GIS ГАЗИНФОРМ СЕРВИС

Конституционный Суд
Российской Федерации

EFROS CONFIG INSPECTOR

Опыт использования

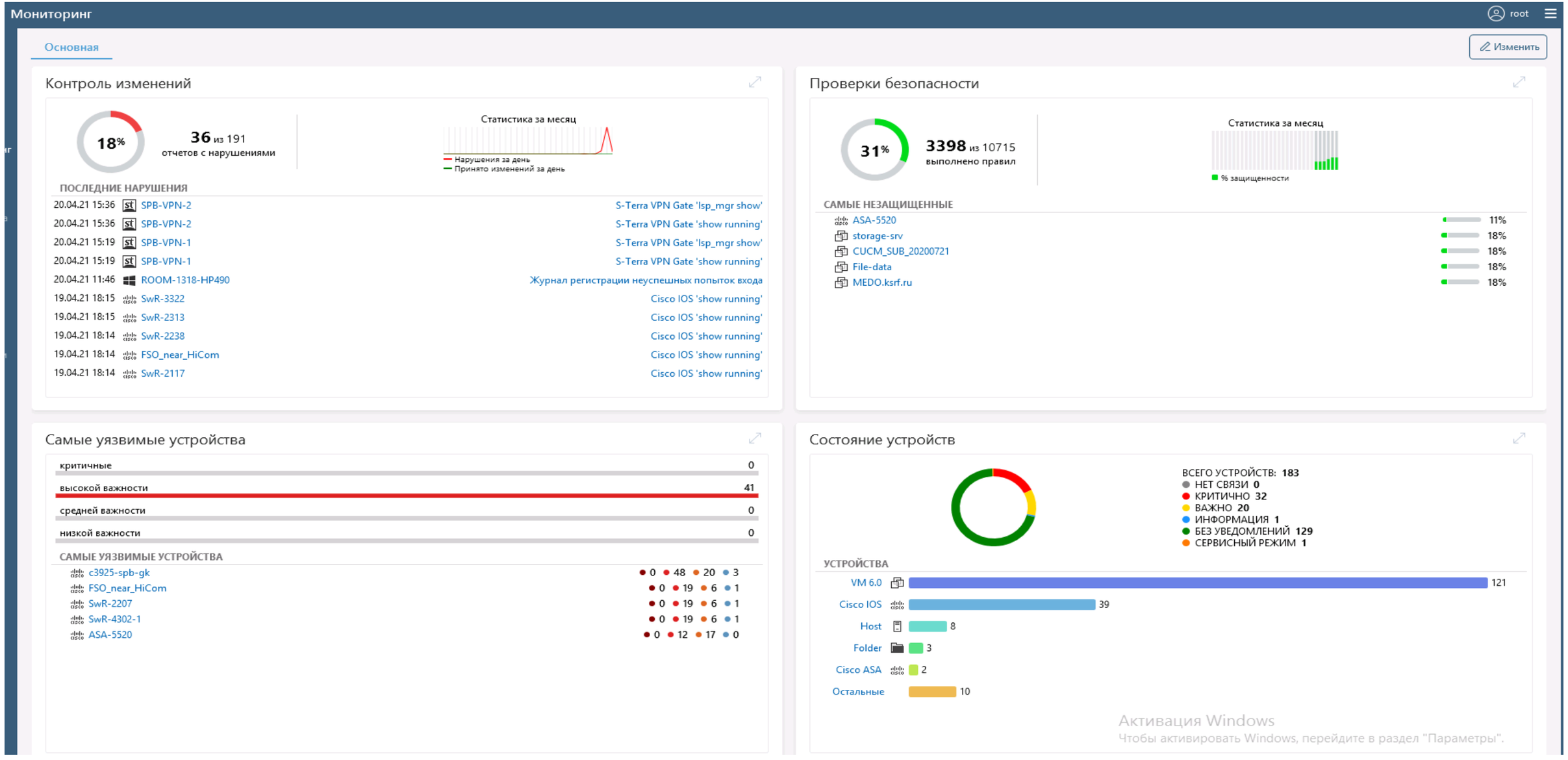
Самохин Иван Сергеевич
Заместитель начальника
Управления правовой информации

EFROS

CONFIG INSPECTOR

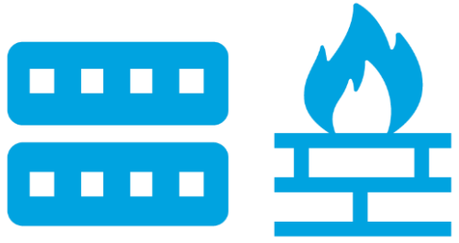
Контроль безопасности конфигураций и состояний сетевого оборудования, сред виртуализации, операционных систем, серверов, АРМ и др.

