netwrix

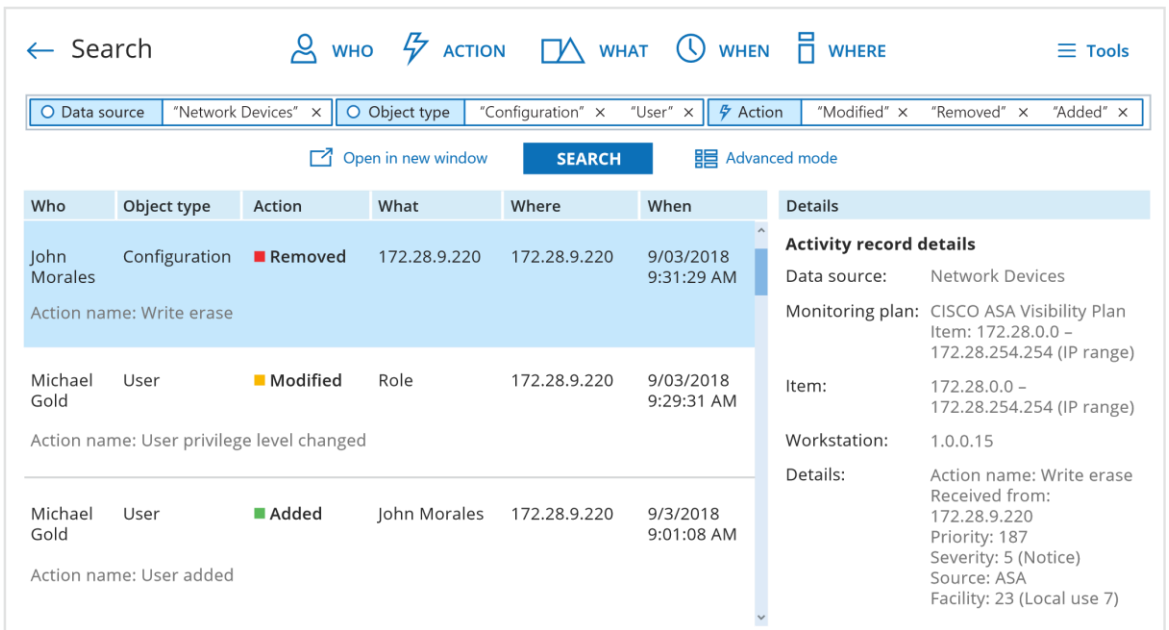
Топ-5 инцидентов с сетевыми устройствами, которые нужно контролировать

Содержание

1. Изменения конфигурации

Вам необходимо отслеживать все изменения конфигурации сетевых устройств: протоколы, порты, ограничения для подключения и т. д. Любое несанкционированное или ненадлежащее изменение может вызвать проблемы с подключением, в том числе привести к полной недоступности сети. Вам также необходимо сразу же получать уведомления о том, что кто-то изменил групповую политику или создал нового пользователя, поскольку это может быть признаком инсайдерской атаки или злоупотребления полномочиями. Netwrix Auditor отслеживает как успешные, так и неудачные попытки изменения конфигурации, позволяя быстро найти ответ на следующие вопросы:

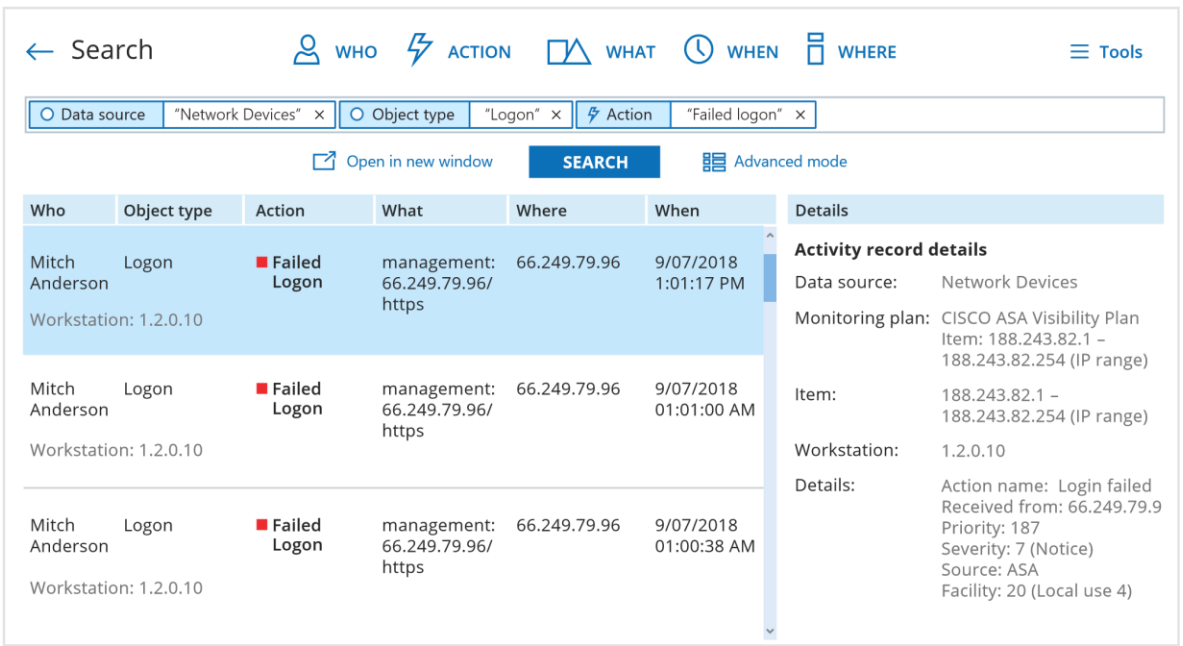
1. Кто сбросил настройки конфигурации определенного сетевого устройства?
2. Какие настройки брандмауэра были изменены?
3. С какого IP-адреса поступила команда на перезагрузку?
4. Когда был сброшен пароль маршрутизатора?



