

AD Services Screening-Check

EFFIZIENT UND ÜBERSICHTLICH

Wir führen für Sie im Vorfeld von geplanten Infrastrukturänderungen oder zur Funktionsprüfung des Status Quo einen kompakten Check und Bewertung Ihrer Active Directory Umgebung und abhängiger Dienste durch.

Als Ergebnis präsentieren wir Ihnen eine Expertise über technische oder gestalterische Auffälligkeiten mit Bewertungen. Darauf basierend empfehlen wir Ihnen präventiver Maßnahmen zur Konsolidierung und Optimierung.

Der Umfang der Prüfungen richtet sich nach Ihrem Bedarf und der Komplexität der Infrastruktur. Durch den Screening-Check erhalten Sie eine funktionelle Effizienzsteigerung. So können Sie die Entwicklung Ihrer ADS-Infrastruktur sicher lenken.

DIE ACTIVE DIRECTORY PRÜFPUNKTE

- DNS-Konfigurationsstatus
- Betriebsmaster /GC Konfiguration
- Replikationstopologie von ADS und Sysvol
- Gruppenrichtlinienstatus in Zusammenhang mit dem GPO Konzept
- Analyse und Beurteilung von Events und Logs
- ADS-Backup und Restore
- Basic Security Checks - Patchmanagement
- weitere Checks, je nach Design und Vorlage der bestehenden Infrastruktur

UNSERE LEISTUNGEN

- Erfassung der bestehenden Domänen-Infrastruktur mit Funktionschecks anhand von Prüflisten, Script-basierten Abfragen und Interviews
- Erstellung einer Expertise zum Status Quo von ADDS und Bereitstellung eines Maßnahmen-Katalogs
- Dokumentation der Erfassungsdaten
- Beratung und Empfehlungen zu resultierenden Konfigurationsarbeiten

AD-Rechtekonzept

ACTIVE DIRECTORY SERVICES RECHTEKONZEPT

Holen Sie noch mehr Security Features aus der ADS!

Mit einem AD-Rechteverwaltungsmodell reduzieren Sie die den Verwaltungsaufwand und erhöhen zudem den Security Level. Mit rollenbasierten Rechteverwaltungsmodellen erhalten Sie nachvollziehbare und transparente Berechtigungs- und Authentifizierungsvorgänge.

DAS UNTERNEHMEN IN DIE IT SPIEGELN

Funktionsrollen im Unternehmen werden in Windows Gruppen abgebildet. Mit der rollenbasierten Delegation von Berechtigungen können

- festgelegte administrative Aufgaben
- begrenzte Ausführungsrechte
- begrenzte Bereiche im Active Directory Verzeichnisdienst und in der IT-Peripherie
- die Abbildung von Verwaltungsfunktionen in IT-Anwendungen definiert werden.

Damit werden die Zugriffe gesteuert. Dies ist ein wichtiger Bestandteil von IT-Security. Das Funktionsrollenmodell ist weiterhin die Grundlage für Identity Management Plattformen und die ITIL-Integration.

TRANSPARENZ MACHT SICHER UND SPART ARBEIT

Die dezentrale Verteilung der IT-Administration über Gruppen und Funktionsrollen bündelt die allgemeinen administrativen Aufgaben in der IT. Voraussetzungen für eine erfolgreiche Rechtedelegation ist:

- die Abbildung des Unternehmensorganigramm in AD-Organisationseinheiten (OU)
- die Festlegung der Verwaltungsrollen innerhalb der Arbeitsprozesse
- die Abbildung der Funktionsrollen in Windows Gruppen

NOCH MEHR SECURITY

Ein wesentlicher Gewinn an Sicherheit basiert auf der minimierten Rechtevergabe innerhalb der gesamten AD-Infrastruktur in allen exekutiven Bereichen durch eingeschränkte Windowsgruppenmitgliedschaften (least amount of privilege) und angepasste Gruppenrichtlinienanwendungen.

