B4 - Factsheet

Autoren: Lukas Freundensprung, Abd-Sattaar Matitu, Sebastian Trostmann, Morris Tichy

Inhaltsverzeichnis

1. 4.1 Mail Services

1.1. Postfix

Postfix ist ein Mail Transfer Agent (MTA), der auf Unix-ähnlichen Betriebssystemen läuft. Er wird verwendet, um E-Mails zu empfangen, weiterzuleiten und zuzustellen. Postfix ist bekannt für seine hohe Leistung, Sicherheit und Flexibilität. Es ist eine beliebte Wahl für Server, die E-Mail-Dienste bereitstellen. Es unterstützt verschiedene Protokolle wie SMTP (Simple Mail Transfer Protocol) und kann mit anderen E-Mail-Servern kommunizieren. Postfix bietet auch Funktionen wie Spam-Filterung, Virenschutz und Unterstützung für virtuelle Domains. Es ist einfach zu konfigurieren und wird häufig in Kombination mit anderen E-Mail-Diensten wie Dovecot oder Cyrus IMAP verwendet.

1.2. Dovecot

Dovecot ist ein Open-Source-IMAP- und POP3-Server, der für Unix-ähnliche Betriebssysteme entwickelt wurde. Er wird häufig in Kombination mit Postfix verwendet, um E-Mail-Dienste bereitzustellen. Dovecot ermöglicht es Benutzern, ihre E-Mails über verschiedene Clients abzurufen und zu verwalten. Es unterstützt verschiedene Authentifizierungsmethoden und bietet Funktionen wie Maildir- und mbox-Speicherformate, SSL/TLS-Verschlüsselung und Unterstützung für virtuelle Benutzerkonten. Dovecot ist bekannt für seine hohe Leistung, Sicherheit und einfache Konfiguration.

1.3. Thunderbird

Mozilla Thunderbird ist ein Open-Source-E-Mail-Client, der von der Mozilla Foundation entwickelt wurde. Er ist für verschiedene Betriebssysteme verfügbar und bietet eine benutzerfreundliche Oberfläche zum Verwalten von E-Mails. Thunderbird unterstützt mehrere E-Mail-Konten, IMAP und POP3-Protokolle, RSS-Feeds und bietet Funktionen wie Spam-Filterung, Kalenderintegration und Erweiterungen durch Add-ons. Es ist eine beliebte Wahl für Benutzer, die einen leistungsstarken und anpassbaren E-Mail-Client suchen.

1.4. Checkliste

- ☐ Installation der erforderlichen Dienste
- ☐ Bearbeitung von Konfigurationsdateien **main.cf**
- ☐ Bearbeitung der Konfigurationsdateien **10-auth.conf**
- ☐ Bearbeitung der Konfigurationsdateien **10-mail.conf**
- ☐ Installation von Bind9

- [ ] Bearbeitung der Konfigurationsdateien **named.conf.local**
- [ ] Bearbeitung der Zonendatei **db.<domain>**
- [ ] Anlegen der User
- [ ] Installation von Thunderbird
- [ ] Konfiguration von Thunderbird
- [ ] Senden der Email

1.5. Befehlsreferenz

Command	Erklärung
`sudo apt update && sudo apt install postfix dovecot-core dovecot imapd dovecot-pop3d opendkim opendkim-tools bind9` (bash)	Installation der erforderlichen Dienste

`myhostname = mailserver.htl3rtestlab.com`
`mydomain = htl3rtestlab.com`
`myorigin = $mydomain`
`inet_interfaces = all`
`inet_protocols = ipv4`
`mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain`
`relayhost =`
`mynetworks = 127.0.0.0/8 [::1]/128 192.168.181.0/24`
`home_mailbox = maildir/`
`smtpd_banner = $myhostname ESMTP`
`local_transport = local`
`relay_domains =`
`smtpd_relay_restrictions = permit_mynetworks, reject` (bash)
	Konfiguration der main.cf Datei

`sudo systemctl restart postfix`	Neustarten des Postfix Dienstes
`auth_mechanisms = plain login` `disable_plaintext_auth = no` (bash)	Bearbeitung der Konfigurationsdateien **10-auth.conf**

Command	Erklärung
`mail_location = maildir:~/maildir`	Anpassung der Datei **10-mail.conf**
`sudo systemctl restart dovecot`	Neustarten des Dovecot Dienstes
`sudo useradd <user>`	Anlegen eines Users
`sudo mkdir /home/<user>/maildir`	Anlegen des Maildir Verzeichnisses
`sudo chown -R <user>:<user> /home/<user>/maildir`	Zuweisen der Rechte

2. 4.2 DFS

DFS ist ein verteiltes Dateisystem, welches es ermöglicht, Dateien auf mehreren Servern zu speichern und zu verwalten.

