Absichern eines Samba-Fileservers in einem Active Directory

Stefan Kania

7. Mai 2018

Distribution

Vorüberlegungen zur Distribution

Distribution

Vorüberlegungen zur Distribution

- Auswahl der Distribution

Distribution

Vorüberlegungen zur Distribution

- Auswahl der Distribution
  - Einheitliche Distributionen im Unternehmen

Distribution

Vorüberlegungen zur Distribution

- Auswahl der Distribution
  - Einheitliche Distributionen im Unternehmen
  - LTS-Versionen

Distribution

Vorüberlegungen zur Distribution

- Auswahl der Distribution
  - Einheitliche Distributionen im Unternehmen
  - LTS-Versionen
  - Pflege der Samba-Pakete

Distribution

Vorüberlegungen zur Distribution

- Auswahl der Distribution
  - Einheitliche Distributionen im Unternehmen
  - LTS-Versionen
  - Pflege der Samba-Pakete
- Einheitliche Paketquellen

Distribution

Vorüberlegungen zur Distribution

- Auswahl der Distribution
  - Einheitliche Distributionen im Unternehmen
  - LTS-Versionen
  - Pflege der Samba-Pakete
- Einheitliche Paketquellen
  - Selber bauen

Distribution

Vorüberlegungen zur Distribution

- Auswahl der Distribution
  - Einheitliche Distributionen im Unternehmen
  - LTS-Versionen
  - Pflege der Samba-Pakete
- Einheitliche Paketquellen
  - Selber bauen
  - Aus der Distribution

Distribution

Vorüberlegungen zur Distribution

- Auswahl der Distribution
  - Einheitliche Distributionen im Unternehmen
  - LTS-Versionen
  - Pflege der Samba-Pakete
- Einheitliche Paketquellen
  - Selber bauen
  - Aus der Distribution
  - SerNet Pakete

Systemsicherheit

Installation und Konfiguration des Systems

Systemsicherheit

Installation und Konfiguration des Systems

- Keine grafische Oberfläche

Systemsicherheit

Installation und Konfiguration des Systems

- Keine grafische Oberfläche
- Nur benötigte Pakete installieren

Systemsicherheit

Installation und Konfiguration des Systems

- Keine grafische Oberfläche
- Nur benötigte Pakete installieren
- Partitionierung

Systemsicherheit

Installation und Konfiguration des Systems

- Keine grafische Oberfläche
- Nur benötigte Pakete installieren
- Partitionierung
  - root-Partiton (rw)

Systemsicherheit

Installation und Konfiguration des Systems

- Keine grafische Oberfläche
- Nur benötigte Pakete installieren
- Partitionierung
  - root-Partiton (rw)
  - /boot (ro)

Systemsicherheit

Installation und Konfiguration des Systems

- Keine grafische Oberfläche
- Nur benötigte Pakete installieren
- Partitionierung
  - root-Partiton (rw)
  - /boot (ro)
  - /usr (ro)

Systemsicherheit

Installation und Konfiguration des Systems

- Keine grafische Oberfläche
- Nur benötigte Pakete installieren
- Partitionierung
  - root-Partiton (rw)
  - /boot (ro)
  - /usr (ro)
  - /var (rw)

Systemsicherheit

Installation und Konfiguration des Systems

- Keine grafische Oberfläche
- Nur benötigte Pakete installieren
- Partitionierung
  - root-Partiton (rw)
  - /boot (ro)
  - /usr (ro)
  - /var (rw)
  - /tmp (rw,noexec)

Systemsicherheit

Installation und Konfiguration des Systems

- Keine grafische Oberfläche
- Nur benötigte Pakete installieren
- Partitionierung
  - root-Partiton (rw)
  - /boot (ro)
  - /usr (ro)
  - /var (rw)
  - /tmp (rw,noexec)
  - /daten (rw,noexec)

Systemsicherheit

Installation und Konfiguration des Systems

- Keine grafische Oberfläche
- Nur benötigte Pakete installieren
- Partitionierung
  - root-Partiton (rw)
  - /boot (ro)
  - /usr (ro)
  - /var (rw)
  - /tmp (rw,noexec)
  - /daten (rw,noexec)
- Nur benötigte Netzwerkprotokolle

Systemsicherheit

Installation und Konfiguration des Systems

- Keine grafische Oberfläche
- Nur benötigte Pakete installieren
- Partitionierung
  - root-Partiton (rw)
  - /boot (ro)
  - /usr (ro)
  - /var (rw)
  - /tmp (rw,noexec)
  - /daten (rw,noexec)
- Nur benötigte Netzwerkprotokolle
- Nur benötigte Dienste (ein Server, ein Dienst)

Samba-Einrichten

Grundeinstellung der smb.conf

Samba-Einrichten

Grundeinstellung der smb.conf

- deaktivieren von NetBIOS

Samba-Einrichten

Grundeinstellung der smb.conf

- deaktivieren von NetBIOS
- client ipc min protocol = smb2_10

Samba-Einrichten

Grundeinstellung der smb.conf

- deaktivieren von NetBIOS
- client ipc min protocol = smb2_10
- client min protocol = smb2_10

