# Netwrix Auditor для контроля действий администраторов

Аудит изменений в инфраструктуре Microsoft: Active Directory, Exchange, Group Policy

## Обзор продукта

Аудит изменений **Active Directory** (AD) — крайне важная процедура для отслеживания несанкционированных модификаций и ошибок в конфигурациях AD и групповых политик. Программа Netwrix Auditor отслеживает сделанные в AD и групповых политиках изменения, генерирует отчеты и оповещения по каждому инциденту, отражая добавления, удаления и изменения всех типов объектов AD. Помимо этого, в отчеты включена информация о значениях “до” и “после” по каждой модификации, для оперативного восстановления данных.

**Microsoft Exchange** – один из ключевых компонентов ИТ- инфраструктуры. Netwrix Auditor для Exchange позволяет контролировать изменения в настройках сервера, хранилищ, параметрах протоколов, правах доступа и других объектов, отслеживать создаваемые и удаляемые почтовые ящики и многое другое.

**Групповые политики (GP)** – основной инструмент для контроля доступа к важной информации. Штатные системы аудита не предоставляют полные данные обо всех изменениях в политиках. Netwrix Auditor для Групповых политик собирает данные об изменениях объектов GP, формирует подробные отчеты и рассылает уведомления, отражающие информацию об источнике изменений и значениях до и после модификации.

## Преимущества Netwrix Auditor для инфраструктуры MS:

- Подробные отчеты по заданным параметрам или из библиотеки стандартных отчетов (более 200 видов);
- Возможность рассылки отчетов по расписанию;
- Фильтры событий по пользователям, OU, контроллерам;
- Работа в режиме использования агентов/без использования агентов;
- Масштабируемость и надежность;
- Единый интерфейс управления Netwrix для всех компонентов инфраструктуры Microsoft;
- Возможность интеграции с Microsoft System Center и SIEM-системами: RSA enVision®, ArcSight® Logger™, Novell® Sentinel™, NetIQ® Security Manager™, Symantec SIM IBM Tivoli® Security Information and Event Manager™;
- Возврат изменений в AD и GP без перезагрузки контроллеров домена.

## Отличия от встроенных средств аудита

- Консолидация событий на всех контроллерах домена;
- Оповещения в режиме реального времени;

- Отслеживание любых атрибутов, понятные отчеты (не только GUID);
- Фиксация значений «до» и «после» изменения для оперативного восстановления информации;
- Оповещения владельцев о попытках доступа к их почтовым ящикам;
- Долгосрочное хранение данных аудита (до 7 лет и более) для соответствия требованиям нормативов информационной безопасности.

## Функции Netwrix Auditor для **Active Directory**

- Консолидация данных нескольких контроллеров домена;
- Возможность задавать настройки индивидуально для каждого из объектов инфраструктуры;
- Предоставление детальной информации обо всех изменениях в AD;
- Доставка отчетов об изменениях по расписанию, заданным пользователям;
- Ежедневная отправка по электронной почте, в формате HTML и CSV, отчетов со списком всех произведенных за день изменений;
- Предоставление отчетов в форматах Adobe Acrobat, Microsoft Excel, Microsoft Word, CSV;
- Отображение значений атрибутов системы AD в состоянии «до» и «после» внесенных изменений;
- Отображение состояния атрибутов системы Active Directory на любую заданную дату в прошедшем периоде;
- Предоставление доступа к отчетам через веб-интерфейс с возможностью гибкой настройки поиска, фильтрации и группировки данных;
- Восстановление предыдущих значений для любых изменений без перезагрузки контроллера домена;
- Поддержка протоколов SMTP- аутентификации и SSL.

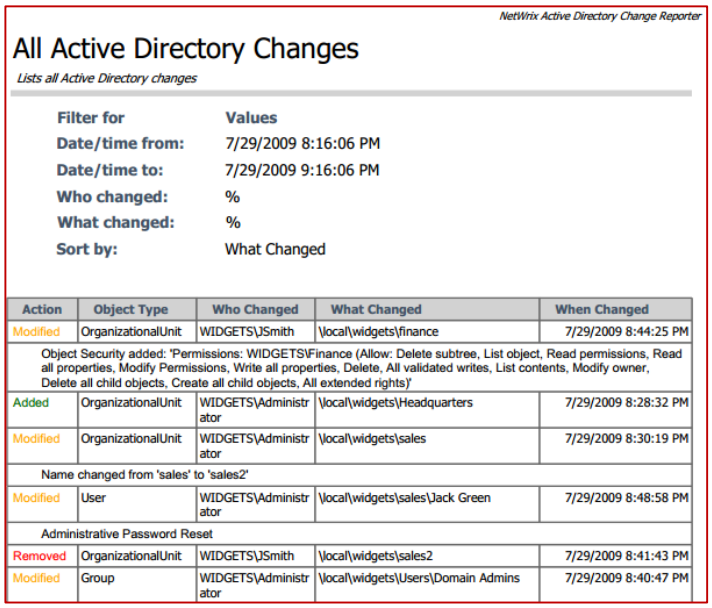
## Функции Netwrix Auditor для **Exchange**

