

NetIQ Change Guardian for Group Policy

Einhaltung aufsichtsrechtlicher Vorschriften durch Überwachung der Änderungen an Gruppenrichtlinien

Im Überblick

NetIQ Change Guardian for Group Policy minimiert die mit Änderungen an Gruppenrichtlinienobjekten (GPO) verbundenen Risiken und trägt dazu bei, alle befugten und unbefugten Gruppenrichtlinienänderungen innerhalb der Produktionsumgebung zu ermitteln und zu dokumentieren.

Die Lösung automatisiert und vereinfacht die Überwachung von Änderungen an Gruppenrichtlinienobjekten im Active Directory, indem Art und Urheber der Änderungen angezeigt werden. Mit NetIQ Change Guardian for Group Policy lassen sich Änderungen an Gruppenrichtlinien in Echtzeit denkbar einfach überwachen, überprüfen und verfolgen; hierbei werden alle Änderungen in einer Auditing-Datenbank erfasst. Mit dieser Funktion zur Änderungsüberwachung lässt sich gegenüber Prüfern nachweisen, dass die zur Erfüllung aufsichtsrechtlicher Vorschriften implementierten Unternehmensrichtlinien genauestens eingehalten werden.

Zeitgemäße Lösung

Bei einwandfreier Bereitstellung und Umsetzung sind Gruppenrichtlinien eine sehr leistungsstarke Komponente zur Active-Directory-Verwaltung, die zu einer sicheren und zuverlässigen Windows-Umgebung beiträgt. Werden die Änderungen an Gruppenrichtlinien jedoch nicht einwandfrei überwacht und kontrolliert, können Serviceunterbrechungen, Replikationsprobleme, fehlerhafte Administratorrechte und böswillige Modifikationen an Gruppenrichtlinienobjekten die Folge sein.

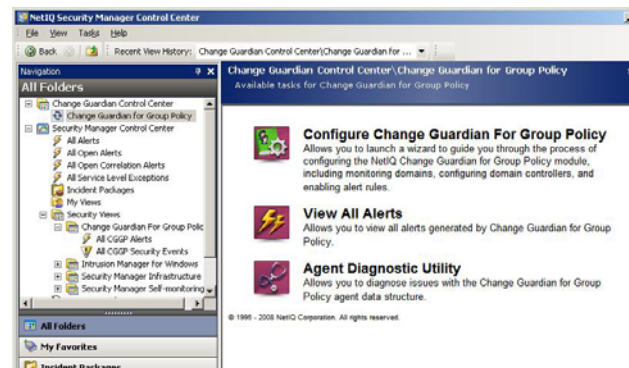
NetIQ Change Guardian for Group Policy meldet Änderungen an Gruppenrichtlinienobjekten in Echtzeit und erfasst Änderungsmaßnahmen in einer Auditing-Datenbank unter Angabe von Zeitpunkt und Urheber.

Entscheidende Vorteile

Garantierte Compliance durch Änderungsüberwachung – Die Lösung vermittelt den nötigen Überblick, um unsachgemäße Änderungen an Gruppenrichtlinienobjekten zu stoppen, bevor diese die Sicherheit oder Verfügbarkeit der Active-Directory-Umgebung beeinträchtigen können.

Verbesserung von IT-Servicelevel und Reaktionsfähigkeit – Die Produktivität der Mitarbeiter wird verbessert, indem durch fehlerhafte Änderungen an Gruppenrichtlinienobjekten verursachte Systemausfälle minimiert werden.

Änderung an Gruppenrichtlinien in Echtzeit – Änderungen an kritischen Komponenten der Gruppenrichtlinienumgebung werden sofort wirksam.



Audit-freundliche Berichte über verwaltete und nicht verwaltete Änderungen; detaillierte Ansichten zur Durchführung routinemäßiger Kontrollen.

Benachrichtigung bei bestimmten Änderungen der Gruppenrichtlinien unter Angabe der Änderungsbefugnis – Änderungen an Gruppenrichtlinienobjekten werden per E-Mail oder Pager sofort mitgeteilt, um unverzüglich darauf reagieren zu können. In Verbindung mit NetIQ Group Policy Administrator™ kann das Kontrollsystem die Änderungen als befugt oder unbefugt klassifizieren.

Detaillierte Dokumentation aller Gruppenrichtlinienänderungen – Änderungen an Gruppenrichtlinienobjekten werden genau und vollständig mit einer übersichtlichen Änderungsmarkierung ausgewiesen.