Графический интерфейс



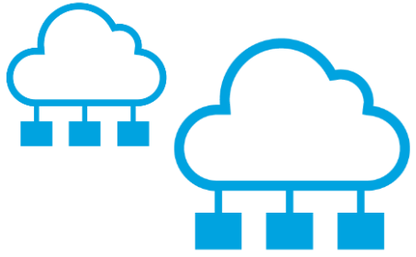
GIS ГАЗИНФОРМ СЕРВИС

Мониторинг изменений конфигураций сетевых устройств



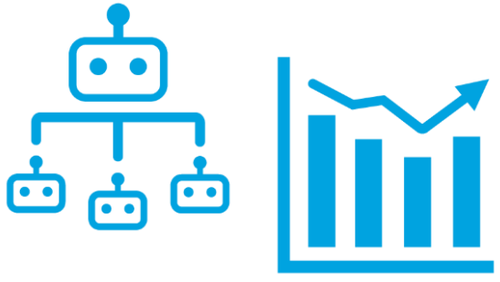
Контроль работоспособности

Доступность. Выход модулей из строя



Контроль изменений

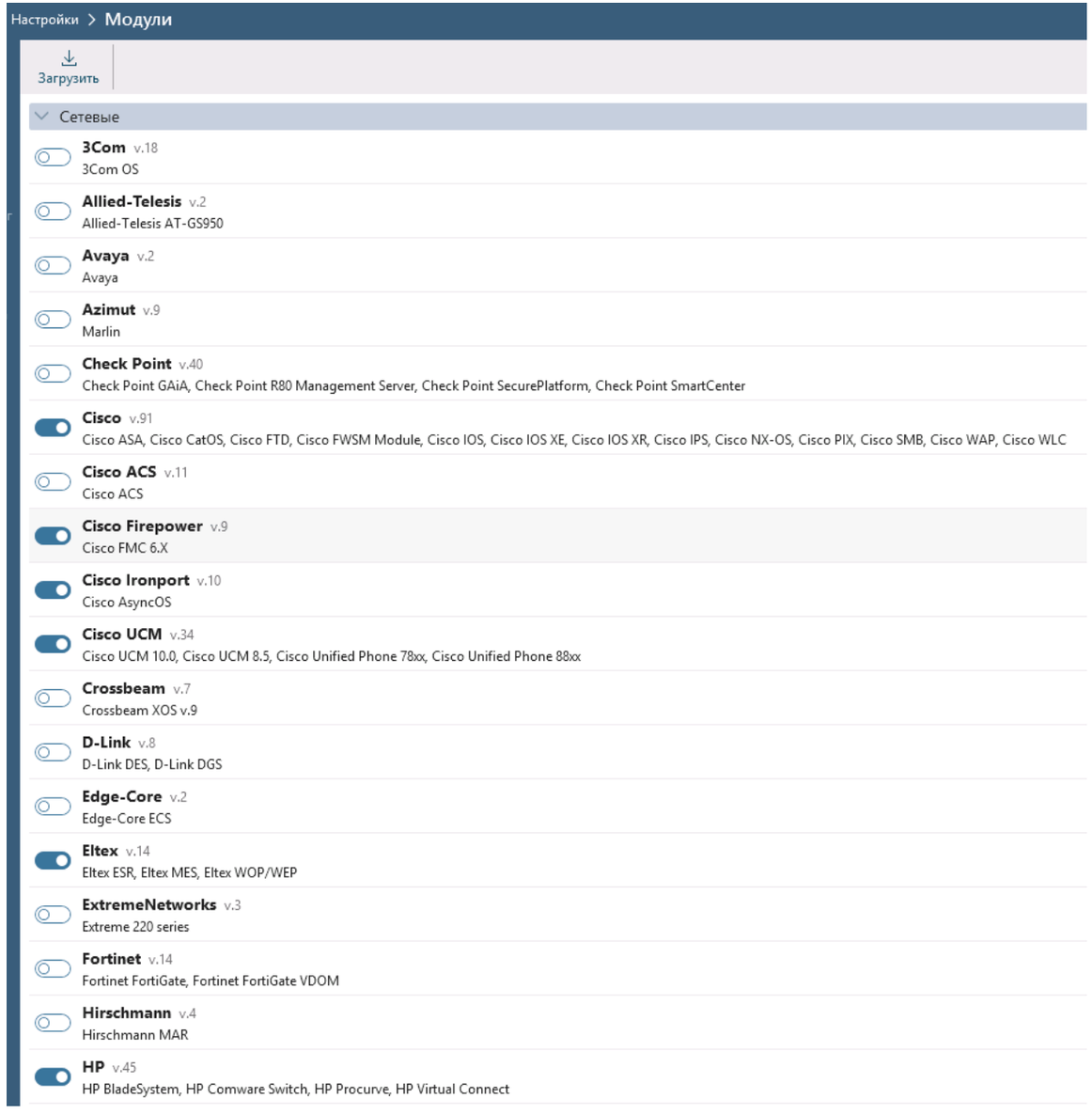
Отследить изменения выполненные другими сотрудниками или интеграторами



Наблюдаем за чем хотим

Можно создавать мониторинг своих команд

Используемые модули



GIS ГАЗИНФОРМ СЕРВИС

Используемые модули

ZyXEL v.8
ZyXEL ZyNOS

Полигон v.6
Полигон Арлан, Полигон ИнЗер

Фактор-ТС v.29
Dionis-LX, Dionis-NX 1.1, Dionis-NX 1.2, Dionis-NX 2.0

Виртуализация

Hyper-V v.14
Hyper-V 2008 R2 VM, Hyper-V 2008 R2 хост, Hyper-V 2008 R2 хост с контролем целостности, Hyper-V 2012 R2 VM, Hyper-V 2012 R2 хост, Hyper-V 2012 R2 хост с контролем целостности, Hyper-V 2016 VM, Hyper-V 2016 хост, Hyper-V 2016 хост с контролем целостности, Hyper-V 2019 VM, Hyper-V 2019 хост, Hyper-V 2019 хост с контролем целостности, SCVMM Group, Standalone Hyper-V 2008 R2, Standalone Hyper-V 2012 R2, Standalone Hyper-V 2016, Standalone Hyper-V 2019, Virtual Machine Manager 2008 R2, Virtual Machine Manager 2012 R2, Virtual Machine Manager 2016, Virtual Machine Manager 2019

vCenter v.24
Cluster, Datacenter, ESXi ОС с контролем файлов по HTTPS, ESXi ОС с контролем файлов по SSH, Folder, Host, Host с контролем целостности файлов по HTTPS, Host с контролем целостности файлов по SSH, Resource Pool, Standalone ESXi с контролем файлов по HTTPS, Standalone ESXi с контролем файлов по SSH, vApp, vCenter VCSA, vCenter Windows, VM 5.0, VM 5.1, VM 5.5, VM 6.0, VM 6.5

Операционные системы

Active Directory v.9
AD Domain

Citrix XenServer v.19
XenServer

Linux v.33
AIX, Astra Linux, FreeBSD, HP-UX, Linux, SunOS

Windows v.29
Сервер приема сообщений запущен.
Windows

Сервисные

SNMP Trap сервер v.1

Syslog сервер v.3

Отправка Syslog v.2

Отправка писем по протоколу SMTP v.3
Отправить тестовое сообщение

Отправка сообщений через MS Exchange v.4

Отправка сообщений через MS Lync v.3

Управление устройствами v.3

Экспорт событий v.3

GIS ГАЗИНФОРМ СЕРВИС

Изменение на межсетевых экранах в правилах

Отчет "Cisco ASA 'show running'" изменен и помещен в архив

Сводка события

Устройство:	SPB-ASA-CLUSTER открыть в консоли
Размещение:	cisco ASA
Профиль:	cisco asa
Время:	06.04.2020 21:00:31
Триггер:	Изменения контролируемых отчетов
Тип события:	Изменение отчета

Отчет "Cisco ASA 'show running'" изменен и помещен в архив.

Изменения:

```
-    object network Lenovo-monoblok
992   host 192.168.5.137
992   host 192.168.5.127
1010 object network room-1334
1011  host 192.168.9.214
1012  description Buranova M.G.
2479 access-list External_access_in extended permit tcp object Savyshkina77A_Zdobnikova object Zdobnikova eq 3389
3096 Cryptochecksum:256251753bf814499c45b1a86709f928
3094 Cryptochecksum:908f7b83ea6dd6a83052da03c32c4e95
```

Изменение на межсетевых экранах в правилах

Отчет "Cisco ASA 'show running'" изменен и помещен в архив

Сводка события

Устройство:	SPB-ASA-CLUSTER открыть в консоли
Размещение:	cisco ASA
Профиль:	cisco asa
Время:	11.04.2020 15:45:31
Триггер:	Изменения контролируемых отчетов
Тип события:	Изменение отчета

Отчет "Cisco ASA 'show running'" изменен и помещен в архив.