- Консолидация данных из нескольких серверов Exchange;
- Предотвращение потери данных аудита в случае перезаписи журнала событий;
- Оповещения в реальном времени о критичных изменениях в настройках Microsoft Exchange;
- Предоставление детальной информации обо всех изменениях в настройках Microsoft Exchange;
- Оповещение владельцев о попытках доступа к их почтовым ящикам и других событиях;
- Отображение значений атрибутов системы Microsoft Exchange в состоянии до и после внесенных изменений;
- Доставка отчетов об изменениях по расписанию, заданным пользователям;
- Ежедневная отправка по электронной почте, в формате HTML и CSV, отчетов со списком всех произведенных за день изменений;
- Предоставление отчетов в форматах Adobe Acrobat, Microsoft Excel, Microsoft Word, CSV;
- Библиотека отчетов, необходимых для аудита на соответствие стандартам безопасности;
- Восстановление предыдущих значений для любых изменений без перезагрузки контроллера домена.

# Функции Netwrix Auditor для **Group Policy**

- Предоставление детальной информации обо всех изменениях GP;
- Отображение значений атрибутов групповых политик в состоянии «до» и «после» внесенных изменений;
- Автоматическое резервирование и восстановление объектов GP для защиты настроек GP от непреднамеренных изменений;
- Автоматическая отправка отчетов указанным получателям;
- Снимки состояния групповых политик (snapshots) для проведения детального анализа изменений объектов;
- Стабильная работа программы в инфраструктуре любого масштаба (отслеживание до 1 млн. объектов).

# Пример отчета



*NetWrix Active Directory Change Reporter*

## All Active Directory Changes

*Lists all Active Directory changes*

| Filter for | Values |
|---|---|
| Date/time from: | 7/29/2009 8:16:06 PM |
| Date/time to: | 7/29/2009 9:16:06 PM |
| Who changed: | % |
| What changed: | % |
| Sort by: | What Changed |

| Action | Object Type | Who Changed | What Changed | When Changed |
|---|---|---|---|---|
| Modified | OrganizationalUnit | WIDGETS\JSmith | \local\widgets\finance | 7/29/2009 8:44:25 PM |
| Object Security added: 'Permissions: WIDGETS\Finance (Allow: Delete subtree, List object, Read permissions, Read all properties, Modify Permissions, Write all properties, Delete, All validated writes, List contents, Modify owner, Delete all child objects, Create all child objects, All extended rights)' | | | | |
| Added | OrganizationalUnit | WIDGETS\Administrator | \local\widgets\Headquarters | 7/29/2009 8:28:32 PM |
| Modified | OrganizationalUnit | WIDGETS\Administrator | \local\widgets\sales | 7/29/2009 8:30:19 PM |
| Name changed from 'sales' to 'sales2' | | | | |
| Modified | User | WIDGETS\Administrator | \local\widgets\sales\Jack Green | 7/29/2009 8:48:58 PM |
| Administrative Password Reset | | | | |
| Removed | OrganizationalUnit | WIDGETS\JSmith | \local\widgets\sales2 | 7/29/2009 8:41:43 PM |
| Modified | Group | WIDGETS\Administrator | \local\widgets\Users\Domain Admins | 7/29/2009 8:40:47 PM |

# Дополнительно

Для оценки возможностей продуктов Netwrix воспользуйтесь следующими вариантами:

- скачайте пробную версию;
- пройдите online тест-драйв;
- запишитесь на демонстрацию программы.

# О Netwrix Corporation

Netwrix Corporation – международная компания, основанная в 2006 году, специализирующаяся на разработке, внедрении и сопровождении программного обеспечения для эффективного управления IT-ресурсами. Компания Netwrix предлагает инновационные технологии и приложения, неоднократно отмечаемые наградами на престижных международных конкурсах и IT-выставках. Netwrix помогает решать проблемы контроля и безопасности IT-инфраструктуры с помощью простых, надежных и эффективных продуктов, не требующих больших временных затрат на внедрение и настройку и не оказывающих негативного воздействия на существующую IT-систему. Офисы компании открыты в США, Великобритании и России.

**Netwrix Corporation,** 197374, РФ, Санкт-Петербург, Торфяная дор, д. 7, лит. Ф, БЦ «Гулливер2»

**Тел.: +7 (812) 309-5498**

**Офисы:**
New York, Atlanta, Columbus, Irvine, London

**Int'l:** +1 (949)407-5125

netwrix.com/social