Disaster Recovery einer Samba4 Active Directory Domäne

Stefan Kania

SLAC 2024

6. Mai 2024

Stefan Kania
IT-Consulting durch Training

Brauche wir einen Plan zur Wiederherstellung der Domäne?

Brauche wir einen Plan zur Wiederherstellung der Domäne?

- Warum, wir haben doch mehrere DC an unterschiedlichen Standorten

Brauche wir einen Plan zur Wiederherstellung der Domäne?

- Warum, wir haben doch mehrere DC an unterschiedlichen Standorten
- Wir sichern doch immer alle VMs

Brauche wir einen Plan zur Wiederherstellung der Domäne?

- Warum, wir haben doch mehrere DC an unterschiedlichen Standorten
- Wir sichern doch immer alle VMs
- Die Domäne ist noch nie ausgefallen

Brauche wir einen Plan zur Wiederherstellung der Domäne?

- Warum, wir haben doch mehrere DC an unterschiedlichen Standorten
- Wir sichern doch immer alle VMs
- Die Domäne ist noch nie ausgefallen
- Wenn es doch passiert, bekommen wir das schon irgendwie hin

Brauche wir einen Plan zur Wiederherstellung der Domäne?

- Warum, wir haben doch mehrere DC an unterschiedlichen Standorten
- Wir sichern doch immer alle VMs
- Die Domäne ist noch nie ausgefallen
- Wenn es doch passiert, bekommen wir das schon irgendwie hin
- Der Aufwand, das immer wieder zu testen ist zu hoch

Ja, wir brauchen einen Plan!

Ja, wir brauchen einen Plan!

- Irgendwann wird der Ausfall kommen

Ja, wir brauchen einen Plan!

- Irgendwann wird der Ausfall kommen
- Dann ist eine schnelle Reaktion nötig

Ja, wir brauchen einen Plan!

- Irgendwann wird der Ausfall kommen
- Dann ist eine schnelle Reaktion nötig
- Nur wiederholte Tests des Recoveries schafft Sicherheit

Ja, wir brauchen einen Plan!

- Irgendwann wird der Ausfall kommen
- Dann ist eine schnelle Reaktion nötig
- Nur wiederholte Tests des Recoveries schafft Sicherheit
- Der Zeitaufwand ist gering

Ja, wir brauchen einen Plan!

- Irgendwann wird der Ausfall kommen
- Dann ist eine schnelle Reaktion nötig
- Nur wiederholte Tests des Recoveries schafft Sicherheit
- Der Zeitaufwand ist gering
- Im Ernstfall kann schnell und effizient gehandelt werden

Welche Möglichkeiten gab es und gibt es heute

Welche Möglichkeiten gab es und gibt es heute

- Bis Samba 4.9 Backup nur über ein Shell-Skript

Welche Möglichkeiten gab es und gibt es heute

- Bis Samba 4.9 Backup nur über ein Shell-Skript
- Ab 4.10 Online Backup mit samba-tool

Welche Möglichkeiten gab es und gibt es heute

- Bis Samba 4.9 Backup nur über ein Shell-Skript
- Ab 4.10 Online Backup mit samba-tool
- Seit Samba 4.15 Offline Backup

Online Backup

Online Backup

- Alle Datenbanken werden gesichert

Online Backup

- Alle Datenbanken werden gesichert
- GPOs werden gesichert

Online Backup

- Alle Datenbanken werden gesichert
- GPOs werden gesichert
- SYSVOL und smb.conf werden gesichert

Online Backup

- Alle Datenbanken werden gesichert
- GPOs werden gesichert
- SYSVOL und smb.conf werden gesichert
- Der Vorgang läuft ähnlich wie ein Join eines neuen DCs

Online Backup

- Alle Datenbanken werden gesichert
- GPOs werden gesichert
- SYSVOL und smb.conf werden gesichert
- Der Vorgang läuft ähnlich wie ein Join eines neuen DCs
- Ein Authentifizierung ist notwendig

