontrolliert. Die Parameter werden dazu in die beim Booten ausgelesenen Konfigurationsdatei `/etc/sysctl.conf` bzw. in Dateien im Verzeichnis `/etc/sysctl.d` hinterlegt. Die Automatisierung sorgt dafür, dass die definierten Werte regelmäßig sowohl in der jeweiligen Konfigurationsdatei als auch im laufenden System korrekt gesetzt sind. Weitere Einstellungen lassen sich in zusätzlichen Dateien unter `/etc/sysctl.d` vornehmen. Dabei ist es nicht zulässig, die hier nachfolgend genannten Einstellungen zu überschreiben.

4.8.1 Kernel

Für den Kernel sind die folgenden Werte vorgegeben:

```
fs.suid_dumpable = 0
kernel.randomize_va_space = 2
kernel.sysrq = 0
```

Weiterhin wird die Nutzung des Hauptspeichers über diesen Parameter gesteuert:

```
vm.swappiness = 10
```

Der konkrete Wert hängt von der Nutzungsart des Systems ab und kann durch den Kunden vorgegeben werden.

4.8.2 Netzwerk IPv4

Für das IPv4 Protokoll werden die nachfolgenden Einstellungen vorgenommen:

```
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.arp_announce = 2
net.ipv4.conf.all.arp_ignore = 2
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.secure_redirects = 1
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.all.shared_media = 1
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.log_martians = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.secure_redirects = 1
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.default.shared_media = 1
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.icmp_ratelimit = 100
net.ipv4.icmp_ratemask = 88089
net.ipv4.ip_forward = 0
net.ipv4.tcp_rfc1337 = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_timestamps = 0
```

Die Einstellung `net.ipv4.ip_forward=0` verhindert das Weiterleiten von Netzwerkpaketen zwischen verschiedenen Interfaces. Ein Host darf laut Security-Vorgaben nicht als Router fungieren. Diese Funktionalität muss jedoch für bestimmt Anwendungen (z.B. Docker) verfügbar sein. In diesen Fällen muss dies gesondert beauftragt werden, damit dies zentral über das Konfigurationsmanagement aktiviert werden kann.

4.8.3 Netzwerk IPv6

Für IPv6 sind die folgenden Einstellungen festgelegt:

```
net.ipv6.conf.all.accept_ra = 0
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_source_route = 0
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.all.forwarding = 0
net.ipv6.conf.default.accept_ra = 0
net.ipv6.conf.default.accept_ra_defrtr = 0
net.ipv6.conf.default.accept_ra_pinfo = 0
net.ipv6.conf.default.accept_ra_rtr_pref = 0
net.ipv6.conf.default.accept_redirects = 0
net.ipv6.conf.default.accept_source_route = 0
net.ipv6.conf.default.autoconf = 0
net.ipv6.conf.default.dad_transmits = 0
net.ipv6.conf.default.max_addresses = 1
```

```
net.ipv6.conf.default.router_solicitations = 0
```

Diese deaktivieren die Nutzung von IPv6. Falls ein System die IPv6-Anbindung benötigt, so muss dies explizit beauftragt werden.

Eine generelle Aktivierung von IPv6 kann eventuell zukünftig durch die Netzwerkinfrastruktur vorgeben werden.

4.9 Netzwerk

Netzwerkeinstellungen wie IP-Adressen und Routen dürfen ausschließlich durch ITENOS verwaltet werden. Um die Netzwerkinfrastruktur nicht zu beeinflussen, dürfen auch auf dem Host selber nur zugeteilte Netzbereiche genutzt werden (z.B. bei Verwendung von Docker).

Firewallfreischaltungen werden durch das Netzwerkteam durchgeführt und müssen gesondert beauftragt werden. Eine durchgeführte Firewallfreischaltung führt nicht automatisch zur Konfiguration einer zugehörigen Route auf den Servern. Daher muss zusätzlich zu einer eventuell notwendigen Firewallfreischaltung die Anpassung des Routing auf Client und Server beauftragt werden.

