



**АКЦИОНЕРНОЕ ОБЩЕСТВО «ТРАНССЕТЬ»
(АО «Транссеть»)**

ТРАНССЕТЬ. ЕДИНАЯ СИСТЕМА КОНТРОЛЯ

**Руководство Пользователя
(Материалы)**

2020

СОДЕРЖАНИЕ

1 ОБЩИЕ ПОЛОЖЕНИЯ	4
1.1 Наименование системы.....	4
1.2 Назначение и цели разработки системы	4
1.2.1 Назначение системы.....	4
1.2.2 Цели разработки системы.....	4
1.3 Требования к оборудованию и программному обеспечению.....	4
1.4 Требования к квалификации пользователей.....	5
1.5 Перечень условных обозначений и сокращений	5
2 ОПИСАНИЕ ПРОГРАММНОГО ПРОДУКТА	11
2.1 Структура ТЕСК и назначение её частей.....	11
2.1.1 Ядро мониторинга	11
2.1.2 Модули ТЕСК	12
3 ПОДГОТОВКА К РАБОТЕ	14
3.1 Роли пользователей.....	14
3.2 Права доступа	14
3.3 Установка программного обеспечения	14
3.4 Состав и содержание дистрибутивного носителя данных	14
3.5 Загрузка приложения	14
4 ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ	16
4.1 Боковая панель.....	16
4.2 Информационные панели	22
4.2.1 Настройка информационной панели	22
4.2.2 Добавление элемента на информационную панель.....	24
4.2.3 Создание новой информационной панели	26
5 ОПИСАНИЕ ОПЕРАЦИЙ	28
5.1 Настройка Хостов.....	29
5.1.1 Просмотр свойств хоста.....	29
5.1.2 Создание хоста.....	31
5.1.3 Проверка настроек хоста	32
5.1.4 Просмотр статуса хоста	34
5.1.5 Поиск хостов по заданным параметрам.....	35
5.1.6 Массовое редактирование хостов.....	37
5.1.7 Импорт и экспорт хостов в CSV	39
5.1.8 Настройка хостов при распределенном мониторинге	41
5.1.9 Создание нового кластера	42
5.2 Настройка Сервисов.....	43
5.2.1 Просмотр сервисов.....	43
5.2.2 Конфигурирование сервисов.....	44
5.2.3 Удаление нежелательных сервисов	45

5.2.4	Настройка сервисов вручную	47
5.2.5	Пассивные сервисы	47
5.3	Обработка аварий	48
5.3.1	Процедура подтверждения	48
5.3.2	Отображение подтверждения в ТЕСК	49
5.4	НАСТРОЙКА КОНСОЛИ СОБЫТИЙ	50
5.4.1	Просмотры событий	50
5.4.2	Команды и рабочий процесс в событиях	51
5.4.3	Видимость событий	53
5.4.4	Просмотр состояний событий в активном мониторинге	53
5.4.5	Переадресация Консоли Событий «Logwatch»	54
ПЕРЕЧЕНЬ РИСУНКОВ		59
ПЕРЕЧЕНЬ ТАБЛИЦ		62

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Наименование системы

Полное наименование системы: Транссеть. Единая Система Контроля.

Условное наименование системы: ТЕСК, Система.

1.2 Назначение и цели разработки системы

1.2.1 Назначение системы

ТЕСК предназначена для контроля работоспособности критических ИС ИТ-инфраструктуры, а также контроля качества предоставления ИТ-услуг, необходимых для выполнения бизнес-процессов Заказчика, путем сбора, хранения и анализа данных о состоянии связанных с ними ИТ-ресурсов.

ТЕСК содержит компоненты, реализующие функции ведения структурированного учёта событий, аварийных ситуаций, своевременного оповещения о данных событиях и аварийных ситуациях. Компоненты ТЕСК предоставляют удобный графический интерфейс для ведения оперативного контроля за оборудованием.

1.2.2 Цели разработки системы

Целями разработки ТЕСК являются:

- Повышение качества и оперативности работ по обнаружению и анализу событий в ИС;
- Снижение уровня непредвиденных затрат за счет получения актуальных данных о состоянии и работоспособности ИТ-ресурсов;
- Сокращение сроков проведения, выполняемых в рамках технологического цикла по эксплуатации ИТ-ресурсов и повышение их качества;
- Автоматизация учета сетевых ресурсов;
- Снижение затрат на проведение операций инвентаризации ИТ-ресурсов;
- Повышение эффективности использования ИТ-ресурсов.

1.3 Требования к оборудованию и программному обеспечению

Требования к аппаратно-программному обеспечению ТЕСК приведены в документе «Общее описание системы», входящем в комплект документации на ТЕСК.

1.4 Требования к квалификации пользователей

Настоящее Руководство ориентировано на пользователей, владеющих основными навыками работы в операционной системе MS Windows и unix - подобными ОС.

1.5 Перечень условных обозначений и сокращений

Термины и сокращения представлены в Табл. 1.1.