Online Backup

- Alle Datenbanken werden gesichert
- GPOs werden gesichert
- SYSVOL und smb.conf werden gesichert
- Der Vorgang läuft ähnlich wie ein Join eines neuen DCs
- Ein Authentifizierung ist notwendig
- Eine Sicherung über das Netzwerk ist möglich

Online Backup

- Alle Datenbanken werden gesichert
- GPOs werden gesichert
- SYSVOL und smb.conf werden gesichert
- Der Vorgang läuft ähnlich wie ein Join eines neuen DCs
- Ein Authentifizierung ist notwendig
- Eine Sicherung über das Netzwerk ist möglich
- Alle Dienste des Domaincontroller müssen laufen

Offline Backup

Offline Backup

- Alle Datenbanken werden gesichert

Offline Backup

- Alle Datenbanken werden gesichert
- GPOs werden gesichert

Offline Backup

- Alle Datenbanken werden gesichert
- GPOs werden gesichert
- SYSVOL und smb.conf werden gesichert

Offline Backup

- Alle Datenbanken werden gesichert
- GPOs werden gesichert
- SYSVOL und smb.conf werden gesichert
- Zusätzliche Debug-Informationen werden gesichert

Offline Backup

- Alle Datenbanken werden gesichert
- GPOs werden gesichert
- SYSVOL und smb.conf werden gesichert
- Zusätzliche Debug-Informationen werden gesichert
- Keine Sicherung über das Netz möglich

Offline Backup

- Alle Datenbanken werden gesichert
- GPOs werden gesichert
- SYSVOL und smb.conf werden gesichert
- Zusätzliche Debug-Informationen werden gesichert
- Keine Sicherung über das Netz möglich
- Keine Authentifizierung nötig

Offline Backup

- Alle Datenbanken werden gesichert
- GPOs werden gesichert
- SYSVOL und smb.conf werden gesichert
- Zusätzliche Debug-Informationen werden gesichert
- Keine Sicherung über das Netz möglich
- Keine Authentifizierung nötig
- Nur als Benutzer root möglich

Offline Backup

- Alle Datenbanken werden gesichert
- GPOs werden gesichert
- SYSVOL und smb.conf werden gesichert
- Zusätzliche Debug-Informationen werden gesichert
- Keine Sicherung über das Netz möglich
- Keine Authentifizierung nötig
- Nur als Benutzer root möglich
- Die Samba-Dienste müssen nicht laufen

Regeln für das Backup

Regeln für das Backup

- Niemals wird ein Backup des ADs eingespielt solange noch ein DC funktioniert

Regeln für das Backup

- Niemals wird ein Backup des ADs eingespielt solange noch ein DC funktioniert
- Das Sichern einer VM ist kein AD-Backup

Regeln für das Backup

- Niemals wird ein Backup des ADs eingespielt solange noch ein DC funktioniert
- Das Sichern einer VM ist kein AD-Backup
- Die Datei des Backups darf nicht auf dem DC gespeichert werden

Regeln für das Backup

- Niemals wird ein Backup des ADs eingespielt solange noch ein DC funktioniert
- Das Sichern einer VM ist kein AD-Backup
- Die Datei des Backups darf nicht auf dem DC gespeichert werden
- Jeder, der die Backupdatei in die Hand bekommt, kann das AD wiederherstellen, inklusive aller Passwörter

Regeln für das Backup

- Niemals wird ein Backup des ADs eingespielt solange noch ein DC funktioniert
- Das Sichern einer VM ist kein AD-Backup
- Die Datei des Backups darf nicht auf dem DC gespeichert werden
- Jeder, der die Backupdatei in die Hand bekommt, kann das AD wiederherstellen, inklusive aller Passwörter
- Ein offline Backup kann auch per Skript durchgeführt werden