Erstellung leistungsstarker, umfassender Berichte – In der Auditing-Datenbank werden sämtliche Änderungsereignisse nach benutzerdefinierten Kriterien protokolliert, einschließlich der Parameter vor und nach Durchführung der Änderung. Zu jeder Änderungsbenachrichtigung lassen sich detaillierte Berichte erstellen.

Integration in vorhandene Überwachungsinfrastruktur – Die Lösung integriert sich in die gängigen Systemverwaltungslösungen, wie AppManager®, NetIQ Security Manager™ und Microsoft Operations Manager (MOM). Dies vereinfacht die Konfiguration und die Bereitstellung im Sinne einer schnellen und kostengünstigen Implementierung.

NetIQ Change Guardian for Group Policy

NetIQ Change Guardian for Group Policy erleichtert die Einhaltung aufsichtsrechtlicher Vorschriften durch Überwachung der Änderungen an Gruppenrichtlinien. Die Lösung integriert sich reibungslos in AppManager, NetIQ Security Manager und MOM.

Technische Merkmale

- Benachrichtigung in Echtzeit bei Änderungen an Gruppenrichtlinien, Sicherheitsfiltern und Links
- Dokumentation der Änderung, des Urhebers und des Zeitpunkts
- Benachrichtigung über E-Mail oder Pager
- Regelbasierte Überwachung gemäß mehr als 100 vordefinierten Regeln für jedes Gruppenrichtlinienobjekt
- Integration in AppManager, NetIQ Security Manager und MOM
- Umfassendes Reporting mit detaillierten Berichten zu jeder Benachrichtigung
- Abfragen aus Auditing-Datenbanken unter Angabe aller Aktivitäten nach benutzerdefinierten Kriterien
- Audit-Reports mit Ausweisung der Parameter vor und nach der Änderung
- Audit-Datenbank mit einer vollständigen und detaillierten Historie der Gruppenrichtlinienänderungen
- Unterstützung der GPO-Einstellungen in Windows 2000, Windows 2003 und Windows XP
- Unkomplizierte Filterung der Berichtsergebnisse nach mehreren Parametern, wie Organisationseinheit (OU), Standort (Site) und Gruppenrichtlinienobjekt (GPO)

Systemvoraussetzungen

Hardwarekonfiguration:

- CPU des Datenbankservers: Intel Pentium 4 mit mindestens 550 MHz
- Plattenkapazität des Datenbankservers: 5 GB freie Kapazität
- Arbeitsspeicher des Datenbankservers: Mindestens 512 MB RAM, 1 GB RAM empfohlen

Kontakt

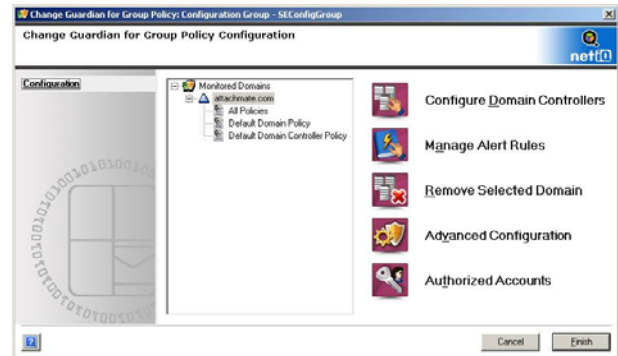
Internationaler Sitz
NetIQ, An Attachmate
Business
1233 West Loop South
Suite 1800
Houston, TX 77027, USA
713.548.1700
713.548.1771 Fax
888.323.6768 Verkauf

NetIQ Deutschland GmbH
+49 (0)89 99351-0
infoDE@Netiq.com
www.netiq.de

NetIQ Schweiz
+41 43399 3090
infoCH@Netiq.com
www.netiq.de

NetIQ Österreich
+43 15954335
infoDE@NetIQ.com
www.netiq.de

Informationen über weitere Geschäftsstellen, Partner und Wiederverkäufer finden Sie auf unserer Website unter www.netiq.com/contacts



Echtzeit-Benachrichtigungen für kritische Änderungen an Gruppenrichtlinien.

Softwarekonfiguration:

- AppManager, Security Manager oder Microsoft

Operations Manager

- Betriebssystem des Datenbankservers:
 - Windows 2000 SP3 oder neuer
 - Windows 2003
 - Windows 2003 SP1
 - Windows 2008
 - Windows XP SP1
 - Windows XP SP2
 - Windows Vista
- Microsoft SQL Server 2000 SP3
- Microsoft Data Access Components 2.6 oder neuer
- Windows 2000 Native Mode mit laufendem DNS