Табл. 1.1 - Термины и сокращения

Наименование термина/сокращения	Описание
ASCII-символы	Символы таблицы ASCII
Business Intelligence, BI	Бизнес-агрегации. Логическое объединение объектов мониторинга для получения конкретных представлений о качестве оказываемой бизнес-услуги в разрезе информационного обеспечения
CPU	Центральный процессор (англ. central processing unit) – электронный блок, либо интегральная схема (микропроцессор), исполняющая машинные инструкции (код программы), главная часть аппаратного обеспечения компьютера или программируемого логического контроллера
CSV	(англ. Comma-Separated Values — значения, разделённые запятыми) — текстовый формат, предназначенный для представления табличных данных
DNS-имя	Символьное имя, которое выступает в роли уникального идентификатора, который присваивается определенному IP-адресу (двух одинаковых быть не может)
FTP	(англ. File Transfer Protocol) — протокол передачи файлов по сети, используется для распространения ПО и доступа к удалённым хостам
HTML	(англ. HyperText Markup Language — «язык гипертекстовой разметки») — стандартизированный язык разметки документов

Табл. 1.1 - Термины и сокращения

Наименование термина/сокращения	Описание
HTTP	(англ. HyperText Transfer Protocol — «протокол передачи гипертекста») — протокол прикладного уровня передачи данных изначально в виде гипертекстовых документов в формате «HTML», в настоящий момент используется для передачи произвольных данных
ID	Уникальный идентификатор объекта, позволяющий отличать его от других объектов
IMAP	(англ. Intelligent Platform Management Interface) — интеллектуальный интерфейс управления платформой, предназначенный для автономного мониторинга и управления функциями, встроенными непосредственно в аппаратное и микропрограммное обеспечения серверных платформ
IP-адрес	Уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP
ICMP	(англ. Internet Control Message Protocol — протокол межсетевых управляющих сообщений) — сетевой протокол, входящий в стек протоколов TCP/IP
Master	(англ.) — главный экземпляр TЕСK при настроенном распределенном мониторинге, который может самостоятельно запрашивать данные у подчиненных экземпляров
SCSI	(англ. Small Computer System Interface) — представляет собой набор стандартов для физического подключения и передачи данных между компьютерами и периферийными устройствами. SCSI-стандарты определяют команды, протоколы и электрические и оптические интерфейсы

Табл. 1.1 - Термины и сокращения

Наименование термина/сокращения	Описание
SAP R/3	Информационная система, предназначенная для координации всех ресурсов и действий, необходимых для выполнения бизнес-процессов, таких как выполнение заказов, выставление счетов, управление персоналом и планирование ресурсов предприятия
Slave	(англ.) — подчиненный экземпляр ТЕСК при настроенном распределенном мониторинге, который не может самостоятельно инициировать передачу своих данных, а передаёт или принимает их только по запросу главного экземпляра
SNMP	(англ. Simple Network Management Protocol — простой протокол сетевого управления) — стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP
Snmp-walk	Процедура, выполняющая серию команд внутри заданного OID'ом диапазона
SSH	(англ. Secure Shell — «безопасная оболочка») — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов)
TCP	(англ. Transmission Control Protocol - протокол управления передачей) - протокол передачи данных интернета, предназначенный для управления передачей данных. Механизм TCP предоставляет поток данных с предварительной установкой соединения, осуществляет повторный запрос данных в случае потери данных и устраняет дублирование при получении двух копий одного пакета, гарантируя целостность передаваемых данных и уведомление отправителя о результатах передачи

Табл. 1.1 - Термины и сокращения

Наименование термина/сокращения	Описание
UDP	(англ. User Datagram Protocol — протокол пользовательских датаграмм) — протокол передачи данных. UDP использует простую без предварительного установления соединения и создания виртуального канала: датаграммы могут прийти не по порядку, дублироваться или не дойти
URL	(англ. Uniform Resource Locator — унифицированный указатель ресурса, сокр. URL) — система унифицированных адресов электронных ресурсов, или единообразный определитель местонахождения ресурса
UTF-8	(англ. Unicode Transformation Format, 8-bit — «формат преобразования Юникода, 8-бит») — распространённый стандарт кодирования текста, позволяющий более компактно хранить и передавать символы Юникода, используя переменное количество байт (от 1 до 4), и обеспечивающий полную обратную совместимость с 7-битной кодировкой ASCII
WATO (Web Administration Tool)	Инструмент для конфигурирования системы с помощью графического интерфейса
Активные проверки	Проверки, инициируемые системой мониторинга с заданной периодичностью
Алиас	Альтернативное наименование хоста
Интерфейс	Сервис мониторящий доступность определенного порта коммутатора/маршрутизатора
Кластер (HA, High-Availability cluster)	(англ. High-Availability cluster, HA cluster — кластер высокой доступности) — группа серверов, спроектированная в соответствии с методиками обеспечения высокой доступности и гарантирующая минимальное время простоя за счёт аппаратной избыточности
Контактные группы	Группа пользователей, которые несут ответственность за определенные хосты или сервисы

Табл. 1.1 - Термины и сокращения






Наименование термина/сокращения	Описание
Конфигурация мониторинга	Набор правил применяемых при определении состояний объектов мониторинга
Операционная система (ОС)	Комплекс взаимосвязанных программ, предназначенных для управления ресурсами оборудования
Пассивные проверки	Проверки, основанные на данных, предоставляемых непосредственно оборудованием без запроса со стороны системы мониторинга
Пользователь автоматизации	Пользователь предназначен для взаимодействия с ТЕСК через Web-API
Сервис	Параметр или набор параметров, получаемых с датчиков и процессов хоста. Примерами сервисов являются проверки значений параметров сетевых интерфейсов, датчиков температуры, файловых систем серверов и т.д.
Событие	Информационный объект, создаваемый системой на основании зафиксированных данных об изменении статуса объекта мониторинга и содержащий необходимую диагностическую информацию
ТЕСК, Система	Транссеть. Единая Система Контроля
Узел	Хосты, составляющие кластер
Форма просмотра	Страница графического интерфейса системы, предназначенная для удобного просмотра информации об объектах мониторинга
Хост	Любое устройство с IP адресом
	Переход в меню действий, доступных для хоста/сервиса
	Запуск немедленной проверки данного сервиса
	Запуск проверки основного сервиса «Check_MK»
	Сервис находится в настоящий момент в запланированном периоде простоя
	Хост находится в настоящий момент в запланированном периоде простоя