DFS Namespace:

Vereint verteilte Dateifreigaben in einer einheitlichen Ordnerstruktur, sodass Nutzer unter einem gemeinsamen Pfad auf alle Ressourcen zugreifen können.

DFS-Replikation:

Synchronisiert Dateien zwischen mehreren Servern automatisch, wodurch Ausfallsicherheit und Lastverteilung verbessert werden.

Vorteile:
- Hohe Verfügbarkeit: Daten bleiben auch bei Serverausfällen erreichbar.
- Lastverteilung: Zugriffe werden über mehrere Server verteilt.
- Zentrale Verwaltung: Einheitlicher Namespace vereinfacht die Administration.

Nachteile:
- Komplexität: Einrichtung und Verwaltung können anspruchsvoll sein.
- Replikationslatenz: Synchronisationsverzögerungen können auftreten.

- Netzwerkbelastung: Replikation erzeugt zusätzlichen Netzwerkverkehr.

2.1. Checkliste

- [ ] ADDS Domäne einrichten
- [ ] Minimum zwei Server einrichten
- [ ] File Share am ersten Server anlegen und diesen freigeben
- [ ] DFS Namespace und Replikation Rolle installieren
- [ ] DFS Namespace anlegen
- [ ] File Share mit identer Ordnerstruktur anlegen und diesen freigeben (keine Berechtigungen setzen)
- [ ] DFS Namespace und Replikation Rolle installieren
- [ ] DFS Replikation konfigurieren

3. File Service Security

3.1. AGDLP

AGDLP steht für:

A (Accounts): Die Benutzerkonten.

G (Global Groups): Diese beinhalten die Benutzerkonten und repräsentieren organisatorische Gruppen (z. B. Abteilungen).

D (Domain Local Groups): Hier werden die Global Groups zusammengefasst und für Ressourcenberechtigungen genutzt.

L/P (Permissions): Den Domain Local Groups werden dann die entsprechenden Berechtigungen auf Ressourcen zugewiesen.

Diese Vorgehensweise erleichtert das Management und die Delegation von Rechten in Active Directory, da sie eine klare Trennung zwischen Benutzergruppen und Ressourcenberechtigungen schafft.

3.2. SMBv3

SMB (Server Message Block) ist ein Netzwerkprotokoll, das es ermöglicht, Dateien, Drucker und andere Ressourcen über ein Netzwerk freizugeben. Es sorgt dafür, dass Clients auf entfernte Ressourcen zugreifen können, als wären diese lokal verfügbar.

SMBv3, eingeführt mit Windows 8 und Windows Server 2012, erweitert dieses Protokoll um wesentliche Verbesserungen:

- Erhöhte Sicherheit: SMBv3 bietet Ende-zu-Ende-Verschlüsselung, die sicherstellt, dass Daten während der Übertragung vor unbefugtem Zugriff geschützt sind.
- Leistungsoptimierung: Mit Funktionen wie SMB-Multichannel können mehrere Netzwerkverbindungen gleichzeitig genutzt werden, was die Durchsatzrate und Ausfallsicherheit erhöht.
- Effizienz in virtualisierten Umgebungen: Verbesserte Mechanismen wie SMB Direct (unterstützt RDMA) sorgen für niedrige Latenz und geringen CPU-Overhead bei der Datenübertragung, was insbesondere in virtualisierten und cloudbasierten Systemen von Vorteil ist.

3.3. Advanced Auditing

Advanced Auditing in Windows nutzt erweiterte Richtlinien (verfügbar ab Windows Vista/ Server 2008), um gezielt festzulegen, welche sicherheitsrelevanten Ereignisse protokolliert werden – etwa Anmeldeversuche, Objektzugriffe oder Änderungen an Sicherheitsrichtlinien.

Das ermöglicht Administratoren:

- Präzisere Ereignisaufzeichnung: Sie können für einzelne Ereigniskategorien Erfolg, Fehler oder beides separat aktivieren.
- Verbesserte Sicherheitsüberwachung: Ungewöhnliche oder verdächtige Aktivitäten lassen sich leichter erkennen und analysieren, was bei der Fehlersuche und Compliance hilft.
- Reduzierung von unnötigen Logeinträgen: Nur die relevanten Ereignisse werden erfasst, was die Verwaltung und Auswertung der Protokolle erleichtert.