Samba-Einrichten

Grundeinstellung der smb.conf

- deaktivieren von NetBIOS
- client ipc min protocol = smb2_10
- client min protocol = smb2_10
- disable netbios = yes

Samba-Einrichten

Grundeinstellung der smb.conf

- deaktivieren von NetBIOS
- client ipc min protocol = smb2_10
- client min protocol = smb2_10
- disable netbios = yes
- smb ports = 445

Einrichten Admin-share

Nur Admins haben Zutritt

Einrichten Admin-share

Nur Admins haben Zutritt

- path = /data/admin-share

Einrichten Admin-share

Nur Admins haben Zutritt

- path = /data/admin-share
- browsable = no

Einrichten Admin-share

Nur Admins haben Zutritt

- path = /data/admin-share
- browsable = no
- read only = no

Einrichten Admin-share

Nur Admins haben Zutritt

- path = /data/admin-share
- browsable = no
- read only = no
- administrative share = yes

Einrichten Freigabe für Anwender

Mit Audit

Einrichten Freigabe für Anwender

Mit Audit

- path = /data/admin-share/Abteilungen

Einrichten Freigabe für Anwender

Mit Audit

- path = /data/admin-share/Abteilungen
- browsable = no

Einrichten Freigabe für Anwender

Mit Audit

- path = /data/admin-share/Abteilungen
- browsable = no
- read only = no

Einrichten Freigabe für Anwender

Mit Audit

- path = /data/admin-share/Abteilungen
- browsable = no
- read only = no
- hide unreadable = yes

Einrichten Freigabe für Anwender

Mit Audit

- path = /data/admin-share/Abteilungen
- browsable = no
- read only = no
- hide unreadable = yes
- vfs objects = full_audit

Einrichten Freigabe für Anwender

Mit Audit

- path = /data/admin-share/Abteilungen
- browsable = no
- read only = no
- hide unreadable = yes
- vfs objects = full_audit
- full_audit:success = mkdir rmdir read pread write pwrite rename unlink connect

Einrichten Freigabe für Anwender

Mit Audit

- path = /data/admin-share/Abteilungen
- browsable = no
- read only = no
- hide unreadable = yes
- vfs objects = full_audit
- full_audit:success = mkdir rmdir read pread write pwrite rename unlink connect
- full_audit:prefix = %u|%I|%m|%S

Einrichten Freigabe für Anwender

Mit Audit

- path = /data/admin-share/Abteilungen
- browsable = no
- read only = no
- hide unreadable = yes
- vfs objects = full_audit
- full_audit:success = mkdir rmdir read pread write pwrite rename unlink connect
- full_audit:prefix = %u|%I|%m|%S
- full_audit:failure = none

Einrichten Freigabe für Anwender

Mit Audit

- path = /data/admin-share/Abteilungen
- browsable = no
- read only = no
- hide unreadable = yes
- vfs objects = full_audit
- full_audit:success = mkdir rmdir read pread write pwrite rename unlink connect
- full_audit:prefix = %u|%I|%m|%S
- full_audit:failure = none
- full_audit:facility = local5

Einrichten Freigabe für Anwender

Mit Audit

- path = /data/admin-share/Abteilungen
- browsable = no
- read only = no
- hide unreadable = yes
- vfs objects = full_audit
- full_audit:success = mkdir rmdir read pread write pwrite rename unlink connect
- full_audit:prefix = %u|%I|%m|%S
- full_audit:failure = none
- full_audit:facility = local5
- full_audit:priority = notice

Die Firewall

Zutrittskontrolle für alle

Die Firewall

Zutrittskontrolle für alle

- Erst mal alles Verbieten

Die Firewall

Zutrittskontrolle für alle

- Erst mal alles Verbieten
- OUTPUT für alle Ports

Die Firewall

Zutrittskontrolle für alle

- Erst mal alles Verbieten
- OUTPUT für alle Ports
- ssh öffnen

Die Firewall

Zutrittskontrolle für alle

- Erst mal alles Verbieten
- OUTPUT für alle Ports
- ssh öffnen
- Port 445 für smb öffnen

Die Firewall

Zutrittskontrolle für alle

- Erst mal alles Verbieten
- OUTPUT für alle Ports
- ssh öffnen
- Port 445 für smb öffnen
- Schutz gegen ssh-Angriffe

Die Firewall

Zutrittskontrolle für alle

- Erst mal alles Verbieten
- OUTPUT für alle Ports
- ssh öffnen
- Port 445 für smb öffnen
- Schutz gegen ssh-Angriffe
- Einfacher Schutz gegen Portscanner

Testen Testen Testen

Überprüfen der Sicherheit

Testen Testen Testen

Überprüfen der Sicherheit

- Regelmäßige Tests

Testen Testen Testen

Überprüfen der Sicherheit

- Regelmäßige Tests
- Testen mit Nmap

Testen Testen Testen

Überprüfen der Sicherheit

- Regelmäßige Tests
- Testen mit Nmap
- Aktualität der Paket prüfen

Testen Testen Testen

Überprüfen der Sicherheit

- Regelmäßige Tests
- Testen mit Nmap
- Aktualität der Paket prüfen
- Andere prüfen lassen