Табл. 1.1 - Термины и сокращения

Наименование термина/сокращения	Описание
	Хост/сервис находится вне периода уведомлений
	Уведомления для данного хоста/сервиса в настоящее время отключены
	Проверки для данного сервиса в настоящее время отключены
	Хост/сервис имеют неактуальный (устаревший) статус
	Хост/сервис находится в нестабильном состоянии (статус flapping)
	Хост/сервис имеет подтверждение аварии
	Существует комментарий для данного хоста/сервиса
	Хост/сервис являются частью VI агрегации
	Возможен прямой доступ к настройкам параметров проверки
	Только для сервисов, анализирующих лог-файлы: при клике на иконку возможен доступ к лог-файлу
	Доступ к графику сервиса
	Хост/сервис имеет данные инвентаризации: клик по значку позволяет просмотреть эти данные
	Хост/сервис добавлен в список избранных
	Доступ к выгруженному конфигурационному файлу
	Быстрое подтверждение проблемы/аварии
	Редактировать
	Доступ к фильтрам данных
	Параметры форм просмотров
	Список команд
	Активация чек-боксов

2 ОПИСАНИЕ ПРОГРАММНОГО ПРОДУКТА

2.1 Структура ТЕСК и назначение её частей

В состав ТЕСК входят следующие компоненты:

- Ядро мониторинга
- Status (Multisite)
- WATO (Web Administration Tool)
- BI (Business Intelligence)
- Inventory
- Reporting
- Graphing
- NagVis
- Event Console
- Notify
- RRD Tool

2.1.1 Ядро мониторинга

Ядро мониторинга - формирует очередь опроса объектов мониторинга, запуск проверок и обработку результатов (см.Рис. 2.1).

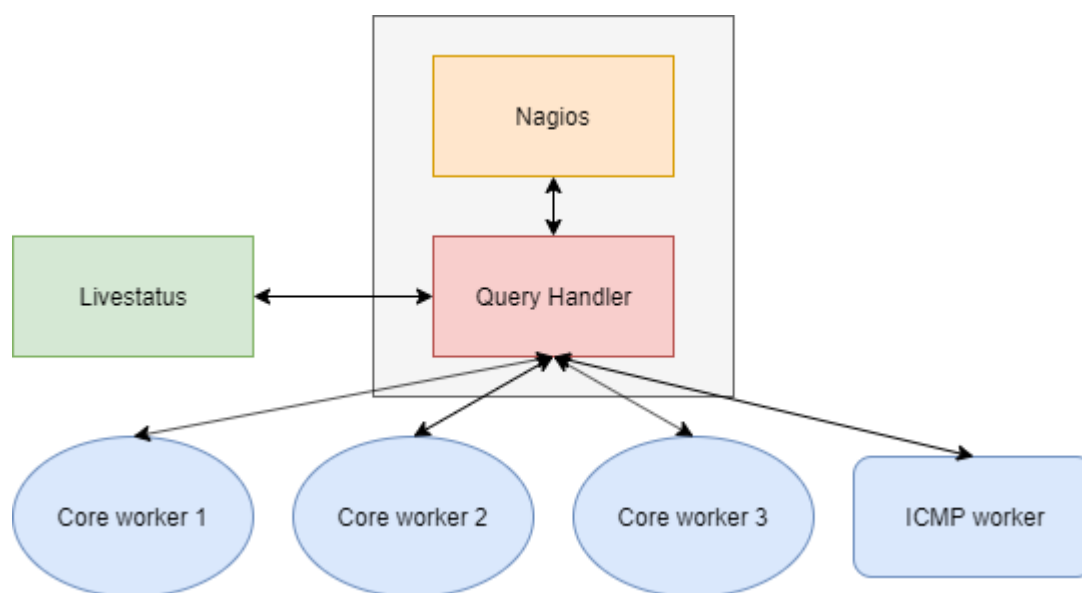


Рис. 2.1 – Ядро мониторинга Nagios

Ядро мониторинга строится на базе системного ПО открытого типа Nagios.

В состав ядра мониторинга входят:

- Core Workers – это процессы, функции которых ограничены выполнением проверок. Обработчики содержат минимальный набор функций, благодаря чему они запускаются быстро, что позволяет увеличить производительность ядра. Для взаимодействия с основным процессом Nagios используется обмен данными через память (IPC через Unix-domain сокеты), без сохранения информации на диск.

Штатные рабочие процессы ответвляются при запуске Nagios и находятся в памяти до завершения работы, что избавляет от необходимости клонирования при выполнении проверок.

- **ICMP worker** – осуществляет проверки доступности хостов.
- **Query Handler** - интерфейс для организации взаимодействия внешних компонентов с Nagios. Через данный интерфейс, в частности, организована работа ранее упомянутых Core Workers.
- **Livestatus** — модуль ядра (брокер), который загружается вместе с Nagios и выполняется в одном адресном пространстве, что обеспечивает ему прямое подключение к данным о состоянии хостов и сервисов. Получает запросы через Unix-сокет или через TCP соединение (порт по умолчанию 6557). Это дает возможность другим модулям, таким как NagVis и Multisite, иметь быстрый и эффективный доступ к данным о состоянии объектов мониторинга. Доступ обеспечивается через простой текстовый протокол (LQL — похож на смесь SQL и HTTP) и возможен для реализации на многих языках программирования без использования специальных библиотек.