Изменения:

```
-    interface Port-channel1.7
142   shutdown
3440 Cryptochecksum:bbf41c21e3cc2b2423d9d1e37d61d26a
3439 Cryptochecksum:c567447123f2970bec1d6022d482578e
```

Уведомление о поломках в устройствах

Отчет "Cisco IOS команда "sh mod"" изменен и помещен в архив

Сводка события

Устройство:	Cisco_6509_R4503 открыть в консоли
Размещение:	cisco-ios
Профиль:	cisco switch 6509
Время:	04.07.2017 12:41:47
Триггер:	Изменения контролируемых отчетов
Тип события:	Изменение отчета

Отчет "Cisco IOS команда "sh mod"" изменен и помещен в архив.

Изменения:

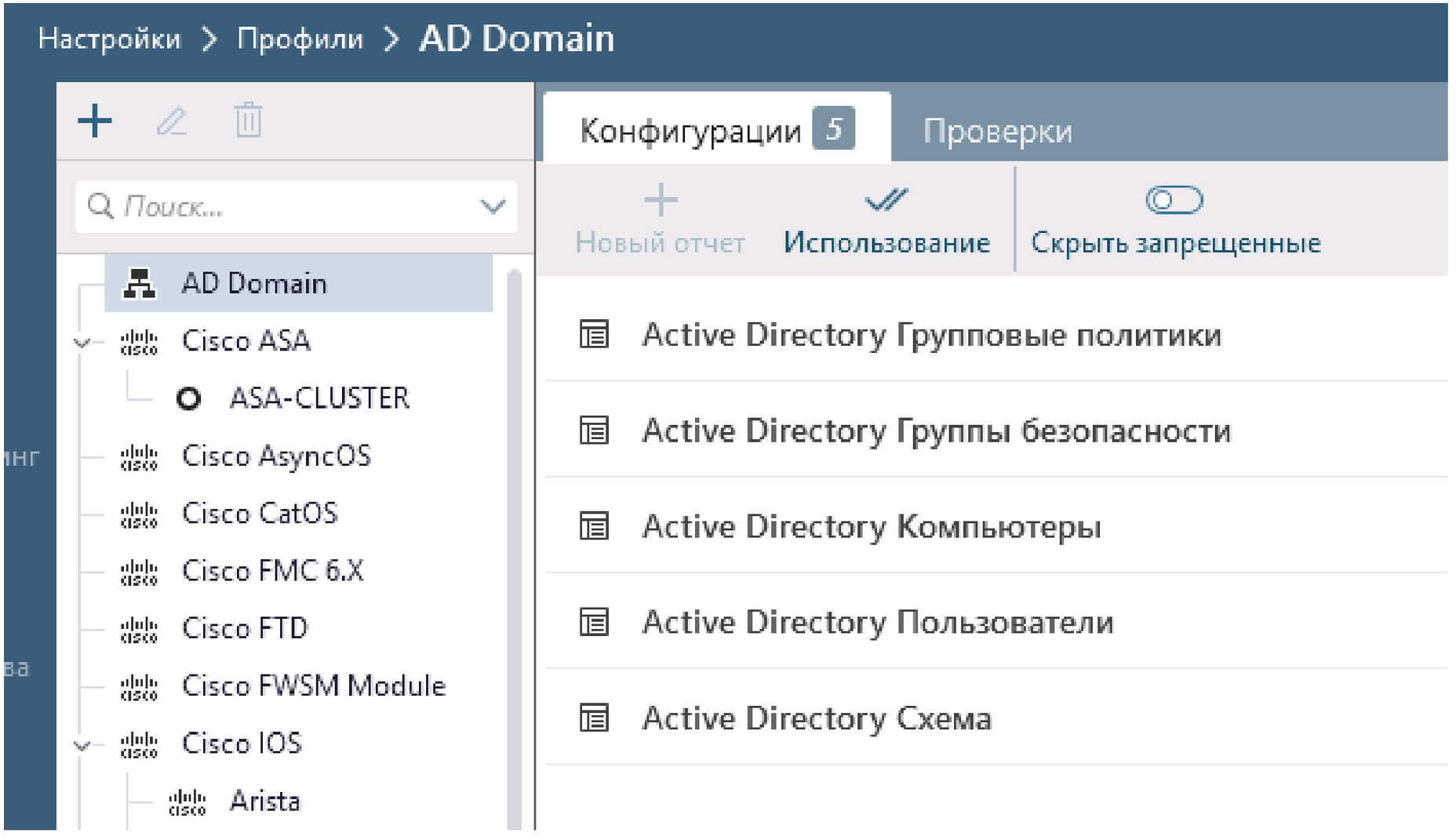
```
-  ---- -------------------------- -----------------
-  - ----------- ------- -------
   25   5  Policy Feature Card 3       WS-F6K-PFC3B
SAL11O1D1R2  2.3    Other
-  ---- -------------------
   35   5  Unknown
   34   5  Not Applicable
```

Детали события

Тип отчета:	Cisco IOS команда "sh mod"
Оповещение при изменении:	Да
Контроль целостности:	Пройден

GIS ГАЗИНФОРМ СЕРВИС

Мониторинг изменений в AD



GIS ГАЗИНФОРМ СЕРВИС

Контроль процесса обновления ОС на АРМ

Пт 15.01.2021 14:50

smev

Изменения контролируемых отчетов. Отчет "Active Directory Компьютеры" изменен и помещен в архив. Устройство: SPB-DC1.ksrf.ru

Кому   Самохин Иван Сергеевич; Андреев Максим М.

Отчет "Active Directory Компьютеры" изменен и помещен в архив

Сводка события

Устройство:	SPB-DC1.ksrf.ru открыть в консоли
Размещение:	AD
Профиль:	По умолчанию
Время:	15.01.2021 14:49:47
Триггер:	Изменения контролируемых отчетов
Тип события:	Изменение отчета

Отчет "Active Directory Компьютеры" изменен и помещен в архив.

Изменения:

- Компьютеры
  - Компьютер([illegible])

    Имя: 3408-B9H

    Операционная система: ~~Windows 7 Профессиональная~~ Windows 10 Pro

Детали события

Тип отчета:	Active Directory Компьютеры
Оповещение при изменении:	Да
Контроль целостности:	Нарушение

Все значения времени указаны в следующем часовом поясе: (UTC+03:00) Russian Standard Time

Сообщение отправлено ЭФРОС® Config Inspector

ГАЗИНФОРМ СЕРВИС

Контроль изменения имени АРМ в домене

Ответить Ответить всем Переслать

Пт 15.01.2021 14:20

smev

Изменения контролируемых отчетов. Отчет "Active Directory Компьютеры" изменен и помещен в архив. Устройство: SPB-DC1.ksrf.ru

Кому Самохин Иван Сергеевич; Андреев Максим М.

Отчет "Active Directory Компьютеры" изменен и помещен в архив

Сводка события

Устройство:	SPB-DC1.ksrf.ru открыть в консоли
Размещение:	AD
Профиль:	По умолчанию
Время:	15.01.2021 14:19:46
Триггер:	Изменения контролируемых отчетов
Тип события:	Изменение отчета

Отчет "Active Directory Компьютеры" изменен и помещен в архив.