3.4. Checkliste

- [ ] ADDS Domäne einrichten
- [ ] OU Struktur überlegen und Anlegen
- [ ] Benutzer anlegen
- [ ] Gruppen anlegen
- [ ] Benutzer zu Gruppen hinzufügen
- [ ] File Share anlegen und diesen freigeben

- [ ] Berechtigungen für den File Share setzen
- [ ] SMBv3 aktivieren
- [ ] SMBv3 Verschlüsselung aktivieren
- [ ] GPO für Advanced Auditing anlegen
- [ ] GPO anwenden

4. Remote Desktop Services

Remote Desktop Services (RDS) ist eine Microsoft-Technologie zur zentralisierten Bereitstellung von Desktops und Anwendungen. Benutzer greifen über eine Remotesitzung auf Ressourcen zu, wodurch Hardwareanforderungen auf der Client-Seite sinken und zentrale Verwaltung möglich wird.

4.1. Komponenten

Remote Desktop Session Host (RDSH)
- Führt Benutzer-Desktops oder Remote-Apps aus.
- Benutzer verbinden sich per RDP mit dem RDSH.
- Jeder Benutzer bekommt eine eigene Sitzung auf demselben Server.

Remote Desktop Connection Broker (RDCB)
- Verteilt und verwaltet Sitzungen zwischen RDSH-Servern.
- Unterstützt Lastverteilung und Sitzungswiederaufnahme (Session Reconnect).
- Speichert Infos über aktive Sessions in einer SQL-Datenbank.

Remote Desktop Licensing (RDLS)
- Lizenzierungsdienst für den RDS-Zugriff.
- Erforderlich für den produktiven Einsatz.
- Vergibt CALs (Client Access Licenses) an Benutzer oder Geräte.

Remote Desktop Gateway (RDGW)
- Bietet sicheren HTTPS-Zugriff von außen.
- Ermöglicht RDP-Zugriff über das Internet (statt direkt über Port 3389).
- Nutzt TLS und Policies für Zugriffskontrolle.

Remote Desktop Web Access (RDWeb)
- Webinterface zur Bereitstellung von RemoteApps oder Desktops.

- Benutzer melden sich per Browser an und sehen nur ihre Anwendungen.

4.2. Checkliste

4.2.1. session-based RDS

- [ ] Remote Desktop Service Feature installieren
- [ ] alle RDS Server im Installationsprozess auswählen
- [ ] RD Licensing Server hinzufügen
- [ ] RD Licensing Server konfigurieren
- [ ] RDS-Gateway konfigurieren
- [ ] Zertifikat-Template für RD Gateway & Connection Broker erstellen (auf CA)
- [ ] Zertifikate für RD Gateway & Connection Broker konfigurieren (auf RDCB-LS)
- [ ] SSL-Zertifikat für WebAccess konfigurieren
- [ ] RD Licensing konfigurieren
- [ ] WebAccess HTTP redirect erstellen

4.2.2. Session Collections

- [ ] RDS Users & Groups erstellen
- [ ] DFS Share für User Profiles erstellen (auf FileServer)
- [ ] Session Collection erstellen (auf RDCB-LS)
- [ ] Session Collection konfigurieren
- [ ] Adresse des RD Gateway aufrufen und mit Credentials anmelden
- [ ] File herunterladen
- [ ] RDP Session starten

5. Ceph

5.1. Ceph Überblick

Ceph ist eine Open-Source-Software-definierte Speicherlösung, die entwickelt wurde, um die Anforderungen moderner Unternehmen an Block-, Datei- und Objektspeicher zu erfüllen. Dank ihrer hoch skalierbaren Architektur wird sie zunehmend als Standard für wachstumsstarke Blockspeicher, Objektspeicher und Data Lakes eingesetzt. Ceph ermöglicht es, Daten von physischer Speicherhardware zu entkoppeln, was beispiellose Skalierungs- und Fehlermanagementfähigkeiten bietet. Dies macht Ceph ideal für Cloud-Umgebungen, OpenStack, Kubernetes und andere mikroservice- und containerbasierte Workloads, da es effektiv große Datenvolumen speichern kann.