2.1.2 Модули ТЕСК

Status (Multisite) - модуль предназначен для визуализации результатов опросов объектов мониторинга (хостов, сервисов).

WATO (Web Administration Tool) - модуль предназначен для конфигурирования хостов/сервисов (управление и настройка), настройки параметров и порогов мониторинга, тегов, прав пользователей на основе ролей и др.

BI (Business Intelligence) - модуль, который позволяет более эффективно использовать данные, получаемые из мониторинга, отслеживать зависимости сервисов и их статусов на более высоком уровне – бизнес-агрегаций.

Inventory - модуль, реализующий получение и хранение данных инвентаризации и истории ее изменения. В данном модуле реализована функция получения информации о логических ресурсах из конфигурационных файлов активного сетевого оборудования.

Reporting - модуль, позволяющий формировать оперативные отчеты для объектов мониторинга (хостов, сервисов или BI-агрегаций).

Graphing - модуль построения графиков, в основе которого лежит PNP4Nagios.

NagVis– модуль, позволяющий создавать, редактировать, удалять карты и мнемосхемы, добавлять хосты, линии, отображать родительские связи (топологию сети).

Event Console - консоль событий отвечает за обработку результатов пассивных проверок

Notify - модуль, который оперативно информирует пользователей в случае возникновения проблем или других важных событий. В качестве канала оповещения чаще всего используется электронная почта. Существуют и другие методы: отправка SMS, отправка в мессенджеры или через систему автоинформирования. Простой интерфейс данного модуля позволяет создавать собственные правила уведомлений.

RRD Tool - модуль, обеспечивающий хранение полученных во время мониторинга данных измерений состояния хостов и сервисов.

Архитектура ТЕСК представлена на рисунке ниже (см. Рис. 2.2).

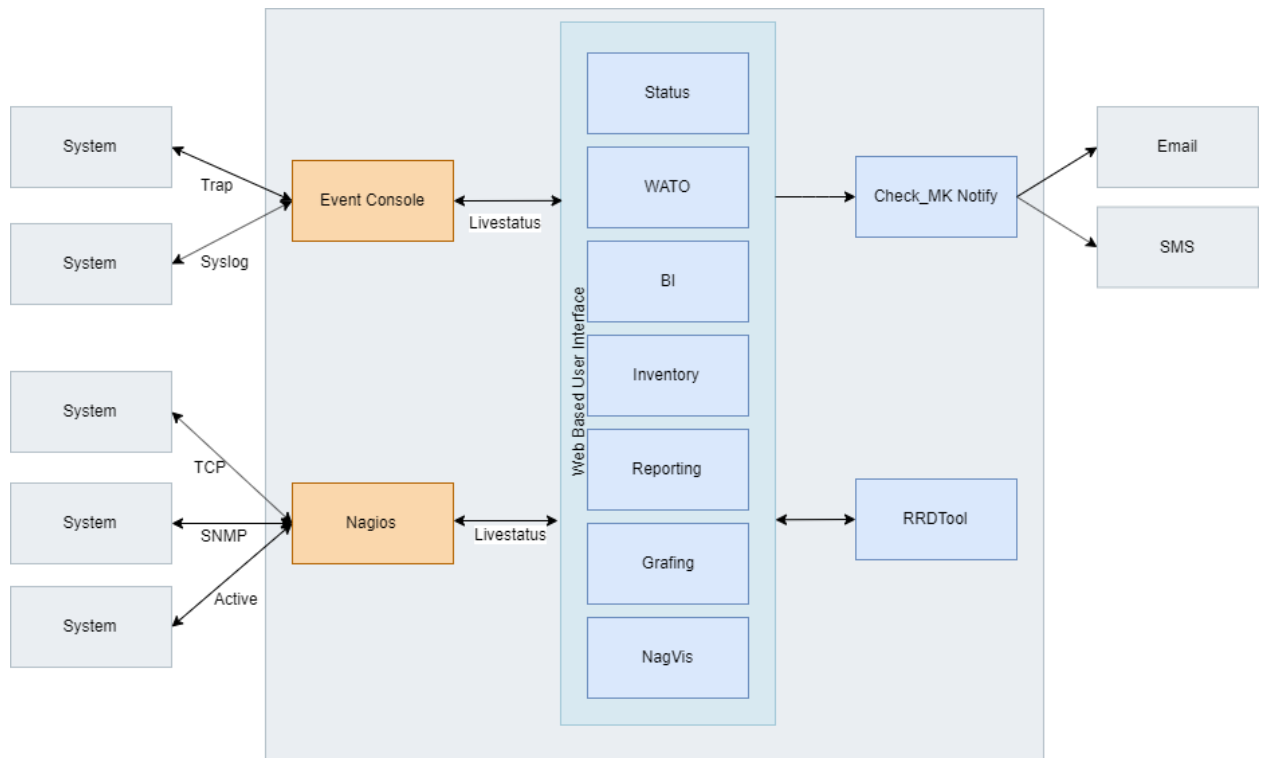


Рис. 2.2 – Архитектурное решение ТЕСК

3 ПОДГОТОВКА К РАБОТЕ

3.1 Роли пользователей

Перечень ролей, определенных для работы с программным продуктом, приведен в документе «Общее описание системы» п. 2.2.3.

