

NetIQ Change Guardian for Active Directory

Garantierte Compliance durch Dokumentation und Meldung aller Änderungen am Active Directory

Im Überblick

NetIQ Change Guardian for Active Directory minimiert die mit betriebsbedingten Änderungen am Active Directory verbundenen Risiken. Diese Lösung verleiht den nötigen Überblick, um Active Directory vor gefährlichen Sicherheitsrisiken und kostspieligen Serviceausfällen schützen zu können, indem sie Änderungen an der Active-Directory-Umgebung einfach und automatisch überwacht.

Zeitgemäße Lösung

Angesichts strengerer Auflagen und höherer interner Risiken arbeiten Unternehmen an Lösungen, die dafür geeignet sind, Schaden von Anteilseignern und Kunden sicher abzuwenden. Active Directory ist die Kernkomponente vieler Programme zur Verwaltung der Sicherheit und Identität in Netzwerken, mit dem Ziel, einschlägige Auflagen zu erfüllen. Die Sicherheit von Active Directory durchgängig zu gewährleisten, ist allerdings eine anspruchsvolle Aufgabe.

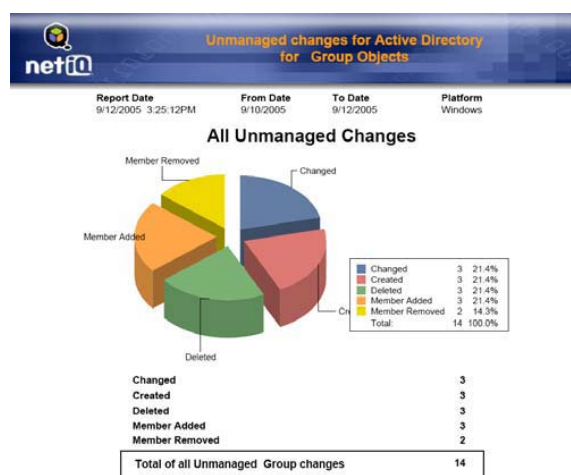
Die Risiken betriebsbedingter Änderungen lassen sich am wirksamsten mit einer abgestimmten Strategie in den Griff bekommen, bei der Änderungen am Active Directory akribisch überwacht werden. Bereits vorhandene Technologien werden mit NetIQ Change Guardian for Active Directory optimal genutzt, während gleichzeitig potenzielle Schwachstellen in dem für Active Directory implementierten Change-Management-Prozess aufgedeckt werden.

Entscheidende Vorteile

Erkennung verwalteter und nicht verwalteter Änderungen – Nicht relevante Warmmeldungen werden signifikant reduziert. Stattdessen kann der Schwerpunkt auf nicht verwaltete Active-Directory-Änderungen mit Benachrichtigung in Echtzeit gelegt werden. So verbessert NetIQ Change Guardian for Active Directory die Kontrolle darüber, ob den Richtlinien im Active Directory entsprochen wird.

Ermittlung von Änderungen mit weitreichenden Auswirkungen – Sobald irgendwo in der Umgebung weitreichende Änderungen erfolgen, werden detaillierte Berichte und Warmmeldungen erstellt. Die Lösung überwacht mit bestimmten Rechten ausgestattete Gruppen und ermöglicht es darüber hinaus, spezielle Gruppen oder Aktivitäten zu definieren, die einer besonders sorgfältigen Überwachung im Unternehmen bedürfen.

Protokollierung und Audit von Änderungen am Active Directory – Es können detaillierte Berichte über Änderungen in der jeweiligen Umgebung erstellt werden, die Aufschluss über den Anteil nicht verwalteter Änderungen geben. Mitgelieferte Vorlagen erleichtern zudem die Erstellung von Change-Audit-Reports.



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

Einfache Integration in den vorhandenen Active-Directory-Änderungsprozess – Die Lösung integriert sich problemlos in die bereits vorhandenen Tools zur Verwaltung der Active-Directory-Umgebung und weist auf Modifikationen im Änderungsprozess hin.