2. Неоднократные неудачные попытки входа в систему

Крайне важно отслеживать успешные попытки входа в систему на сетевых устройствах, чтобы проверить, действительно ли пользователь имеет соответствующие права. Однако не менее важно отслеживать неоднократные неудачные попытки входа: они могут означать, что кто-то пытается методом перебора узнать пароль администратора. Если злоумышленники получат доступ к сетевому устройству, они смогут контролировать весь сетевой трафик и похитить конфиденциальные данные. Netwrix Auditor отслеживает как успешные, так и неудачные попытки входа в систему, позволяя выявить возможные атаки методом перебора и быстро найти ответ на следующие вопросы:

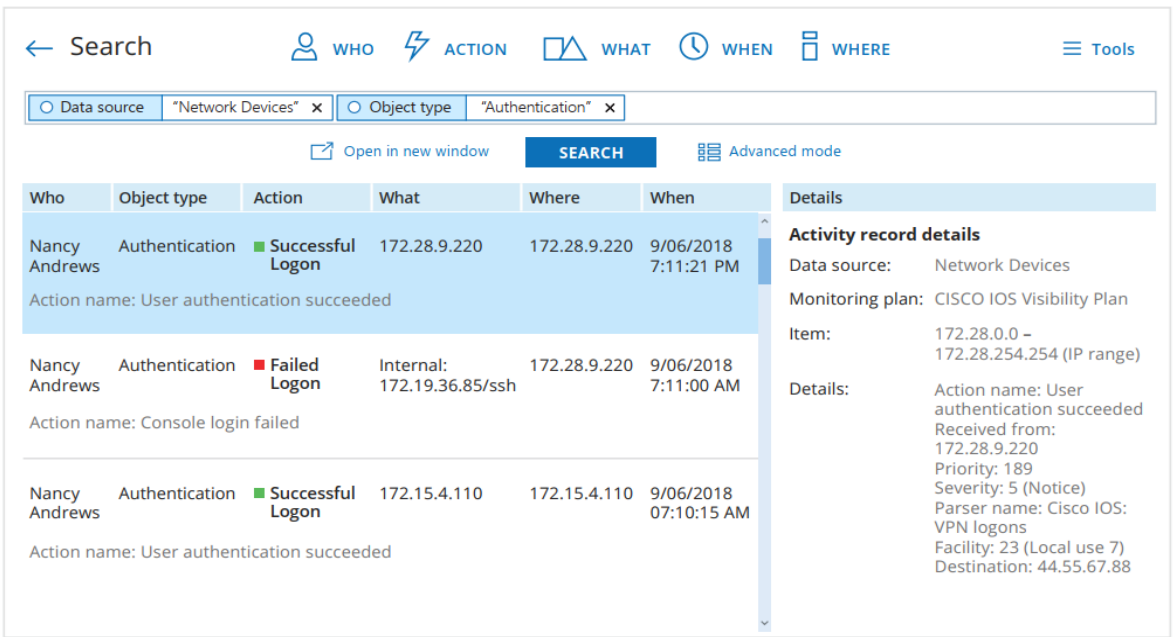
1. Кто превысил максимально допустимое число последовательных неудачных попыток входа в систему?
2. Что стало причиной ошибок при входе в систему?
3. С какого IP-адреса были сделаны эти попытки?
4. Сколько попыток было предпринято?
5. Когда были сделаны неудачные запросы аутентификации?
6. На каком устройстве пользователь пытался войти в систему?