3.2 Права доступа

Подробный перечень прав доступа представлен в документе «Руководство пользователя с правами Администратор» п. 4.8.

3.3 Установка программного обеспечения

Подготовка к работе, установка и настройка программного обеспечения ТЕСК осуществляется силами Исполнителя на оборудовании Заказчика.

3.4 Состав и содержание дистрибутивного носителя данных

Дистрибутив клиентской части отсутствует. Доступ к ТЕСК осуществляется посредством глобальной сети обмена данными Интернет с помощью интернет-браузера.

3.5 Загрузка приложения

Доступ к ТЕСК осуществляется 24/7.

Для авторизации в ТЕСК необходимо запустить интернет-браузер и в адресной строке ввести следующее значение:

http://<ip_регионального_сервера>:7780/check_mk/.

Откроется форма авторизации (Рис. 3.1).



Рис. 3.1 – Форма авторизации

На открывшейся форме требуется ввести имя пользователя и пароль и нажать на кнопку «Login». По умолчанию открывается раздел «Главный обзор» (Рис. 3.2).



Рис. 3.2 – Экранная форма «Главный обзор»

Экранная форма состоит из блока боковой панели и главного экрана. Подробное описание, боковой панели – в п. 4.1, полное описание интерфейса Пользователя - в п. 4 настоящего руководства.

4 ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ

4.1 Боковая панель

Боковая панель представляет возможные варианты просмотров текущего состояния, обобщенной информации по мониторингу, панели поиска в виде различных информационных блоков (Рис. 4.1). Информационные блоки могут быть расположены в любом порядке, удобном пользователю. Содержимое блоков можно сворачивать и разворачивать, а также перемещать вверх/вниз боковой панели.

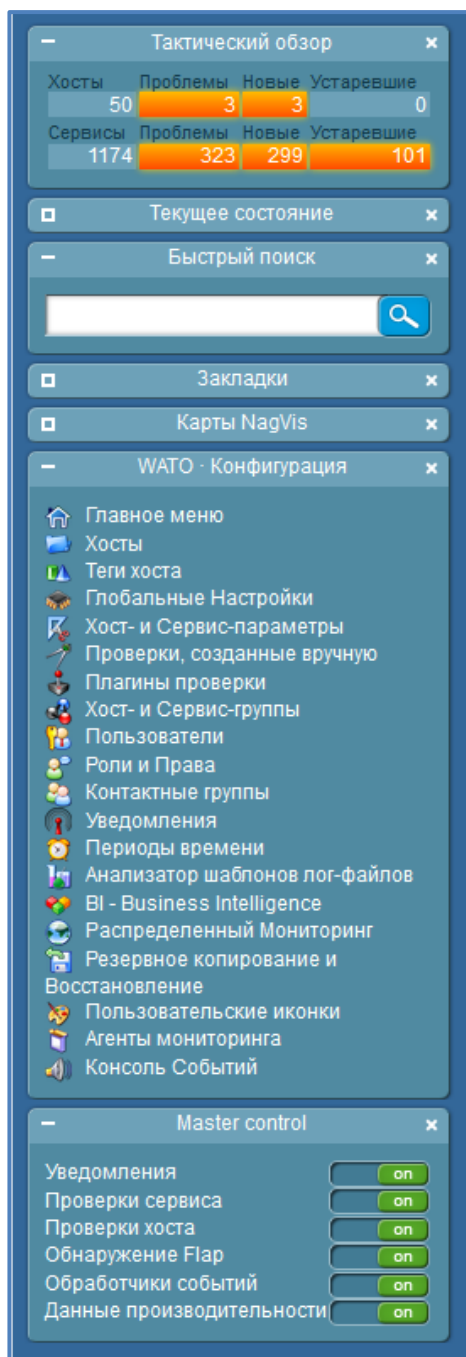
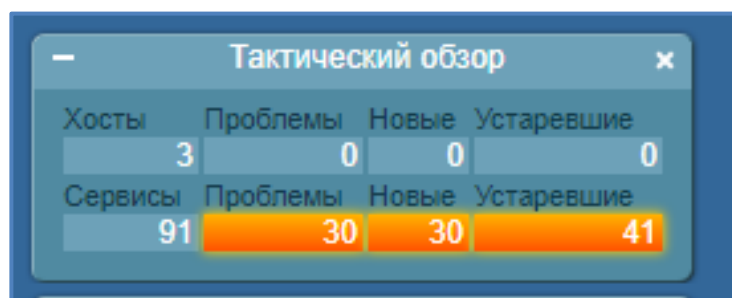


Рис. 4.1 – Боковая панель

Блок «Тактический обзор» - показывает количество опрашиваемых хостов и сервисов, текущие проблемы (обработанные) и новые (необработанные из них,

а также устаревшие проблемы (связанные с хостами/сервисами с истекшим периодом опроса) (Рис. 4.2).



Хосты	Проблемы	Новые	Устаревшие
3	0	0	0
Сервисы	Проблемы	Новые	Устаревшие
91	30	30	41

Рис. 4.2 – Блок боковой панели «Тактический обзор»

При нажатии на значения в полях происходит переход к соответствующему экрану детализации.

Блок «Быстрый поиск» - поле для поиска хостов и сервисов (Рис. 4.3).