Изменения:

- Компьютеры
  - Компьютер (f7b4f8a3-8491-4a1d-98b4-8a32f3a266f)
    - Имя: ~~ROOM-3408~~ 3408-B9H
    - DNS-имя: ~~room-3408.ksrf.ru~~ 3408-B9H.ksrf.ru
    - Имя компьютера(пред Windows 2000): ~~ROOM-3408$~~ 3408-B9H$

Детали события

Тип отчета:	Active Directory Компьютеры
Оповещение при изменении:	Да
Контроль целостности:	Нарушение

Все значения времени указаны в следующем часовом поясе: (UTC+03:00) Russian Standard Time
Сообщение отправлено ЭФРОС® Config Inspector

GIS ГАЗИНФОРМ СЕРВИС

Контроль создания, включения и отключения объектов

Чт 26.11.2020 11:24

smev

Изменения контролируемых отчетов. Отчет "Active Directory Пользователи"

Кому Самохин Иван Сергеевич

Отчет "Active Directory Пользователи" изменен и помещен в архив

Сводка события

Устройство:	SPB-DC1.ksrf.ru открыть в консоли
Размещение:	AD
Профиль:	По умолчанию
Время:	26.11.2020 11:23:51
Триггер:	Изменения контролируемых отчетов
Тип события:	Изменение отчета

Отчет "Active Directory Пользователи" изменен и помещен в архив.

Изменения:

- Пользователи
  - Пользователь (4458150e-8b71-45e7-b636-c02e1199417e)
    - Имя: HealthMailbox4458150e8b7145e7b636c02e1199417e
    - Имя входа: HealthMailbox4458150e8b7145e7b636c02e1199417e@ksrf.ru
    - Имя входа(пред Windows 2000): HealthMailbox4458150
    - Основная группа: Пользователи домена
    - Папка: ksrf.ru/Microsoft Exchange System Objects/Monitoring Mailboxes
    - Состояние
      - Доступен: Да
      - Заблокирован: Нет
      - Срок действия:
    - Член групп
      - Группа (3bda831ba1a8f244b7ddac45a0948e49)
        - Имя: Пользователи домена
        - Папка: ksrf.ru/Users
  - Пользователь (3b66538799034405915ff2aa37bee1fc)
    - Имя: HealthMailbox3b66538799034405915ff2aa37bee1fc
    - Имя входа: HealthMailbox3b66538799034405915ff2aa37bee1fc@ksrf.ru
    - Имя входа(пред Windows 2000): HealthMailbox3b66538
    - Основная группа: Пользователи домена
    - Папка: ksrf.ru/Microsoft Exchange System Objects/Monitoring Mailboxes
    - Состояние
      - Доступен: Да
      - Заблокирован: Нет
      - Срок действия:
    - Член групп
      - Группа (3bda831ba1a8f244b7ddac45a0948e49)
        - Имя: Пользователи домена
        - Папка: ksrf.ru/Users

Отчет "Active Directory Компьютеры" изменен и помещен в архив

Сводка события

Устройство:	SPB-DC1.ksrf.ru открыть в консоли
Размещение:	AD
Профиль:	По умолчанию
Время:	18.11.2020 12:40:24
Триггер:	Изменения контролируемых отчетов
Тип события:	Изменение отчета

Отчет "Active Directory Компьютеры" изменен и помещен в архив.

Изменения:

- Компьютеры
  - Компьютер (375321ff-f140-444f-ba36-a2b131c96894)
    - Имя: ELISEEV
    - Операционная система: ~~Windows 7 Профессиональная~~ Windows 10 Pro
  - Компьютер (f07d3b8a-5855-4d43-b2d4-aa3da93c8080)
    - Имя: VGATE
    - DNS-имя: vgate.ksrf.ru
    - Имя компьютера(пред Windows 2000): VGATE$
    - Операционная система: Windows Server 2016 Standard
    - Основная группа: Компьютеры домена
    - Папка: ksrf.ru/Computers
    - Состояние
      - Доступен: Да
      - Заблокирован: Нет
      - Срок действия:
    - Член групп
      - Группа (07144cc9582004478d1451a22f0c1307)
        - Имя: Компьютеры домена
        - Папка: ksrf.ru/Users

GIS ГАЗИНФОРМ СЕРВИС

Изменения членства в группах

Отчет "Active Directory Компьютеры" изменен и помещен в архив

Сводка события

Устройство:	SPB-DC1.ksrf.ru открыть в консоли
Размещение:	AD
Профиль:	По умолчанию
Время:	26.11.2020 09:53:52
Триггер:	Изменения контролируемых отчетов
Тип события:	Изменение отчета

Отчет "Active Directory Компьютеры" изменен и помещен в архив.

Изменения:

- Компьютеры
  - Компьютер (14386330-bbfa-4432-8682-48a697a873fa)
    - Имя: SPB-EXCH2
    - Член групп
      - Группа (a0084a0f93f4a84f9c00fabb153404a9)
        - Имя: Managed Availability Servers
        - Папка: ksrf.ru/Microsoft Exchange Security Groups
      - Группа (a04d34d4a17015468b7bd42150111728)
        - Имя: Exchange Install Domain Servers
        - Папка: ksrf.ru/Microsoft Exchange System Objects
      - Группа (48a894084a878343a4df5a853a1cc3fb)
        - Имя: Exchange Trusted Subsystem
        - Папка: ksrf.ru/Microsoft Exchange Security Groups
      - Группа (42ccf8795483bf041b704ca8ca0881f4c)
        - Имя: Exchange Servers
        - Папка: ksrf.ru/Microsoft Exchange Security Groups

Изменения членства в группах

Отчет "Active Directory Пользователи" изменен и помещен в архив

Сводка события

Устройство:	SPB-DC1.ksrf.ru открыть в консоли
Размещение:	AD
Профиль:	По умолчанию
Время:	25.11.2020 12:37:10
Триггер:	Изменения контролируемых отчетов
Тип события:	Изменение отчета

Отчет "Active Directory Пользователи" изменен и помещен в архив.

Изменения:

- Пользователи
  - Пользователь (47a2125d-919b-4230-bf83-a084cd9a0716)
    - Имя: Зиновьева Елена Сергеевна
    - Член групп
      - Группа (b342d65f877aa74d8490bbaaaffbc9c4)
        - Имя: ESA Mobile Application Users
        - Папка: ksrf.ru/ESET Secure Authentication
  - Пользователь (d0220dcf-a4a7-410c-b9aa-37acd0fbd5f2)
    - Имя: sptest
    - Состояние
      - Доступен: ~~Да~~ Нет

Контроль изменения OU

Отчет "Active Directory Компьютеры" изменен и помещен в архив

Сводка события

Устройство:	SPB-DC1.ksrf.ru открыть в консоли
Размещение:	AD
Профиль:	По умолчанию
Время:	22.11.2020 22:02:48
Триггер:	Изменения контролируемых отчетов
Тип события:	Изменение отчета

Отчет "Active Directory Компьютеры" изменен и помещен в архив.