Einsatz in gängigen, flexiblen Infrastrukturen – Die Investitionen machen sich in kurzer Zeit bezahlt; die Funktionalität von NetIQ Security Manager™ oder Microsoft Operations Manager wird voll genutzt, wodurch beide Produkte sinnvoll eingesetzt werden können, um die Sicherheit und Compliance der Active-Directory-Umgebung zu gewährleisten.

NetIQ Change Guardian for Active Directory

Technische Merkmale

Benachrichtigung in Echtzeit

- Zentrale Protokollierung verwalteter und nicht verwalteter Änderungen am Active Directory
- Zahlreiche Funktionen zur Erzeugung von Warnmeldungen über NetIQ Security Manager oder Microsoft Operations Manager, z.B. über E-Mail, Pager oder Anwendungskonsole
- Beschränkung der Warnmeldungen auf klassifizierte Änderungstypen, ob verwaltete Änderungen oder Änderungen mit weitreichenden Auswirkungen
- Warnmeldungen zu potenziellen Sicherheitsproblemen im Active Directory, noch bevor eine Schädigung erfolgen kann

Audit-freundliches Reporting

- Detaillierte Berichte über Änderungen am Active Directory
- Bessere Lesbarkeit der Berichte durch Konzentration auf den Änderungstyp, z.B. verwaltete Änderungen, Änderungen mit weitreichenden Auswirkungen oder nicht verwaltete Änderungen
- Ausweisung des Anteils der in der Umgebung vorgenommenen, nicht verwalteten Änderungen
- Einfache Analyse von Audit-Reports mithilfe vorbereiteter Vorlagen für unterschiedliche Zielgruppen, z.B. Prüfer oder Unternehmensleitung

Leistungsstarkes Log-Management über NetIQ Security Manager

- Unkomplizierte Verwaltung großer Sicherheitsdatenmengen mit flexiblen Log-Archivierungsfunktionen
- Berichte und Werkzeuge für die Trendanalyse
- Leistungsstarke Funktionen zur forensischen Untersuchung

Kontakt

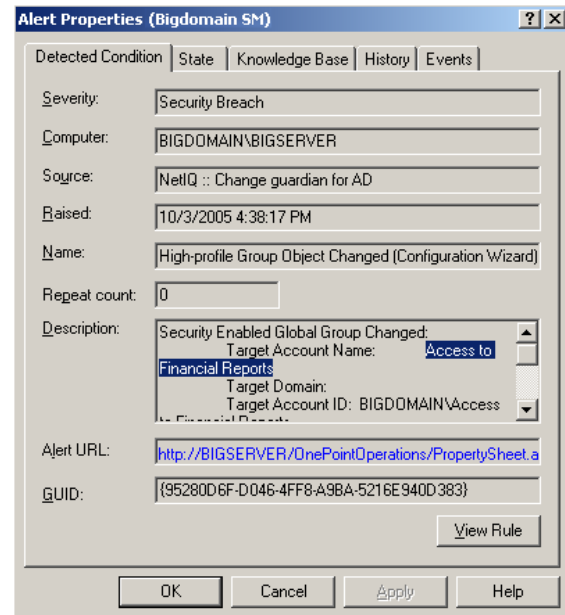
Internationaler Sitz
NetIQ, An Attachmate
Business
1233 West Loop South
Suite 1800
Houston, TX 77027, USA
713.548.1700
713.548.1771 Fax
888.323.6768 Verkauf

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



Bei weitreichenden Änderungen am Active Directory werden Warnmeldungen ausgelöst, um unverzüglich Maßnahmen zur Gewährleistung der Sicherheit ergreifen zu können.

Systemvoraussetzungen

Voraussetzungen des Monitoring-Servers:

- Windows 2000/2003 Server
- NetIQ Security Manager 5.1 SP1 (mit Hotfix 48546) oder Microsoft Operations Manager 2005

Überwachte Active-Directory-Umgebung:

- Windows 2000/2003 Server Domänencontroller in einer Active-Directory-Umgebung