Je nach Anforderung werden die Netzwerkkonfiguration sowie die Routen durch die Automatisierung eingerichtet. In diesem Fall sind alle Änderungen ausschließlich über die zentrale Konfiguration möglich. Unautorisierte Änderungen an der Konfiguration (z.B. von Hand eingetragene Routen) werden von der Automatisierung wieder gelöscht.

Für die Konfiguration der Interfaces sowie der Routen werden die relevanten Dateien unter `/etc/sysconfig/network-scripts` (RedHat, OracleLinux) und `/etc/network` (Debian, Ubuntu) durch die Automatisierung angelegt und verändert. Weiterhin werden die Routen auch dynamisch im laufenden System hinzugefügt oder entfernt, so dass bei Änderungen am Routing kein Neustart erforderlich ist.

4.10 Benutzer & Gruppen

In der Benutzerverwaltung wird zwischen System- & Anwendungsaccounts sowie persönlichen Accounts unterschieden.

Gemäß den Sicherheitsrichtlinien wird für alle Systemaccounts außer `root` standardmäßig die Anmeldung unterbunden, die Shell auf `/usr/sbin/nologin` gesetzt und ein eventuell gesetztes Passwort gesperrt. Als Systemaccount gelten alle Accounts mit einer User-ID kleiner 999 (Debian/Ubuntu) bzw. 499 (alle übrigen Betriebssysteme). Auf Anforderung kann dies für benannte Systemaccounts unterbunden werden.

Anwendungsaccounts werden bei der Installation einer Anwendung erstellt und für den Betrieb der Anwendung genutzt. Diese Accounts sind nicht für eine direkte Anmeldung über das Netzwerk vorgesehen. Dementsprechend werden für diese Accounts auch keine SSH-Schlüssel hinterlegt. Kundenspezifische Anwendungsaccounts sind vom Kunden einzurichten. Die Nutzung dieser Accounts erfolgt durch die Anmeldung mit persönlichen Accounts und einem anschließenden Wechsel in den Anwendungsaccount mittels Sudo.

Persönlich Accounts für die interaktive Anmeldung werden durch ITENOS eingerichtet. Dabei ist bei der Beauftragung zur Dokumentation der Name sowie eine E-Mail-Adresse des Benutzers anzugeben.

Interaktive Benutzeraccounts und die für ein Dateiübertragung genutzten Accounts müssen Mitglied in einer dafür reservierten Gruppe sein, damit die Anmeldung per SSH oder SFTP erlaubt wird. Weiterhin wird für jeden Benutzer eine gleichnamige Gruppe angelegt.

Bei der Einrichtung eines lokalen Accounts wird die numerische User-ID durch das System vergeben. Im Falle einer Anbindung an ein Active Directory ist die numerische User-ID durch das AD festgelegt. Aus betrieblichen Gründen sind Wunsch-IDs nicht möglich.

Die Pflege der benutzerspezifischen Konfigurationsdateien (z.B. Shell-Profile) liegt in der Verantwortung des jeweiligen Nutzers. Eine zentrale Verteilung ist nicht vorgesehen.

4.11 Umask

Um das Einsehen sensitiver Daten durch andere Benutzer zu unterbinden, dürfen standardmäßig alle neu angelegten Dateien nur Berechtigungen für den Eigentümer bekommen. Dies wird durch den Wert des Shell-Parameters `umask` realisiert. Durch den konfigurierten Wert `077` werden zunächst für die Gruppe und alle anderen Benutzer die Rechte zum Lesen, Schreiben und Ausführen der Datei gesperrt.

Diese Einstellung wird über die zentral verwalteten Dateien `/etc/profile.d/umask.sh` sowie `/etc/login.defs` vorgenommen.

Wenn Dateien für die Gruppe oder alle anderen Benutzer zugreifbar sein soll, dann muss dies also durch den Eigentümer der Datei explizit so konfiguriert werden.

4.12 Software Repositories

Software Repositories für gängige Betriebssysteme und häufig genutzte Anwendungen werden in der Regel auf einem durch die ITENOS betriebenen Repository Server angeboten. Dabei können nur solche Repositories zentral bereitgestellt werden, die im Internet im Standardformat für das jeweilige Betriebssystem (APT oder YUM) vorliegen.