UNSERE LEISTUNGEN

- Beratung zu AD-Rechte- und Delegationskonzepten
- Erfassung der Geschäftsprozesse und Entwicklung einer Rechtestrategie
- Erstellen eines Maßnahmenkataloges für das AD-Delegationsmodell
- Organisationsdesign nach Organigramm und Standort Topologie
- Abbildung der Verwaltungsrollen in einem Windows-Gruppen-Design
- Präsentation einer Rechte-Matrix nach dem "Floating Rights"-Prinzip
- Delegationsvorlagen für Gruppenrichtlinien- und Exchange User-Management
- Delegierte User Helpdesk Verwaltung für 1.-3. Level mit on-board Konsolen (ITIL-konform)
- Delegierte Funktionsserver-Verwaltung in der Peripherie
- Script-basierte Rechtevergabe und Zugriffslistenbereinigung
- Dienstkonten-Verwaltung im Rahmen vom Rechtekonzept
- Überwachungsfunktionen zur Verifizierung der Delegationen
- Identity Management Beratung

Dateiserver- und Ressourcen-Rechtekonzept

SICHERHEITSELEVEL ANHEBEN

Es gibt viele Gründe für die Ablösung vorhandener Dateiserversysteme und die Umstellung auf virtuelle oder physikalische neue Dateiserver auf Basis von Windows Server: Der wichtigste ist die Anhebung des Sicherheitslevel beim Datenmanagement! Die Umstellung auf ein aktuelles Dateiserversystem bietet eine exponierte Chance zur Konsolidierung ihrer Dateiserverinfrastruktur. Damit erhalten Sie einen dauerhaften, sicheren und stets nachvollziehbaren Zugriffsschutz für ihre sensiblen Unternehmensdaten.

BERECHTIGUNGSKONZEPT AUF DREI SÄULEN

- Der Normierung von rollenbasierten Gruppen- und Gruppenmitgliedschaften im Active Directory
- statischen, einmaligen Berechtigungseinträge in den Zugriffskontroll-Listen (ACL) bei den Datenverzeichnissen auf dem Dateiserver unter Einhaltung der vordefinierten Verzeichnistiefe
- Integration der Organisationseinheiten (OU) und des Windowsgruppendesigns in bestehende ADS-Infrastrukturen

KLARE STEUERUNG

Die Berechtigungsvergabe erfolgt ausschließlich in der ADS über Gruppenzugehörigkeiten. Mit On-board-Verwaltungskonsolen und dem User Helpdesk kann in das Management durch Delegation eingebunden werden. Die Abbildung des Berechtigungsflow erfolgt nachvollziehbar über eine Matrix. Sensible Daten werden identifiziert und gesondert abgesichert. Die Anwender erhalten den Zugriff auf ihre Daten mit Hilfe einer einzigen Netzlaufwerksverbindung, der Gruppenrichtlinien-Preferences zugewiesen wird.

Das Berechtigungs-Modell kann für den Zugriff auf andere Ressourcen außerhalb der Dateiserver-Infrastruktur dynamisch adaptiert werden.

Niederlassungen und Kontakt

UNSERE LEISTUNGEN

- Erfassung anteiliger „Geschäftsprozesse“ für die Entwicklung der Berechtigungs-Strategie
- Design von Organisationseinheiten und Norm-Windowsgruppen für das Zugriffsmodell
- Erstellung einer Matrix für die Anordnung der Datenverzeichnisse (floating rights)
- Erstellung eines Entscheider Papiers für die interne Projektpräsentation
- Separate Absicherung sensibler Datenverzeichnisse mit „empty groups“- Konzept
- GPO-Konsolidierung mit Bereitstellung von einem Laufwerk für die Anwender per GPO
- Praktische Unterstützung beim Datenumzug in neue Struktur
- ACL Bereinigung mit Revision von Einzelberechtigungen, Vermeidung von Phantom-SIDs
- Archiv-Lösungen bei der Datenmigration und dynamischen Datensammlungen
- Übertragung vom Berechtigungskonzept auf andere IT-Ressourcen
- Effizienter Einsatz und Nutzung von Windows Server Features
- Optionale Verzeichniszugriffsüberwachung für sensible Datenablagen
- Dokumentationen mit Tools

Die Leistungen sind abhängig von der bereits bestehenden Infrastrukturumgebung. Die Planung und Budgetierung der Leistungen erfolgen individuell nach der ersten Begutachtung und der IST-Analyse. Im Mittel sind 2-4 Tage operativer Service notwendig.

LUZ & GRUB AG ZENTRALE

Am Sandfeld 9
76149 Karlsruhe
Tel.: +49(721)98184-0

Tim Nattermann
Tel.: +49 (721) 9818423
E-Mail: tnattermann@lutzundgrub.de



Zentrale Karlsruhe
Am Sandfeld 9
76149 Karlsruhe
Telefon: +49 (721)-98184-0



Niederlassung Nürnberg
Frankenstraße 160
90461 Nürnberg
Tel: +49 (911)-710460-0
Niederlassung Stuttgart



Gutenbergstr. 11
70771 Leinfelden-Echterdingen
Tel: +49 (711) 5087148-0
Niederlassung Heilbronn



Neckargartacherstraße 90
74080 Heilbronn
Tel: +49 (7131) 264160-0