Изменения:

- Компьютеры
  - Компьютер (3c1839a3-f12b-414a-b283-10caa0ca4cd5)
    Имя: ROOM-1314
    Папка: ~~ksrf.ru/APM в домене~~ ksrf.ru/Отключенные APM
  - Компьютер (4a831862-3a8c-4760-8d2a-90df6c3332a3)
    Имя: EXCH16-1
    Папка: ~~ksrf.ru/Computers~~ ksrf.ru/Servers
  - Компьютер (ac7f2853-348c-4d92-879d-b760c18cb151)
    Имя: EXCH16-2
    Папка: ~~ksrf.ru/Computers~~ ksrf.ru/Servers
  - Компьютер (342497f4-6a61-43fb-a9ca-a5667cb7a898)
    Имя: DAG16
    Папка: ~~ksrf.ru/Computers~~ ksrf.ru/Servers
  - Компьютер (f07d3b8a-3855-4d63-b2d4-aa3da93c8080)
    Имя: VGATE
    Папка: ~~ksrf.ru/Computers~~ ksrf.ru/Servers
  - Компьютер (617d9c07-9ab9-4112-a94d-30da014a67c8)
    Имя: 1314-BDM
    Папка: ~~ksrf.ru/Computers~~ ksrf.ru/APM в домене

Сводка события

Устройство:	SPB-DC1.ksrf.ru открыть в консоли
Размещение:	AD
Профиль:	По умолчанию
Время:	18.11.2020 01:24:28
Триггер:	Изменения контролируемых отчетов
Тип события:	Изменение отчета

Отчет "Active Directory Пользователи" изменен и помещен в архив.

Изменения:

- Пользователи
  - Пользователь (78ff2c2a0-a304-4d1a-9844-b23320a959cc)
    Имя: Царькова Светлана Геннадьевна
    Папка: ~~ksrf.ru/Сотрудники~~ ksrf.ru/Отключенные пользователи
  - Пользователь (1a1a2895-001b-4d31-baa2-61a2f0996f74)
    Имя: Филиппова Ирина Никитична
    Папка: ~~ksrf.ru/Сотрудники~~ ksrf.ru/Отключенные пользователи
  - Пользователь (2712ab75-7130-4105-9c01-a957a58f886f)
    Имя: Япрынцев Иван Михайлович
    Папка: ~~ksrf.ru/Сотрудники~~ ksrf.ru/Отключенные пользователи

Мониторинг состояния виртуализации

Отчет "VMware vSphere Дерево иерархии" изменен и помещен в архив.

Изменения:

Inventory Tree

Inventory Tree

- Datacenters (group-d1)
  Folder
  - KSRF_SPB (datacenter-2)
    Datacenter
    - Hosts (group-h4)
      Folder
      - Cluster (domain-c36)
        Cluster
        - vmwared1.ksrf.ru (host-10190)
          Host
        - vmwared1.ksrf.ru (host-10399)
          Host
    - Datastores (group-s5)
      Folder
      - ARM_BACKUP (datastore-3430)
        Datastore
        - Host mounts
          Hosts attached to this datastore
          - vmwared1.ksrf.ru (host-10399)
            Host Mount

            name: vmwared1.ksrf.ru
            host name
            path: /vmfs/volumes/5dadbbe5-8c5953d8-3511-9840bbcb51d8
            Local file path where file system volume is mounted, if applicable
            Access mode: readWrite
            Access mode to the underlying file system for this host
            mounted: Да
            The mount state of this mount point
            accessible: Да
            Flag that indicates if the datastore is currently accessible from the host
          - vmwared1.ksrf.ru (host-10190)
            Host Mount

            name: vmwared1.ksrf.ru
            host name
            path: /vmfs/volumes/5dadbbe5-8c5953d8-3511-9840bbcb51d8
            Local file path where file system volume is mounted, if applicable
            Access mode: readWrite
            Access mode to the underlying file system for this host
            mounted: Да
            The mount state of this mount point
            accessible: Да
            Flag that indicates if the datastore is currently accessible from the host

Создание и удаление виртуальных машин
Проблемы в связи с СХД по FC

Изменения:

Inventory Tree

Inventory Tree

- Datacenters (group-d1)
  Folder
  - KSRF_SPB (datacenter-2)
    Datacenter
    - Hosts (group-h4)
      Folder
      - Cluster (domain-c34)
        Cluster
        - vmwared6.ksrf.ru (host-48)
          Host
    - Datastores (group-s3)
      Folder
      - ARM_BACKUP (datastore-3450)
        Datastore
        - Host mounts
          Hosts attached to this datastore
          - vmwared6.ksrf.ru (host-48)
            Host Mount

            name: vmwared6.ksrf.ru
            host name
            path: /vmfs/volumes/5dadbbe5-8c5953d8-3511-9840bbcb51d8
            Local file path where file system volume is mounted, if applicable
            Access mode: readWrite
            Access mode to the underlying file system for this host
            mounted: Да
            The mount state of this mount point
            accessible: Да
            Flag that indicates if the datastore is currently accessible from the host
      - DataFX (datastore-61)

Отчет "VMware vSphere Дерево иерархии" изменен и помещен в архив.

Изменения:

Inventory Tree

Inventory Tree

- Datacenters (group-d1)
  Folder
  - KSRF_SPB (datacenter-2)
    Datacenter
    - Networks (group-n6)
      Folder
      - PortGroupSQL_node1.1 (network-10340)
        Network
      - PortGroupWIN_MNGMNT (network-10192)
        Network
    - Virtual Machines (group-v8)
      Folder
      - Discovered virtual machine (group-v10189)
        Folder
        - SQL-Node1-1.ksrf.ru (vm-10194)
          Virtual Machine
          - Networks
            A collection of references to the subset of network
            - VM Network (network-11)
              Network
            - PortGroupSQL_node1.1 (network-10340)
              Network

ГАЗИНФОРМ СЕРВИС

Создание виртуальных машин

Изменения:

Inventory Tree

Inventory Tree

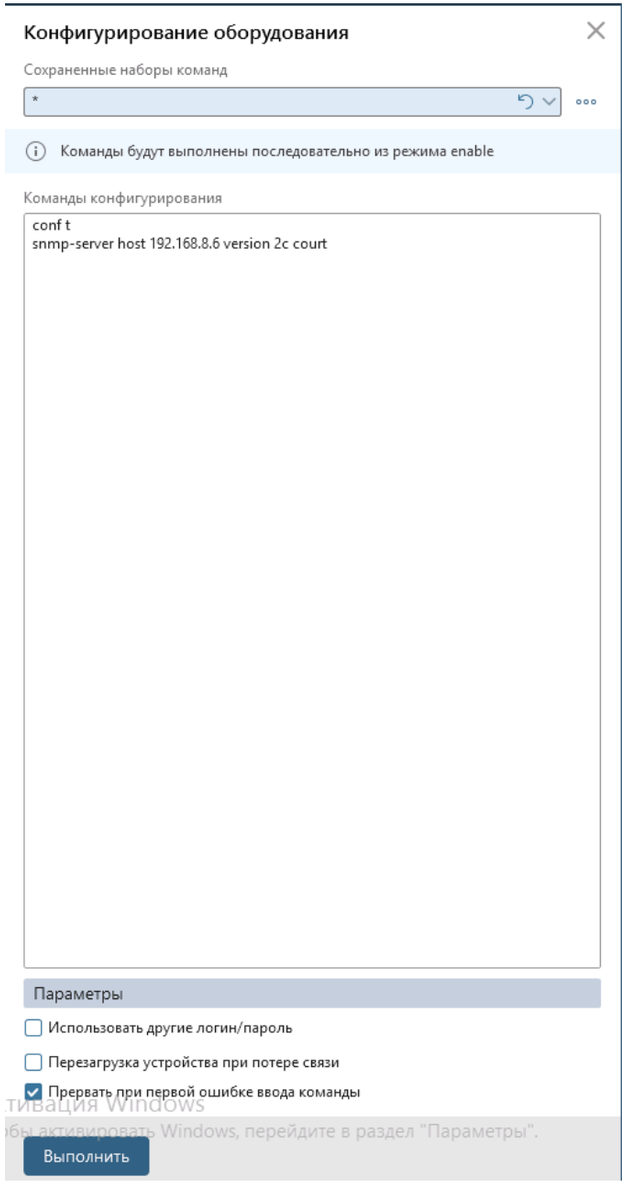
- Datacenters (group-d1)
  Folder
  - KSRF_SPB (datacenter-2)
    Datacenter
    - Virtual Machines (group-v6)
      Folder
      - mind (vm-4892)
        Virtual Machine
        - Networks
          A collection of references to the subset of network objects in the datacenter that is used by this virtual machine
          - VM Network (network-11)
            Network
        - Datastores
          Attached datastores
          - DataFX (datastore-41)
            Datastore

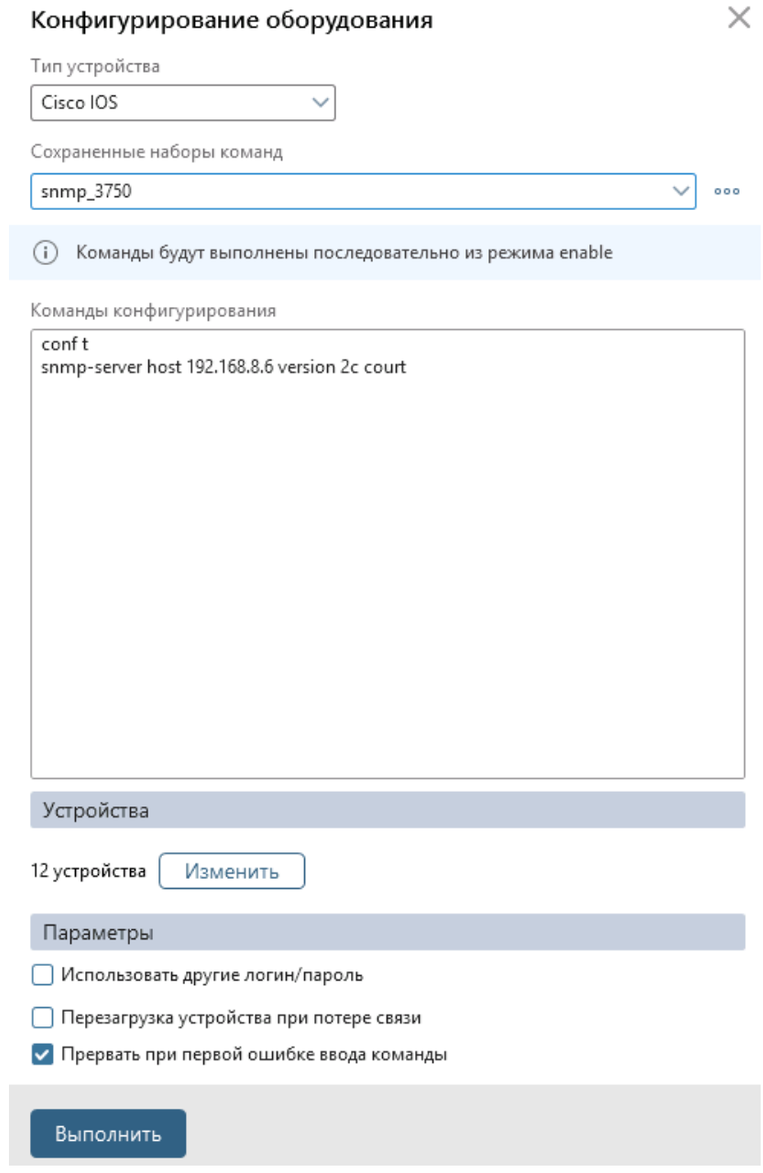
Упрощение администрирования оборудования

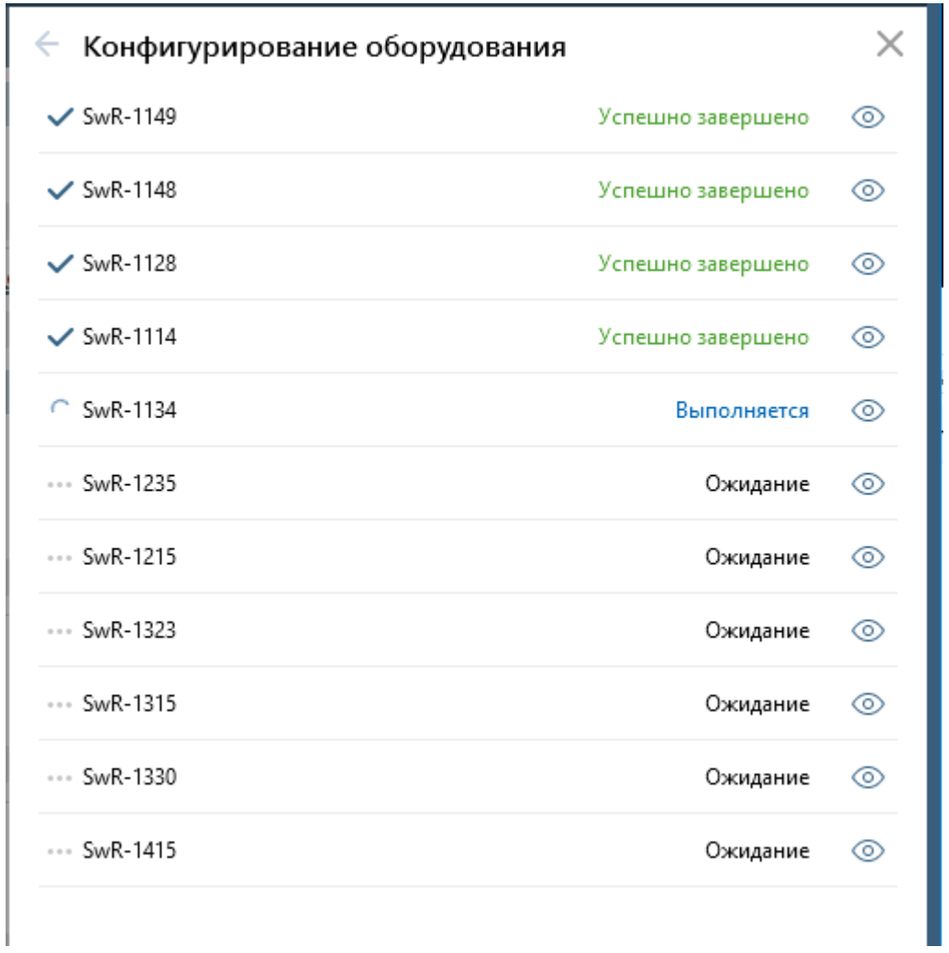
Быстрый доступ к устройству по ssh http/https telnet