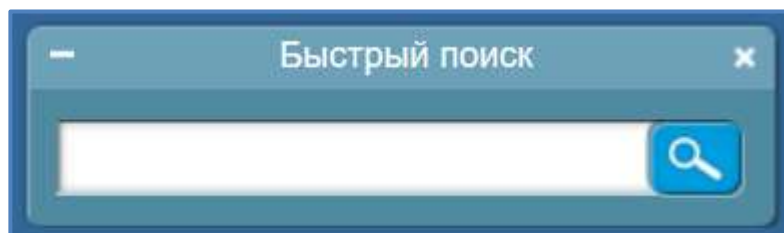


Рис. 4.3 – Быстрый поиск

Блок «Текущее состояние» – предлагает доступ к различным вариантам отображения хостов, сервисов и другой информации, полученной в ходе мониторинга (Рис. 4.4).

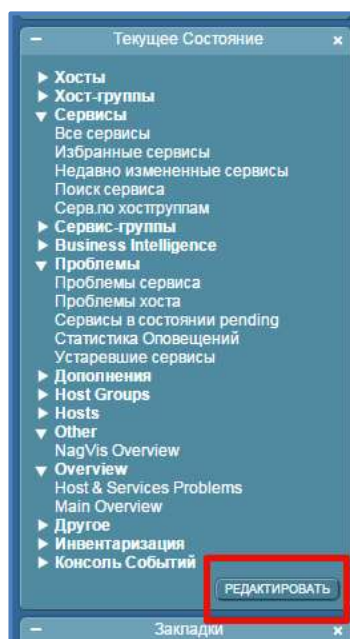


Рис. 4.4 – Блок боковой панели «Текущее состояние»

- «Хосты» – блок включает в себя перечень обзоров, представляющих состояния хостов.
- «Хост-группы» – блок включает в себя перечень обзоров, представляющих состояния хостов в разрезе хост-групп.

- «Сервисы» – блок включает в себя перечень обзоров, представляющих состояния сервисов.
- «Сервис-группы» – блок включает в себя перечень обзоров, представляющих состояния сервисов в разрезе сервис-групп.
- «Business Intelligence» – блок включает в себя перечень обзоров, представляющих состояния хостов в разрезе созданных бизнес агрегаций.
- «Проблемы» – блок включает в себя перечень обзоров, представляющих хосты и сервисы в состоянии «DOWN», «CRIT», «PEND».
- «Other» – блок включает в себя обзор карт «Nagvis Overview».
- «Обзор» – блок включает в себя «Главный обзор», по нажатию на ссылку происходит переход к стартовой странице ТЕСКа, и «Хост & Сервис-проблемы», представляющий обзор хостов и сервисов в состоянии «DOWN», «CRIT», «WARN».
- «Другое» – блок включает в себя перечень обзоров, где доступно отображение и удаление запланированных простоев, просмотр история запланированных простоев, просмотр всех комментариев для хостов и сервисов, просмотр глобального лог-файла, хост- и сервис события и уведомления.
- «Инвентаризация» – блок включает в себя перечень обзоров, представляющих результаты инвентаризации хоста в разрезе различных параметров, например: CPU, LLDP-интерфейсы, Версия ОС, Датчики, Сетевые интерфейсы.
- «Консоль событий» – блок включает в себя обзоры событий и недавнюю историю событий, полученных из «Консоли событий».

Блок «Закладки» – предоставляет удобный доступ к регулярно используемым страницам (Рис. 4.5).

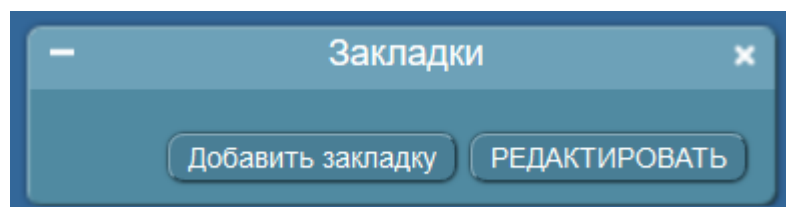


Рис. 4.5 – Блок «Закладки»

Блок «WATO конфигурация» – блок для конфигурирования ТЕСК с помощью графического интерфейса, который содержит перечень ссылок на страницы конфигурации (Рис. 4.6).



Рис. 4.6 – Блок «WATO конфигурация»

- «Главное меню» – содержит список всех модулей WATO, с кратким описанием каждого (Рис. 4.7).



Рис. 4.7 – Главное меню

- «Хосты» – доступ для управления хостами, находящимися на мониторинге (Рис. 4.8).



Рис. 4.8 – Экранная форма раздела «Хосты»

- «Хост- и Сервис-параметры» – содержит полный перечень проверок для настройки мониторинга хостов, которые были созданы при обнаружении в автоматическом режиме (Рис. 4.9).



Рис. 4.9 – Экранная форма раздела «Хост- и Сервис-параметры»

- «Активные проверки»: позволяет настроить активные проверки конкретных сетевых служб и протоколов (HTTP, SSH, FTP, DNS);
 - «Группирование»: определяет назначение хостов и сервисов к хост-, сервис- и контактным группам;
 - «Конфигурация мониторинга»: в данной группе определяются параметры интервалов проверок, повторных проверок, уведомлений, кластеризация, настройки инвентаризации и другое;
 - «Доступ к агентам»: определены настройки параметров, касающихся подключения к Check_MK- и SNMP-агентам;
 - «Параметры обнаруженных сервисов»: здесь определяются уровни и другие параметры проверок, найденных обнаружением сервисов Check_MK. Данные правила используются, чтобы определить параметры, подобные уровням файловой системы, уровням загрузки CPU и другим понятиям сервисов, которые были найдены автоматическим обнаружением сервисов Check_MK;
 - «Модули источников данных»: здесь определяются специализированные агенты, например, проверка через SSH, ESX vSphere, SAP R/3;
 - «Аппаратная/программная инвентаризация»: в данной группе параметров определяется конфигурация системы инвентаризации аппаратного и программного обеспечения Check_MK;
 - «Консоль событий»: настройки и проверки, касающиеся консоли событий Check_MK.
- «Проверки, созданные вручную» – содержит перечень правил для хостов, при настройке которых создаются сервисы (Рис. 4.10).