Die Konfiguration der Repositories auf einem Server geschieht ebenfalls zentral durch die Automatisierung. Manuell hinzugefügte Repositories werden durch die Automatisierung gelöscht.

Konkret werden je nach Betriebssystem die Verzeichnis und Dateien unter `/etc/apt` (Debian/Ubuntu) oder `/etc/yum.repos.d` sowie `/etc/yum.conf` (RedHat/OracleLinux) zentral verwaltet. Änderungen an diesen Dateien sind nicht zulässig.

Ausnahmen sind hierbei die Betriebssysteme von RedHat. Bedingt durch die Lizenzierung über den RedHat Subscription Manager kann ein RedHat System die Repositories des Betriebssystems ausschließlich über einen Proxy-Server ansprechen.

Generell werden alle Repositories auf dem internen Repository Server höchstens so lange gespiegelt, wie die dort verfügbare Software offiziell unterstützt wird. Es liegt in der Verantwortung des Kunden, rechtzeitig ein Update für die Softwarekomponenten vorzunehmen, bei denen das vom Anbieter dokumentierte End-of-Life bevor steht.

4.13 Softwarepakete

Die Installation von Software kann nur dann durch die ITENOS erfolgen, wenn diese im jeweiligen Standardformat des Betriebssystems (RPM oder DEB) vorliegt. Weiterhin muss die Software in einem öffentliche Repository im Internet abrufbar, so dass eine automatische Aktualisierung ermöglicht wird. In diesem Fall wird das Repository auf einem internen Server gespiegelt.

Der Kunde kann eigenverantwortlich weitere Software auf einem Server installieren, sofern es sich um Pakete aus den vorhandenen Repositories handelt (z.B. Apache, Java, MariaDB, Compiler, Tools, ...). Die Verantwortung für den Betrieb und die Konfiguration dieser Software liegt beim Kunden.

Python-Pakete können durch ITENOS nur aus den normalen Repositories des Betriebssystems installiert werden. Die Installation von Paketen mittels des Python-Paketmanagers PIP ist durch den Kunden

eigenverantwortlich vorzunehmen. Statt einer systemweiten Installation bietet das Python-Tool `virtualenv` (https://virtualenv.pypa.io/) dann genau den Vorteil, dass es Python-Pakete in anwendungsspezifischen Verzeichnissen installieren kann, ohne so dass dafür administrative Rechte nötig sind.

Liegt eine gewünschte Software in einem anderen Format (z.B. TAR) vor, so muss diese ebenfalls vom Kunden eigenverantwortlich installiert werden. Dies ist aber nur zulässig, wenn dadurch die Komponenten des Betriebssystems nicht beeinträchtigt werden. Werden auf diesem Weg beispielsweise Kommandos oder Bibliotheken installiert, so dürfen diese nicht in Systempfaden abgelegt werden. Stattdessen ist für die installierte Software ein individuelles Verzeichnis zu erstellen. Eine systemweite Anpassung des Suchpfades ist dabei nicht zulässig, um die Funktion des Betriebssystems nicht zu beeinträchtigen.

Die Verantwortung für den Betrieb selbst-installierter Software liegt ausschließlich beim Kunden.

4.14 Hosts

Die Datei `/etc/hosts` wird nicht als komplette Datei verwaltet. Stattdessen werden einzelne Einträge individuell konfiguriert. Die für den Systembetrieb durch ITENOS erforderlichen Einträge werden durch die Automatisierung erstellt und gepflegt.

Die besondere Bedeutung des Eintrags für den Host selber (FQDN) ist bereits im Abschnitt *Bereitstellung* hervorgehoben worden.

Kundenspezifische Einträge können durch den Kunden individuell erstellt und angepasst werden. Diese werden durch die Automatisierung nicht beachtet und ausschließlich durch den Kunden gepflegt. Werden durch die Automatisierung im Betrieb neue Einträge hinzugefügt (z.B. aus betrieblichen Gründen), so geschieht das am Ende der Datei. Eine Gruppierung oder Sortierung nach Kundenwunsch kann nicht realisiert werden.

