

AUDITING FÜR GROUP POLICIES

Der Kunde

Das Rechenzentrum der Finanzverwaltung (RZF) des Landes Nordrhein-Westfalen in Düsseldorf stellt als Dienstleister den insgesamt 143 Dienststellen der Festsetzungs-, Betriebsprüfungs- und Strafsachenfinanzämtern, den Oberfinanzdirektionen und den drei Schulungseinrichtungen IT-Leistungen zur Verfügung. Das RZF beschäftigt mehr als 600 Mitarbeiter, darunter über 280 Programmierer, die die Anwendungen etwa für die Veranlagungs-, die Anmeldungs- und Kraftfahrzeugsteuer sowie die Buchführung der Finanzkassen entwickeln und pflegen. Darüber hinaus unterhält das RZF für die Finanzverwaltung ein Wide Area Network (WAN) und lokale Netze (LAN).



„Die von der sepago erarbeitete Auditinglösung fügt sich perfekt in unser Changemanagement ein. Nun haben wir wirklich die volle Kontrolle über sämtliche Veränderungen, die für uns relevant sind“

Dietmar Rilke, Dezernatsleiter Rechenzentrum der Finanzverwaltung NRW

Die Aufgabe

Das RZF betreibt in NRW für mehr als 31.000 Benutzer eine dezentrale Client-Serverumgebung mit 143 Standorten, die zentral gesteuert und administriert wird. Auf zwei getrennten Systemumgebungen (Entwicklungslabor und Produktion) wird ein dreistufiger Change-Prozess (Entwicklung, Qualitätssicherung, Produktion) realisiert. Das eigenständige Entwicklungslabor ist mit einer losgelösten Active Directory (AD) Struktur und allen wesentlichen Infrastrukturdiensten der Produktionsumgebung nachgebildet. Typischerweise werden in einer Laborumgebung Änderungen innerhalb der AD häufiger und schneller vorgenommen als in einer Produktivumgebung. Daher sollte sicher gestellt werden, dass diese im Entwicklungslabor gefundenen veränderten GPO-Einstellungen (Werte und Berechtigungen) regelmäßig in die Produktion übernommen werden. Weitere Herausforderungen waren die Bereitstellung einer Veränderungshistorie (im Entwicklungslabor), sowie der Vergleich der beiden Systemumgebungen Entwicklungslabor und Produktion.

Der Ansatz

Für die Umsetzung wurden im ersten Schritt verschiedene Lösungsmöglichkeiten analysiert. Hier müssten sowohl die entstehenden Kosten für die Umsetzung als auch die Kosten für die spätere Betreuung und Erweiterung des Systems betrachtet werden. Zudem sollte die Lösung für zusätzliche Auditing-Aufgaben (z.B. NTFS Security Groups und NetInstall) leicht erweiterbar sein. Ziel war es, Technologien zu verwenden, die sich bereits im Einsatz befanden, um vorhandenes Know-how zu nutzen und Kosten zu minimieren.

In der Evaluierungsphase wurden schnell die Vorteile einer XML-basierten Abbildung von Strukturen für weitere Auditing Aufgaben erkannt. Die Konsequenz war der Entwurf eines generischen Frameworks für Auditingaufgaben mit folgenden Eigenschaften:

- Ablauf- und Prozesssteuerung
- Aktionsorientierte Schnittstelle
- Leichte Erweiterbarkeit
- Generische Diff-Engine
- Umfangreiches Reporting

Die Lösung

sepago schaffte mit der Realisierung in Form eines Frameworks eine erfolgreiche Lösung für die genannten Anforderungen. Die eigene Ablauf- und Prozesssteuerung des Frameworks leitet die verschiedenen Phasen ein und reagiert auf den ermittelten Status eines überwachten Strukturobjektes, wie z.B. einer GPO. Die wesentliche Komponente des Systems ist die von der sepago entwickelte XML-Diff-Engine, die einen Vergleich auf Basis von vorher erstellten Snapshots im XML-Format durchführt. Über konfigurierbare Filter können bestimmte Eigenschaften der Snapshots von der Überwachung flexibel ausgenommen werden (z.B. Berechtigungen). Daher ist es für die Diff-Engine unerheblich, ob es sich um eine GPO-Struktur bzw. deren Objekte oder um eine AD-Struktur mit NTFS-Security-Groups handelt. So gelingt die gesicherte Erkennung von neuen, gelöschten und veränderten Elementen und deren genauen Einstellungswertveränderungen.

In einer aktionsorientierten Schnittstelle sind Folgeprozesse definiert, wie etwa die automatische Sicherung eines geänderten Group-Policy-Objektes oder die Bereitstellung einer veränderten Policy aus der Produktion für das Entwicklungslabor. Im Falle einer Fehlkonfiguration besteht somit immer die Möglichkeit eines Restore der vorgenommenen Anpassungen. Das umfangreiche Reporting bietet die ermittelten Informationen über Veränderungen in der Struktur über mehrere Kanäle an: per Emailverteiler, über ein Web-Portal als zentrales Informationssystem und ergänzt um ein „Web Parts im SharePoint-Server“. Darüber hinaus wird noch eine zentrale Änderungshistorie geführt. Das erstellte Framework wurde zunächst im Labor für das Auditing der Group Policies erfolgreich implementiert. Nach der Implementierung und Inbetriebnahme der Lösung in der Produktion erfolgte die Übergabe des Systems. Das generische Design ermöglicht es auf sehr einfache Art und Weise, die Lösung um weitere Module zu erweitern. So wird derzeit ein Auditing für die NetInstall-Umgebung implementiert.

Fazit

Das Konzept und die Implementierung haben sich bisher sehr gut bewährt und ermöglichen die Überwachung der wichtigsten Teile einer umfangreichen und komplexen Umgebung mit geringem personellem Aufwand. Die Lösung ermöglicht den unterschiedlichen Fachbereichen sich jederzeit über Änderungen einfach zu informieren und damit auf dem aktuellen Kenntnisstand zu sein. Zudem war es immer möglich, schnell neue Anforderungen in das bestehende System zu integrieren.