GIS ГАЗИНФОРМ СЕРВИС

Конфигурация устройства и группы устройств







Проверка политик безопасности

Проверка политик CIS для Cisco IOS

19.04.2021 10:21:54 (17 мин. назад)

52% (45 из 85)

SwR-4505

Отчет | История изменений

Экспорт | Обновить | Настройки | Свернуть все | Только нарушения | Сравнить | Поиск...

Локальная аутентификация, авторизация и учёт (AAA) Пройдено 5 из 12

- ✓ Необходимо включить централизованный сервис AAA
- ✓ Необходима локальная аутентификация AAA при входе на устройство
- ✓ Необходима локальная аутентификация AAA для режима администрирования
- ✓ Необходима AAA аутентификация для консоли и линий VTY
- ✗ Необходимо задать пароль для режима администрирования

  Описание: Необходимо использовать надёжный пароль для входа в режим администрирования. По умолчанию использование пароля не используется: пользователь входит в привилегированный режим путём нажатия клавиши "Enter" после команды enable. Команда enable secret применяет криптографический хэш-алгоритм MD5, который лучше защищает систему, чем пароли уровня 7.
  Проверка: hostname#sh run | incl enable secret
  Настройка: hostname(config)#enable secret <ENABLE_SECRET>

  Дополнительно: Не задан enable secret!

- ✗ Необходима включить AAA аутентификацию для режима администрирования
- ✓ Необходима AAA аутентификация для входа на устройство
- ✗ Необходимо настроить учет команд AAA
- ✗ Необходимо настроить учет соединений при помощи AAA-сервиса
- ✗ Необходимо настроить учет пользовательского режима (Exec) с использованием AAA
- ✗ Необходимо настроить учет сетевых событий с использованием AAA
- ✗ Необходимо настроить учет системных событий с использованием AAA

Доступ к устройству Пройдено 3 из 5

- ✓ Необходимо установить пользователям уровень привилегий
- ✓ Необходимо использовать SSH для линий VTY

GIS ГАЗИНФОРМ СЕРВИС

Проверка политик безопасности

- ✗ Необходимо установить таймаут для сессий пользователей
- ✓ Необходимо закрыть порт AUX
- ✗ Необходимо настроить ACL для линий VTY

Баннеры Пройдено 0 из 3

- ✗ Необходимо задать баннер EXEC
- ✗ Необходимо задать баннер входа
- ✗ Необходимо задать баннер сообщения дня

Пароли Пройдено 2 из 3

- ✓ Необходимо использовать сервис шифрования паролей
- ✗ Необходимо использовать пароли, привязанные к линиям
- ✓ Необходимо шифровать пароли пользователей

SNMP Пройдено 5 из 9

- ✗ Необходим запрет на использование протокола SNMP
- ✓ Необходим запрет на использование в SNMP community строки "private"
- ✓ Необходим запрет на использование в SNMP community строки "public"
- ✓ Необходим запрет доступа по протоколу SNMP с правами на запись
- ✓ Необходим запрет доступа по протоколу SNMP без ACL
- ✗ Необходим запрет использования SNMP trap
- ✗ При использовании SNMP, необходимо настроить SNMP trap сервер
- ✓ Необходимо разрешить отправку SNMP trap, если определен сервер SNMP
- ✗ Требуется настроить группы для доступа по протоколу SNMP v3

Настройки времени Пройдено 1 из 1

- ✓ Необходимо настроить запрет перехода на летнее время

Глобальные сервисы Пройдено 13 из 16

- ✗ Требуется отключить Cisco Discovery Protocol (CDP)
- ✓ Требуется отключить Packet Assembler/Disassembler сервис
- ✓ Требуется отключить сервис Finger
- ✗ Требуется отключить IP BOOTP сервер
- ✓ Требуется отключить сервер identd
- ✓ Требуется отключить HTTP сервер
- ✓ Требуется отключить HTTPS сервер
- ✓ Требуется отключить удаленную загрузку конфигурации
- ✓ Требуется включить сервис TCP keepalive in
- ✓ Требуется включить сервис TCP keepalive out
- ✓ Требуется отключить tcp small servers

Проверка политик безопасности

- ✓ Требуется отключить udp small servers
- ✓ Требуется отключить TFTP сервер
- ✓ Требуется задать имя устройства
- ✓ Требуется задать имя домена
- ✗ Необходимо запретить ARP прокси на каждом интерфейсе

Настройка протоколов удалённого доступа Пройдено 3 из 3

- ✓ Требуется задать таймаут SSH сессии
- ✓ Требуется задать количество попыток ввода пароля при подключении по SSH
- ✓ Требуется использовать вторую версию протокола SSH

Регистрация событий Пройдено 6 из 8

- ✓ Необходимо включить регистрацию событий
- ✓ Требуется включить логирование в буфер
- ✗ Требуется настроить логирование в консоль устройства
- ✓ Требуется включить логирование на syslog сервер
- ✓ Требуется установить уровень важности сообщений syslog trap
- ✗ Требуется привязать loopback интерфейс к службе syslog
- ✓ Требуется включить отображение временных времени для debug сообщений
- ✓ Требуется включить сервис отметок времени для log сообщений

Служба времени (NTP) Пройдено 1 из 5

- ✓ Требуется настроить подключение к нескольким NTP серверам
- ✗ Требуется настроить аутентификацию с серверами времени (NTP)
- ✗ Требуется настроить ключи шифрования для работы с NTP-серверами
- ✗ Требуется задать доверенный ключ для аутентификации с NTP-серверами
- ✗ Требуется привязать шифрованный ключ для каждого сервера NTP