Рис. 4.10 – Экранная форма блока «Проверки, созданные вручную»

- «Плагины проверки» - данный каталог плагинов проверки дает полный перечень всех плагинов, которые поставляются с установкой Check_MK. Он также позволяет получить доступ к наборам правил для настройки параметров проверок и создания сервисов вручную (Рис. 4.11).



Рис. 4.11 – Каталог плагинов проверки

- «Анализатор шаблонов лог-файлов» - предоставляет возможность проверить определенные шаблоны лог-файла. Используя данное диалоговое окно, можно проанализировать и отладить весь набор шаблонов лог-файлов (Рис. 4.12).

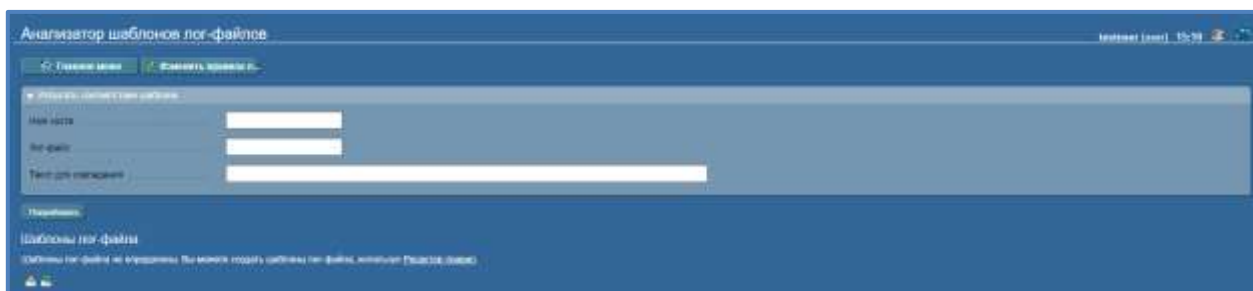



Рис. 4.12 – Экранная форма «Анализатор шаблонов лог-файлов»

- «BI – Business Intelligence» - позволяет сгруппировать несколько хостов с целью получения общего состояния приложений, хостов или других интересующих элементов из набора хостов и сервисов, более гибко настраивая правила определения общего статуса агрегации (Рис. 4.13).



Рис. 4.15 – Информационная панель «Главный обзор»

В ТЕСК есть встроенный редактор информационных панелей. Переход в режим редактирования панели осуществляется нажатием на кнопку шестеренки  в нижней правой части экранной формы (отображается при наведении курсора мышки на область) (Рис. 4.16) и выбором пункта «Редактировать Dashboard» в открывшемся меню.