Ceph speichert Daten als Objekte innerhalb logischer Speicherpools. Ein Cluster kann mehrere Pools haben, die jeweils auf unterschiedliche Leistungs- oder Kapazitätsanforderungen abgestimmt sind. Um Skalierung, Lastverteilung und Wiederherstellung effizient zu handhaben, teilt Ceph die Pools in Platzierungsgruppen (Placement Groups, PGs) auf. Der CRUSH-Algorithmus bestimmt die Platzierungsgruppe für das Speichern eines Objekts und berechnet anschließend, welche OSDs die Platzierungsgruppe speichern sollen.

Zu den Hauptmerkmalen von Ceph gehören:
- Dünn provisionierter Blockspeicher zur Optimierung der Speichernutzung
- Teilweises oder vollständiges Lesen und Schreiben sowie atomare Transaktionen
- Replikation und Erasure Coding zum Datenschutz
- Unterstützung von Snapshots, Klonen und Layering
- POSIX-Dateisystem-Semantik
- Key-Value-Zuordnungen auf Objektebene
- Kompatibilität mit Swift- und AWS S3-Objekt-APIs

Zahlreiche Unternehmen aus verschiedenen Branchen, darunter CERN, Deutsche Telekom, Bloomberg, Cisco, DreamHost und DigitalOcean, nutzen Ceph aufgrund seiner Flexibilität, Skalierbarkeit und Robustheit.

5.2. Ceph Komponenten

5.2.1. Storage Interfaces

Ceph stellt mehrere Wege zum Speichern der Daten bereit. Diese sind: CephFS (ein Filesystem), RBD (block Geräte), RADOS (Objekt Speicher). Alle diese basieren aber eigentlich auf RADOS. Die anderen geben sich nur als Filesystem oder Block Geräte aus.

5.2.2. Daemon Typen

Ein Ceph-Speichercluster besteht aus mehreren Daemon-Typen:
- Cluster-Monitore (ceph-mon): Verwalten den Zustand des Clusters, verfolgen aktive und ausgefallene Knoten, die Cluster-Konfiguration und Informationen über die Datenplatzierung.
- Manager (ceph-mgr): Behalten Laufzeitmetriken des Clusters bei, ermöglichen Dashboard-Funktionen und bieten Schnittstellen zu externen Überwachungssystemen.
- Objektspeichergeräte (ceph-osd): Ein Prozess der auf einem Storage Server rennt und für die Verwaltung eines einzigen Speichers ist. Z.B. eine einzige Disk.

- RADOS Gateways (ceph-rgw): Bieten Objekt-Speicher-APIs (Swift und S3) über HTTP/HTTPS an.
- Metadaten-Server (ceph-mds): Speichern Metadaten für das Ceph-Dateisystem und ermöglichen die Nutzung von POSIX-Semantiken für den Dateizugriff.
- iSCSI Gateways (ceph-iscsi): Stellen iSCSI-Ziele für traditionelle Blockspeicher-Workloads wie VMware oder Windows Server bereit.

5.2.3. Pools

Ein Pool ist eine Abstraktion, die entweder als „repliziert“ oder „erasure coded“ (also fehlerkorrigierend) ausgelegt werden kann. In Ceph wird die Methode des Datenschutzes auf Pool-Ebene festgelegt. Ceph bietet und unterstützt zwei Arten des Datenschutzes: Replikation und Erasure Coding. Objekte werden in Pools gespeichert. Ein Speicherpool ist eine Sammlung von Speichervolumen. Ein Speichervolumen ist die grundlegende Speichereinheit, beispielsweise zugewiesener Speicherplatz auf einer Festplatte oder eine einzelne Bandkassette. Der Server nutzt diese Speichervolumen, um gesicherte, archivierte oder platzverwaltete Dateien zu speichern. Placement Groups sind Teile der Pools

5.3. Checklisten

- [ ] cephadm-Skript herunterladen
- [ ] Skript ausführbar machen und cephadm installieren
- [ ] Mit cephadm ceph-common installieren
- [ ] Monitor-Node-Konfiguration in /etc/ceph/ceph.conf anlegen und Keyrings erstellen
- [ ] Monitor-Node „bootstrappen“
- [ ] Credentials abrufen und am Web-UI einloggen
- [ ] SSH-Key (/etc/ceph/ceph.pub) auf die OSD-Nodes in .ssh/authorized_keys kopieren
- [ ] OSD-Nodes einbinden
- [ ] Labels für OSD-Nodes setzen
- [ ] OSDs mit Festplatten erstellen
- [ ] Die Keyrings auf die OSD-Nodes kopieren
- [ ] Das SD-Pool erstellen
- [ ] Filesystem kreieren
- [ ] Filesystem durch ceph-fuse einbinden