3. Вход в систему с помощью VPN

Администраторы редко входят в систему на сетевых устройствах удаленно, поэтому важно отслеживать попытки входа с помощью VPN. Более того, даже авторизованное устройство с безопасным подключением к корпоративной сети можно взломать и использовать для получения доступа к конфиденциальным файлам. Netwrix Auditor позволяет отслеживать как успешные, так и неудачные попытки входа в систему на сетевых устройствах через VPN и находить ответы на следующие вопросы:

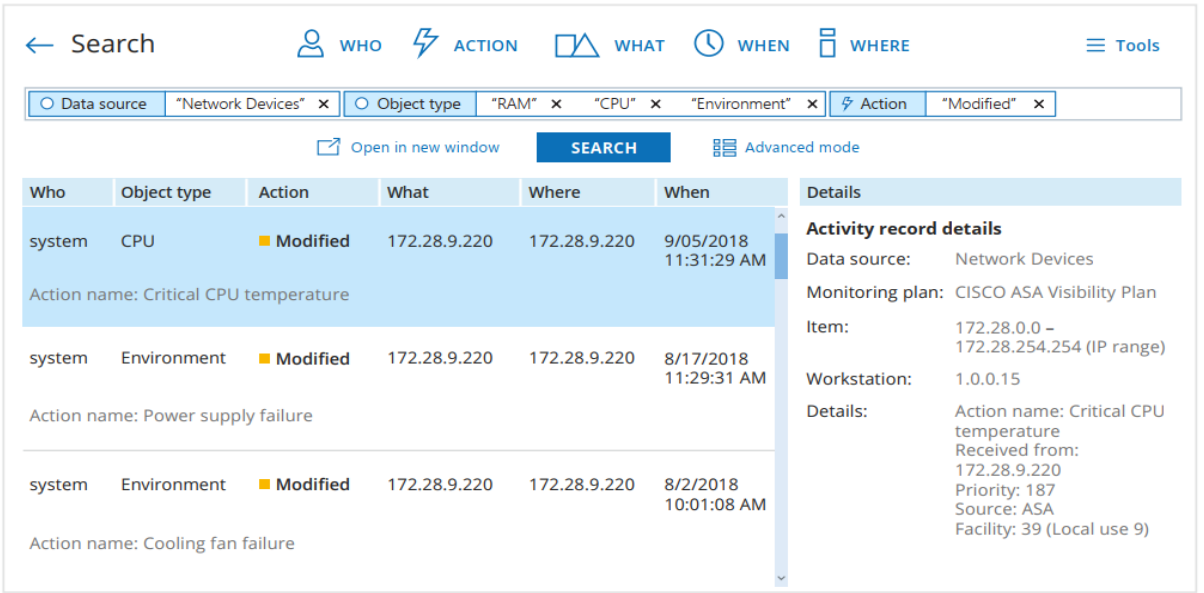
1. Кто пытался получить доступ к сетевым устройствам с помощью VPN?
2. С какого IP-адреса были сделаны попытки аутентификации?
3. Что стало причиной ошибок при входе в систему с помощью VPN?
4. Когда были сделаны неудачные попытки входа в систему с помощью VPN?
5. На каком устройстве пользователь пытался войти в систему?



4. Сбои в работе оборудования

Помимо отслеживания изменений в конфигурации сетевых устройств, необходимо также следить за состоянием оборудования. Если условия окружающей среды или питание сетевого устройства не соответствуют техническим требованиям, это может привести к перегреву устройства, отказу вентиляции или потере мощности с последующим снижением производительности или даже полной остановкой работы сети. Netwrix Auditor отслеживает состояние оборудования и оповещает о критических сбоях в его работе, позволяя найти ответ на следующие вопросы:

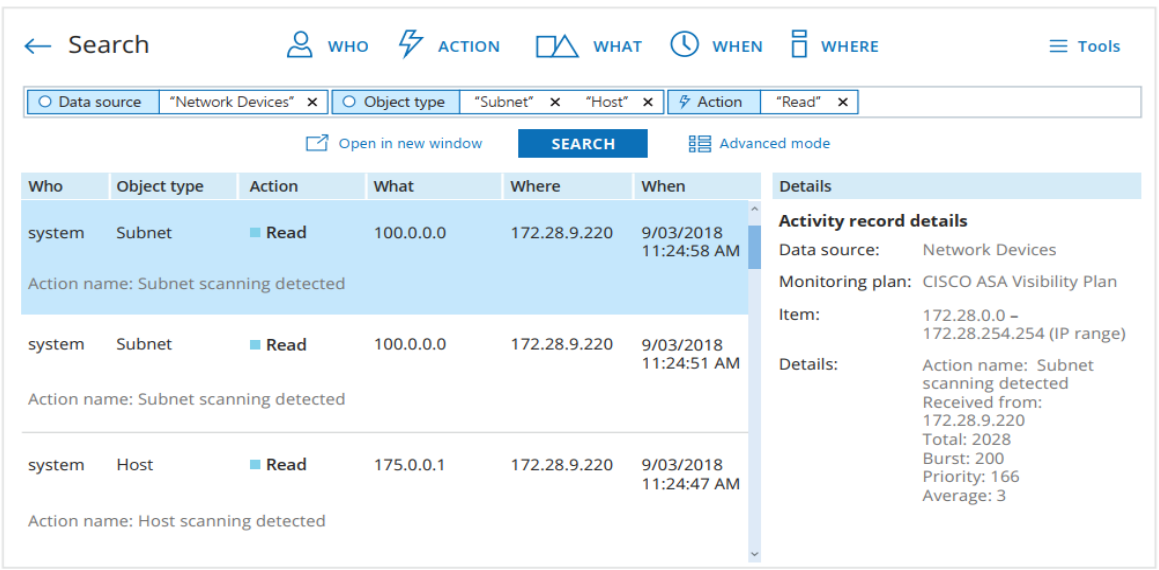
1. Какие действия были выполнены перед отключением сетевого устройства?
2. Какая часть сетевого устройства была повреждена?
3. Когда температура достигла критического уровня?



5. Угрозы сканирования

Сканирование подсетей и хостов не обязательно имеет целью изучение структуры сети и поведения устройств с целью нанесения вреда, однако оно часто используется в разведывательных целях перед попыткой взлома сети и похищения конфиденциальных данных. Netwrix Auditor отслеживает эти действия и позволяет расследовать возможные инциденты и найти ответы на следующие вопросы:

1. Сканирование какого хоста или подсети было выполнено?
2. Когда были сделаны попытки сканирования?
3. С какого IP-адреса было запущено сканирование?
4. Сколько попыток сканирования было сделано с каждого IP-адреса?



О Netwrix Corporation

Компания Netwrix Corporation разрабатывает ПО, которое обеспечивает ИТ-отделам и отделам информационной безопасности возможности полного контроля поведения пользователей, конфигураций систем и конфиденциальности данных в любых гибридных ИТ-инфраструктурах, позволяя защитить данные, где бы они ни находились. Более 9000 организаций в разных странах используют решения Netwrix для выявления и своевременного устранения угроз безопасности данных, прохождения аудита на соответствие стандартам с меньшими затратами сил и средств, а также повышения эффективности работы ИТ-отделов. Компания Netwrix была основана в 2006 году. Она удостоена более чем 140 отраслевых наград и включена в списки самых быстрорастущих компаний в США «Inc. 5000» и «Deloitte Technology Fast 500».

Netwrix Auditor — это платформа, которая обеспечивает анализ поведения пользователей и снижение рисков, позволяя контролировать изменения, конфигурации и права доступа в гибридных ИТ-инфраструктурах для защиты данных, где бы они ни находились. Платформа обеспечивает сбор информации о безопасности для выявления уязвимостей и подозрительного поведения пользователей, а также своевременного расследования потенциальных угроз с целью предотвращения реального ущерба.

Netwrix Auditor включает в себя приложения для Active Directory, Azure AD, Exchange, Office 365, файловых серверов Windows, систем хранения данных EMC и NetApp, SharePoint, Oracle Database, SQL Server, VMware, Windows Server и сетевых устройств. Благодаря интеграции с RESTful API и возможности видеозаписи действий пользователей платформа обеспечивает полный контроль ситуации на локальной площадке и в облачных инфраструктурах.

Подробную информацию можно найти на веб-сайте www.netwrix.ru .

Локальное развертывание	Виртуальное устройство	Облачное развертывание
Загрузите 20-дневную пробную версию бесплатно	Загрузите образ виртуальной машины	Разверните Netwrix Auditor в облаке
netwrix.ru/auditor.html	netwrix.com/go/appliance	netwrix.com/go/cloud

Netwrix Россия: 197374, РФ, г. Санкт-Петербург, Торфяная дорога, д. 7, лит. Ф

Телефон: +7 (812) 309-54-98 **Европа:** +44 (0) 203-588-3023

netwrix.com/social