Маршрутизация Пройдено 2 из 5

- ✓ Требуется запретить направленный broadcast на каждом интерфейсе
- ✗ Требуется запретить IP маршрутизацию от источника
- ✗ Необходимо включить Cisco Express Forwarding
- ✗ Необходимо включить Unicast Reverse-Path Forwarding на каждом интерфейсе
- ✓ Необходимо запретить туннельные интерфейсы

Loopback-интерфейс Пройдено 3 из 5

- ✓ Необходимо настроить loopback интерфейс
- ✓ Необходимо настроить только один loopback интерфейс
- ✓ Необходимо привязать AAA к loopback интерфейсу
- ✗ Необходимо привязать сервис NTP к loopback интерфейсу

Проверка политик безопасности

- ✗ Необходимо привязать TFTP-сервис к loopback интерфейсу

Фильтрация трафика Пройдено 0 из 3

- ✗ Необходимо при помощи ACL запретить попадание в сеть пакетов с внутренними IP адресами из сети Интернет
- ✗ Необходим контроль исходящего трафика на внешних интерфейсах при помощи ACL
- ✗ Необходим контроль входящего трафика на внешних интерфейсах при помощи ACL

Аутентификация в протоколах маршрутизации Пройдено 1 из 7

- ✓ Необходима аутентификация для каждого соседа BGP
- ✗ Необходим интерфейс с настроенной аутентификацией по цепочке ключей для EIGRP
- ✗ Необходим интерфейс с настроенным типом аутентификации для протокола EIGRP
- ✗ Необходима аутентификация message-digest для OSPF
- ✗ Необходим интерфейс с настроенной аутентификацией message-digest для OSPF
- ✗ Необходим интерфейс с настроенной аутентификацией по цепочке ключей для RIP v2
- ✗ Необходим интерфейс с настроенным типом аутентификацией для RIP v2

GIS ГАЗИНФОРМ СЕРВИС

Отчет по уязвимостям

Уязвимости Cisco IOS

19.04.21 10:22 (25 мин. назад)

0 8 4 0 всего: 12

SwR-4505

Отчет | История изменений

Экспорт | Свернуть | Раскрыть | Сравнить | Поиск...

8,3 vuln-CVE-2020-3217

A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device.
The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition.
Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.
This advisory is available at the following link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-nxos-onepk-rce-6Hhyt4dC ["https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-nxos-onepk-rce-6Hhyt4dC"]
This advisory is part of the June 3, 2020, release of the Cisco IOS and IOS XE Software Security Advisory Bundled Publication, which includes 23 Cisco Security Advisories that describe 25 vulnerabilities. For a complete list of the advisories and links to them, see Cisco Event Response: June 2020 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication [" http://tools.cisco.com/security/center/viewErp.x?alertId=ERP-73388"].

Версия совпадает с указанной. 15.2(4)E7

cisco cisco-sa-ios-nxos-onepk-rce-6Hhyt4dC
cve CVE-2020-3217
fstec BDU:2020-02762

AV:A/AC:L/Au:N/C:C/I:C/A:C

7,8 Catalyst 4000 Series TCP Denial of Service Vulnerability

7,8 vuln-CVE-2020-3228

7,6 Cisco IOS and Cisco IOS XE Software Web UI Cross-Site Request Forgery Vulnerability

7,2 vuln-CVE-2020-3204

6,8 vuln-CVE-2020-3200

6,5 Cisco IOS and IOS XE Software Cluster Management Protocol Denial of Service Vulnerability

6,3 vuln-CVE-2020-3235

5,8 Cisco IOS and IOS XE Software HTTP Client Information Disclosure Vulnerability

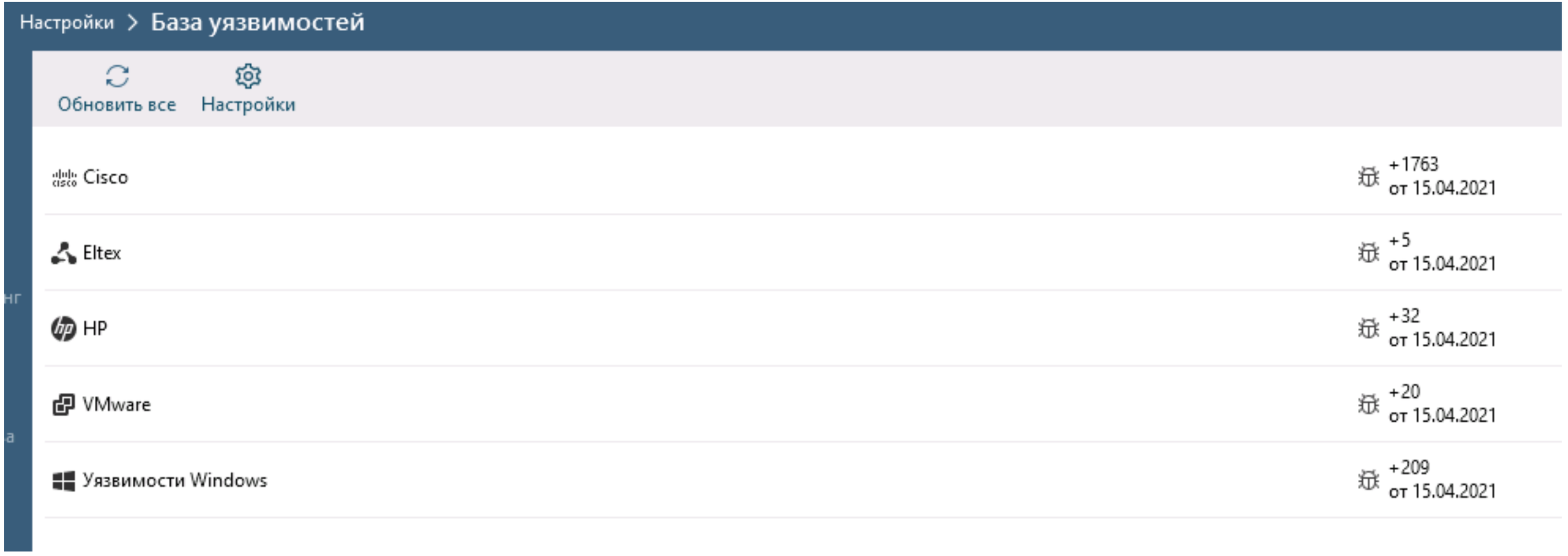
5,0 vuln-CVE-2020-3230

3,3 Cisco IOS and IOS XE HSRP Information Leak Vulnerability

2,1 vuln-CVE-2020-3477

GIS ГАЗИНФОРМ СЕРВИС

Автоматическое обновление баз уязвимостей



GIS ГАЗИНФОРМ СЕРВИС

GIS ГАЗИНФОРМ СЕРВИС

Спасибо за внимание!

Самохин Иван Сергеевич

Заместитель начальника

Управления правовой информации

Конституционный Суд
Российской Федерации