Üblicherweise sind mindestens die folgenden Namen zentral konfiguriert:

- `flexera.itenos.biz`
- `izjffmsv052.itenos.biz`
- `repos.itenos.biz`
- `tos.itenos.biz`

Darüber hinaus ist der Name `localhost` und dessen IPv4 `127.0.0.1` fest vorgegeben und darf nicht verändert werden, da sich einige Dienste (z.B. Monitoring) auf diese Zuordnung verlassen. Dies entspricht dem anerkannten Standard gemäß RFC 6761.

Die Nutzung von `localhost` für eine extern erreichbare IP verbietet sich auch aus Gründen der Security, da sich Netzwerkdienste teilweise darauf verlassen, dass nur für die lokale Nutzung konfigurierte Dienste an `localhost` binden können. Ein Verstoß gegen die im Standard vorgegebene Konvention würde dazu führen, dass Netzwerkdienste fälschlicherweise von außen erreichbar sein könnten.

4.15 Kernel Parameter

Der laufende Kernel erhält beim Starten einige Parameter, damit die sicherheitsrelevanten Subsysteme frühzeitig während des Boot-Vorgangs gestartet werden. Dabei handelt es sich um die nachfolgenden Kernel-Parameter:

- `apparmor`
- `audit`
- `audit_backlog_limit`

- `security`
- `selinux`

Diese werden durch die Automatisierung gesetzt und können nicht verändert werden.

4.16 OpenSSL Schlüssel und Zertifikate

Jedes System bekommt in der Regel ein von einer internen CA der ITENOS ausgestelltes Zertifikat. Dieses Zertifikat mit dem zugehörigen Schlüssel wird unter `/etc/ssl` bzw. `/etc/pki/tls` abgelegt. Alle intern ausgestellten Zertifikate können automatisch und ohne weitere Benachrichtigung erneuert oder in der Gültigkeit verlängert werden.

Die von Anwendungen eines Kunden genutzten Zertifikate werden durch den Kunden bereitgestellt und konfiguriert.

4.17 Zeitzone

Die Zeitzone aller Server ist über die Datei `/etc/timezone` normalerweise auf *Europe/Berlin* eingestellt. Dies kann auf Wunsch geändert werden und muss dann explizit beauftrage werden, da auch diese Einstellung automatisch konfiguriert wird.

Unabhängig von der gewählten Zeitzone wird die Uhrzeit in jedem Fall über das NTP-Protokoll mit einem zentralen Zeitserver synchronisiert.

4.18 Dienste & Anwendungen

Für den normalen und sicheren Systembetrieb sind diverse Dienste erforderlich. Die Automatisierung gewährleistet die korrekte Konfiguration sowie den Start der jeweiligen Dienste.

4.18.1 AppArmor

Auf den Betriebssystemen Debian und Ubuntu wird die Sicherheitssoftware AppArmor entsprechend der Security-Vorgaben aktiviert.

Zur Konfiguration gehören die Kernel Parameter `apparmor` sowie `security`. Weiterhin werden die Pakete `apparmor` und `apparmor-utils` installiert.

4.18.2 Auditing

Zur Konformität gehört die Aktivierung und Konfiguration des Audit-Subsystems. Dazu wird das Auditing durch einen Kernel-Parameter aktiviert und der Prozess `auditd` gestartet. Alle zugehörigen Einstellungen unter `/etc/audit` werden zentral durch die Automatisierung verwaltet.

4.18.3 Job Scheduler At & Cron

Die zeitgesteuerten Job Scheduler `at` und `cron` werden auf allen Systemen installiert und automatisch gestartet.

Standardmäßig ist die Nutzung von zeitgesteuerten Jobs durch `at` oder `cron` nur für die Benutzer erlaubt, die auch eine interaktive Anmeldung per SSH Schlüssel nutzen. Zusätzliche Nutzer (z.B. Anwendungsaccounts) können auf Anforderung für die Nutzung von `at` und `cron` freigeschaltet werden.