Regeln für das Backup

- Niemals wird ein Backup des ADs eingespielt solange noch ein DC funktioniert
- Das Sichern einer VM ist kein AD-Backup
- Die Datei des Backups darf nicht auf dem DC gespeichert werden
- Jeder, der die Backupdatei in die Hand bekommt, kann das AD wiederherstellen, inklusive aller Passwörter
- Ein offline Backup kann auch per Skript durchgeführt werden
- Wird Bind9 als DNS-Server eingesetzt, sind zusätzlich die Konfigurationsdateien des Bind9 zu sichern

Regeln für das Recovery

Regeln für das Recovery

- Niemals wird ein Backup des ADs eingespielt solange noch ein DC funktioniert

Regeln für das Recovery

- Niemals wird ein Backup des ADs eingespielt solange noch ein DC funktioniert
- Verwenden Sie möglichst immer die selbe Distribution

Regeln für das Recovery

- Niemals wird ein Backup des ADs eingespielt solange noch ein DC funktioniert
- Verwenden Sie möglichst immer die selbe Distribution
- Verwenden Sie immer die selbe Samba-Version

Regeln für das Recovery

- Niemals wird ein Backup des ADs eingespielt solange noch ein DC funktioniert
- Verwenden Sie möglichst immer die selbe Distribution
- Verwenden Sie immer die selbe Samba-Version
- Löschen Sie alle Daten aus /var/lib/samba, aber NICHT das Verzeichnis selber

Regeln für das Recovery

- Niemals wird ein Backup des ADs eingespielt solange noch ein DC funktioniert
- Verwenden Sie möglichst immer die selbe Distribution
- Verwenden Sie immer die selbe Samba-Version
- Löschen Sie alle Daten aus /var/lib/samba, aber NICHT das Verzeichnis selber
- Löschen Sie eine eventuell vorhandene smb.conf

Regeln für das Recovery

- Niemals wird ein Backup des ADs eingespielt solange noch ein DC funktioniert
- Verwenden Sie möglichst immer die selbe Distribution
- Verwenden Sie immer die selbe Samba-Version
- Löschen Sie alle Daten aus /var/lib/samba, aber NICHT das Verzeichnis selber
- Löschen Sie eine eventuell vorhandene smb.conf
- Spielen Sie das Backup ein

Regeln für das Recovery

- Niemals wird ein Backup des ADs eingespielt solange noch ein DC funktioniert
- Verwenden Sie möglichst immer die selbe Distribution
- Verwenden Sie immer die selbe Samba-Version
- Löschen Sie alle Daten aus /var/lib/samba, aber NICHT das Verzeichnis selber
- Löschen Sie eine eventuell vorhandene smb.conf
- Spielen Sie das Backup ein
- Passen Sie die neue smb.conf an, ändern Sie aber auf gar keine Fall die dort eingetragenen Pfade

Regeln für das Recovery

- Niemals wird ein Backup des ADs eingespielt solange noch ein DC funktioniert
- Verwenden Sie möglichst immer die selbe Distribution
- Verwenden Sie immer die selbe Samba-Version
- Löschen Sie alle Daten aus /var/lib/samba, aber NICHT das Verzeichnis selber
- Löschen Sie eine eventuell vorhandene smb.conf
- Spielen Sie das Backup ein
- Passen Sie die neue smb.conf an, ändern Sie aber auf gar keine Fall die dort eingetragenen Pfade
- Stellen Sie die Rechte der Freigabe SYSVOL wieder her

Wenn Bind9 zum Einsatz kommt

Wenn Bind9 zum Einsatz kommt

- Nach dem Recovery erst auf den internen DNS-Server umstellen

Wenn Bind9 zum Einsatz kommt

- Nach dem Recovery erst auf den internen DNS-Server umstellen
- NS-Einträge für Reverse-Zonen wiederherstellen