Die erlaubten Benutzer werden über die Dateien `/etc/at.allow` und `/etc/at.deny` sowie `/etc/cron.allow` und `/etc/cron.deny` eingestellt. Diese Dateien werden durch die Automatisierung verwaltet.

Normalerweise wird bei der Ausführung eines Cronjobs eine eventuell entstehende Ausgabe als Mail an den ausführenden Benutzer gesendet. Der Kunde hat sicherzustellen, dass durch von ihm hinterlegte Jobs keine derartigen Mails an Systemaccounts (Beispiel: `root`) versendet werden. Die Ausgabe muss entweder in eine Logdatei umgeleitet oder an einen vom Kunden konfigurierte Mailadresse gesendet werden. Eventuell an Systemaccounts gesendete Mails werden durch ITENOS weder gelesen noch verarbeitet.

4.18.4 Open VM Tools

Falls ein System auf der VMware Virtualisierung läuft, so werden die zugehörigen Tools `open-vm-tools` installiert und konfiguriert. Der zugehörige Dienst `open-vm-tools` für Debian/Ubuntu beziehungsweise `vmtoolsd` für RedHat/OracleLinux wird ebenfalls gestartet.

4.18.5 SELinux

Die Betriebssysteme RedHat und OracleLinux verwenden SELinux als Sicherheitssoftware. Alle Systeme werden ohne weitere Anforderungen mit aktiviertem SELinux im Modus *permissive* bereitgestellt. Damit werden durch
SELinux keine Zugriffe blockiert. Die Konfiguration durch den Kernel Parameter selinux sowie die Konfigurationsdatei `/etc/selinux/config` wird in jedem Fall zentral gesteuert.

Die durch die Security geforderte Einstellung *enforcing* wird auf Anforderung aktiviert. In diesem Fall gewährleistet der Kunde, dass die von ihm betriebenen Anwendungen lauffähig sind. Dies gilt insbesondere, wenn die Aktivierung im Wirkbetrieb erfolgen soll.

Ebenfalls kann SELinux auf Anforderung komplett deaktiviert werden. Der Kunde nimmt in Kauf, dass das System in diesem Fall nicht den Sicherheitsrichtlinien entspricht.

Alle Änderungen erfordern einen Neustart des Rechners.

4.18.6 SNMP

Derzeit wird für die Überwachung der Systeme noch das SNMP-Protokoll genutzt. Dazu wird der zugehörige Dienst gestartet. Die Konfiguration der Dateien im Verzeichnis `/etc/snmp` wird zentral gesteuert. Diese Dateien können nicht verändert werden. Weiterhin wird ein SNMP-User mit Passwort für die Authentifizierung eingerichtet.

4.18.7 SSH

Eine fehlerhafte Konfiguration des SSH-Dienstes kann einerseits zu großen Sicherheitslücken führen und andererseits die Anmeldung am System komplett verhindern. Daher wird hierbei alle Dateien im Verzeichnis `/etc/ssh` zentral verwaltet.

Entsprechend der Vorgabe werden einige Parameter in `/etc/ssh/sshd_config` deaktiviert oder nur auf eingeschränkte Werte gesetzt. Dies betrifft beispielsweise das verwendete Protokoll, die Nutzung von Tunneln und auch die verfügbaren Algorithmen zur Verschlüsselung und Authentifizierung.

Generell gibt die Security vor, dass veraltete Algorithmen deaktiviert werden müssen. Der Kunde hat daher sicherzustellen, dass die für die Anmeldung verwendeten Clients ebenfalls den aktuellen Sicherheitsstandards entsprechen. Weiterhin ist standardmäßig nur eine Remote-Anmeldung mit einem

vom Kunden für jeden Account bereitgestellten SSH-Schlüssel vorgesehen. Die Authentifizierung mit einem Passwort ist in der Konfiguration deaktiviert. Zusätzlich müssen die Accounts für eine Anmeldung per SSH in einer dafür vorgesehenen Gruppe sein.

Weiterhin wird die Konfiguration `/etc/ssh/ssh_config` für den SSH Client ebenfalls gemäß der Sicherheitsvorgaben erstellt. Möchte ein Benutzer für die Verbindung zu einem anderen System aufgeweichte Sicherheitseinstellungen nutzen, so kann er dies durch persönliche Einstellungen für dieses eine System übersteuern. Dazu legt der Benutzer seine individuellen Einstellungen in der Datei `~/.ssh/config` ab. Ein zentrale Pflege der persönlichen Einstellungen ist nicht erforderlich und auch nicht vorgesehen.

Darüber hinaus werden alle persönlichen SSH-Schlüssel zentral verwaltet. Die üblicherweise von SSH genutzte Konfiguration `~/.ssh/authorized_keys` im Home-Directory des Benutzers ist deaktiviert. Ein Benutzer kann daher selber keine weiteren oder anderen persönlichen Keys hinterlegen. Alle Keys werden unter `/etc/keys` abgelegt und das komplette Verzeichnis wird durch Puppet verwaltet. Es können hier manuell keine Änderungen gemacht werden.

Technische Benutzer, die ausschließlich für eine Datenübertragung mit SFTP verwendet werden, müssen bei der Beantragung als solche ausgewiesen werden. So kann eine Konfiguration erstellt werden, die auch nur die Nutzung von SFTP ermöglicht und eine interaktive Anmeldung verhindert. Falls es sich um Accounts zum Datenaustausch handelt und dort regelmäßig Änderungen an den hinterlegten SSH-Keys erforderlich sind, so kann auf Wunsch eine entsprechende Konfiguration erstellt werden, womit die SSH-Schlüssel für diesen Account durch den Kunden in Eigenregie hinterlegt, geändert und gelöscht werden können.

Der SSH-Dienst ist zunächst nur auf dem Management-Interface eines Servers erreichbar. Die Anmeldung ist daher nur aus Management-Netzen möglich. Wird die Anmeldung aus Anwendungsnetzen gewünscht, muss dies gesondert eingerichtet werden.

4.18.8 Syslog

Zur Protokollierung wird der Dienst `rsyslog` genutzt. Dabei werden für das System durchgängig die folgenden Log-Dateien erstellt:

- `/var/log/auth.log`
- `/var/log/cron.log`
- `/var/log/daemon.log`
- `/var/log/kern.log`
- `/var/log/mail.log`
- `/var/log/messages`
- `/var/log/syslog`
- `/var/log/user.log`

Im Gegensatz zum Standard bei einigen Linux-Distributionen werden in `/var/log/messages` nur schwerwiegende Meldungen und in `/var/log/syslog` nur Meldungen des Syslog-Subsystems protokolliert.

Für die Konfiguration werden nochfolgende Dateien genutzt, die allesamt zentral verwaltet werden:

- `/etc/rsyslog.conf`
- `/etc/rsyslog.d/`
- `/etc/rsyslog.d/00_client.conf`
- `/etc/rsyslog.d/20-snmpd.conf`
- `/etc/rsyslog.d/50-default.conf`
- `/etc/rsyslog.d/70-remote.conf`
- `/etc/rsyslog.d/client.conf`

Änderungen an diesen Dateien sind nicht zulässig.

Die Nutzung des Syslog-Dienstes durch Anwendungen ist generell möglich. Dabei sollten bevorzugt neue Dateien erstellt werden, die eindeutig der Anwendung zugeordnet werden können. Entsprechende Regeln können in neuen Konfigurationsdateien unter `/etc/rsyslog.d` erstellt werden. Dabei sollte auch darauf geachtet werden, dass derartige Meldungen der Anwendung nicht an das zentrale Syslog-System (s. `/etc/rsyslog.d/70-remote.conf`) weitergeleitet werden. Es liegt in der Verantwortung des Kunden, dass die zusätzlichen Meldungen den Systembetrieb nicht beeinträchtigen. Dazu gehört ein regelmäßiges Rotieren der anwendungsspezifischen Logfiles als auch eine Planung und Anforderung des zusätzlich erforderlichen Plattenplatzes.