Wenn Bind9 zum Einsatz kommt

- Nach dem Recovery erst auf den internen DNS-Server umstellen
- NS-Einträge für Reverse-Zonen wiederherstellen
- Prüfen Sie die Rechte an /var/lib/samba

Wenn Bind9 zum Einsatz kommt

- Nach dem Recovery erst auf den internen DNS-Server umstellen
- NS-Einträge für Reverse-Zonen wiederherstellen
- Prüfen Sie die Rechte an /var/lib/samba
- Stellen Sie wieder auf den Bind9 um

Was noch zu tun bleibt

Was noch zu tun bleibt

- Einbinden der ursprünglichen Domaincontroller

Was noch zu tun bleibt

- Einbinden der ursprünglichen Domaincontroller
- Übernahme der FSMO-Rollen

Was noch zu tun bleibt

- Einbinden der ursprünglichen Domaincontroller
- Übernahme der FSMO-Rollen
- Entfernen des Revovery-Domaincontrollers

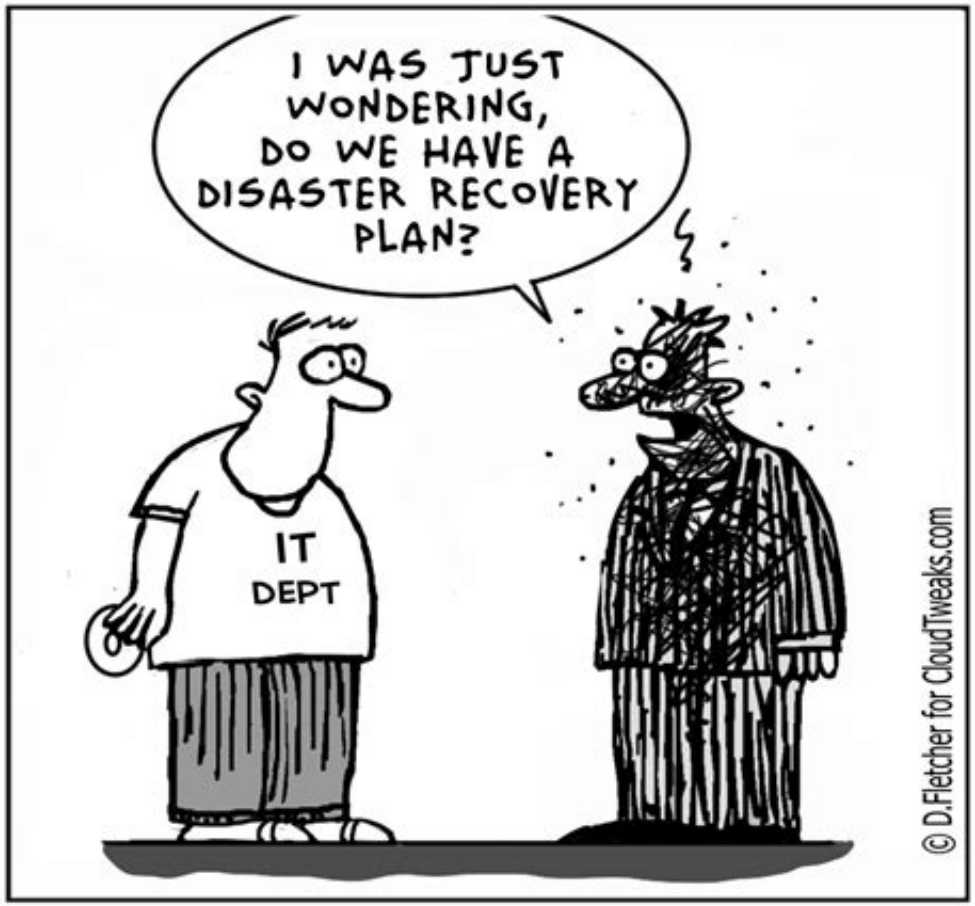

Abbildung: And now the practical part