Die vom System genutzten Logfiles werden regelmäßig rotiert und komprimiert sowie nach eine festgelegten Zeit gelöscht. Dazu sind entsprechende Regeln in nachfolgenden Dateien bzw. Verzeichnissen hinterlegt:

- `/etc/logrotate.conf`
- `/etc/logrotate.d/`

4.18.9 Mail

Die Systeme werden normalerweise ohne konfiguriertes Mailsystem bereitgestellt. Ist der Mailversand erforderlich, kann durch ITENOS ein Mailsystem installiert und konfiguriert werden. Hierbei kommt ausschließlich Postfix zum Einsatz. Dabei ist weder ein externer noch ein lokaler Empfang von Mails vorgesehen, d.h. alle auf dem System erzeugten Mails werden nur weitergeleitet. Die folgenden Konfigurationsdateien werden beim Betrieb von Postfix durch ITENOS zentral verwaltet:

- `/etc/aliases`
- `/etc/mailname`
- `/etc/postfix/dh2048.pem`
- `/etc/postfix/main.cf`
- `/etc/postfix/master.cf`

Darüber hinausgehende Funktionalitäten kann der Kunde eigenverantwortlich umsetzen. In diesem Fall liegt die Konfiguration und der Betrieb des Mailsystems in der Verantwortung des Kunden.

Bei der Nutzung des Mailversands trägt der Kunde Sorge, dass nur gültige Empfänger- und Absenderadressen verwendet werden. Insbesondere sollte als Absender nur ein Mailadresse genutzt werden, die für den Mailempfang konfiguriert wurde und deren Mails gelesen werden.

Für den Mailversand ins Internet stellt ITENOS auf Wunsch den Zugang zu einem Mailrelay zur Verfügung, womit diese Dienstleistung erbracht wird.

4.18.10 Internel-Proxy

Der Zugriff auf das Internet mittels des HTTP-Protokolls muss in der Regel ein Proxy-Server genutzt werden. Dieser wird durch ITENOS konfiguriert und betrieben. Der Kunde liefert dazu eine Aufstellung, welche Domains über den Proxy angesprochen werden sollen, damit diese in der Konfiguration freigeschaltet werden können.

Da sich die Internet-Proxy-Server in der Regel in einer DMZ zwischen internen Netzen und dem Internet/Hitnet befinden, kann von dort aus Gründen der Abschottung keine Verbindung zurück in interne Netze erfolgen. Jede Anwendung, die einen Proxy nutzt, ist derart zu konfigurieren, dass alle internen Zugriffe ohne den Proxy erfolgen.

Auf Kundenwunsch können die entsprechenden Umgebungsvariablen `http_proxy` und `https_proxy` zentral konfiguriert werden. In diesem Fall wird für die Bash eine Profile-Datei hinterlegt (`/etc/profile.d/proxy.sh`), mit der die Variablen für alle interaktiven Sessions bei der Anmeldung gesetzt werden. In diesem Fall liegt es in der Verantwortung des Kunden, dass alle seine Anwendungen mit dieser Einstellung funktionieren. Generell ist es sinnvoller, wenn die Umgebungsvariablen nicht global aktiviert werden, sondern nur in der Umgebung der Anwendungen gesetzt sind, die dies erfordern.

4.18.11 Synchronisation der Uhrzeit mit NTP oder Chrony

Auf allen System ist die Synchronisation der Uhrzeit mit einer vertrauenswürdigen Quelle vorgeschrieben. Dazu wird auf jedem Rechner einer der Dienste NTP oder Chrony installiert. Die Konfiguration umfasst die Dateien `/etc/ntp.conf` und `/etc/ntp.keys` beziehungsweise `/etc/chrony.conf` und `/etc/chrony.keys`. Änderungen an diesen Dateien sind nicht zugelassen.

Die Nutzung eines Systems als Zeitquelle für andere Server ist nicht vorgesehen.

4.18.12 Datenbank Management Systeme

Datenbank Management Systeme (PostgreSQL, MySQL, Oracle) gehören nicht zum Betriebssystem und werden nicht betrieben.

Kontakt

Operation Server

servicedesk@itenos.de

0228 7293 0

Stand 06/2023