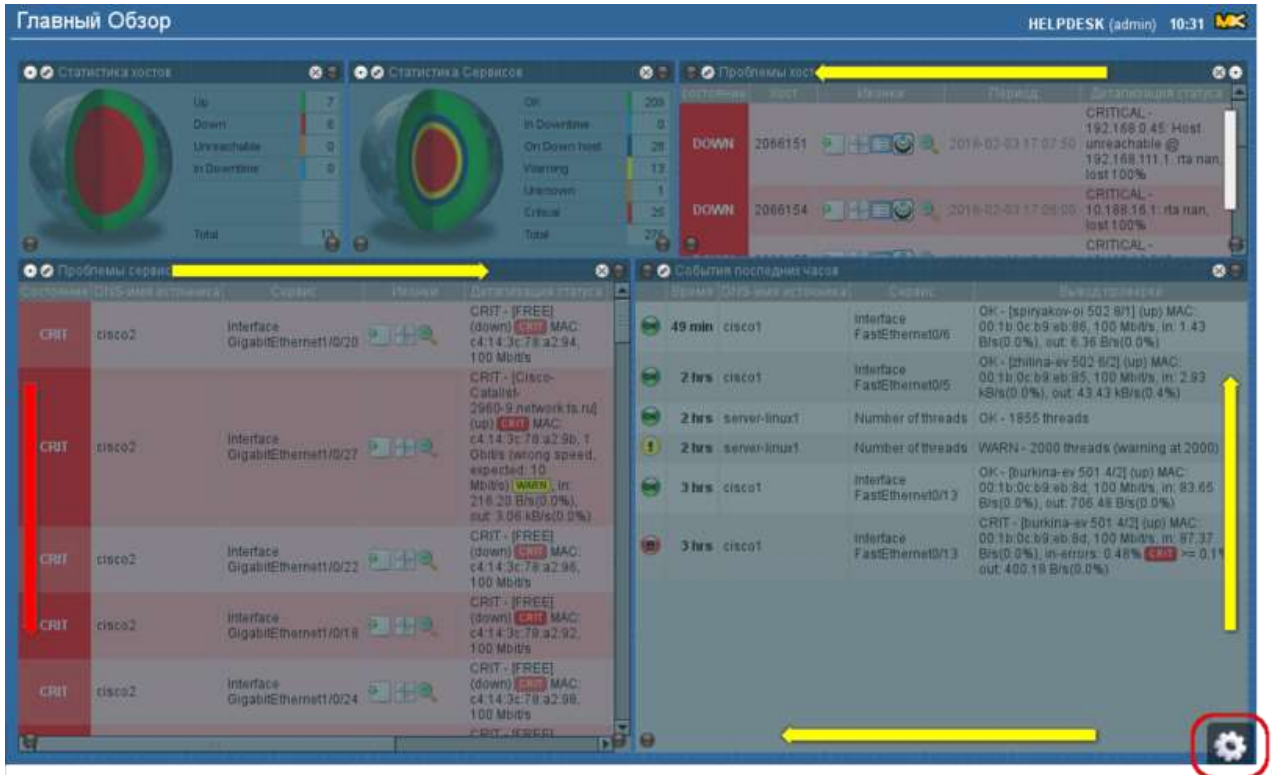







Рис. 4.16 – Режим редактирования дашборда

В режиме редактирования отображаются следующие элементы управления (Рис. 4.17):

-  - удалить данный элемент.
-  - открыть диалоговое окно редактирования для данного элемента.
-  - показывает, к какому углу в настоящее время привязан элемент в информационной панели.
-  - требуется использовать для выбора угла в качестве точки привязки.

Для окончания редактирования, необходимо нажав на иконку «шестеренка»  выбрать пункт «Прекратить редактирование» (Рис. 4.17), чтобы сохранить информационную панель.

4.2.2 Добавление элемента на информационную панель

Добавить новый элемент на информационную панель можно в режиме редактирования, нажав на иконку шестерёнки (Рис. 4.16) и выбрав пункт меню «Добавить dashlet».

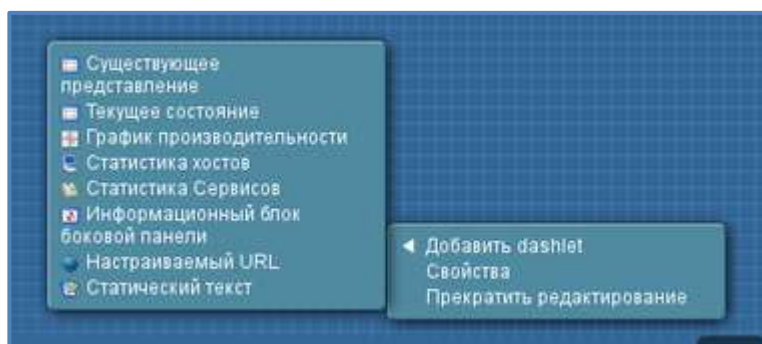


Рис. 4.17 – Редактирование информационной панели. Меню «Добавить dashlet»

Для нового элемента необходимо выполнить следующие настройки (Рис. 4.18):

- блок «Главные настройки»: этот раздел выглядит одинаково для всех типов элементов. Позволяет настроить отображение фона, заголовка;
- блок «Свойства»: в разделе представлены индивидуальные характеристики выбранного элемента.

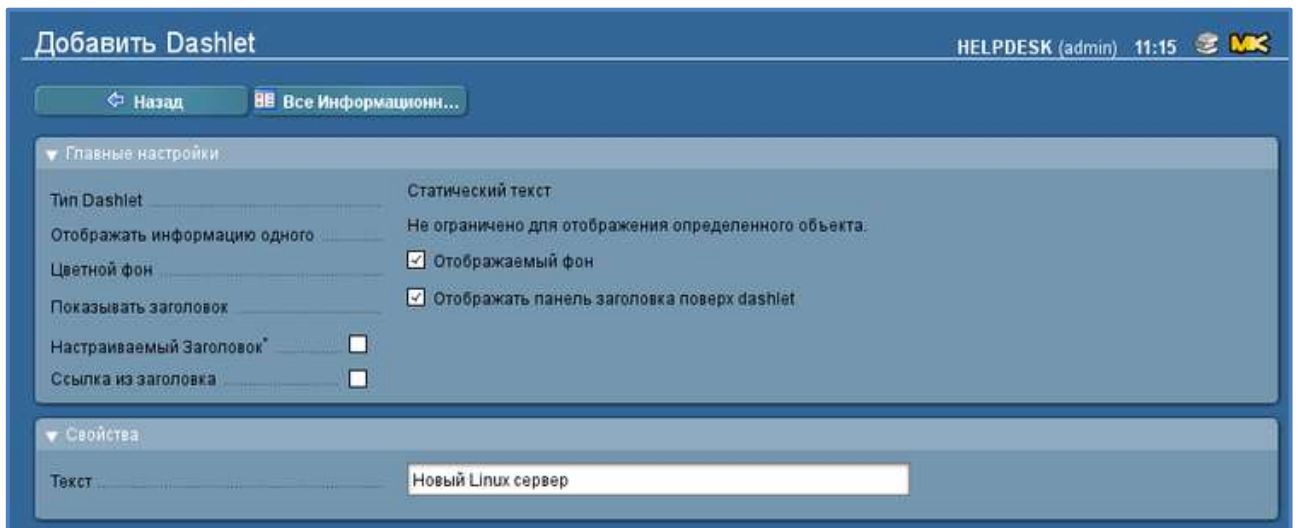


Рис. 4.18 – Редактирование информационной панели. Добавление нового элемента

Также можно добавить новый элемент на информационную панель непосредственно из того места в интерфейсе, где пользователь увидел необходимую информацию. Для этого у каждой формы просмотра или графика есть контекстное меню, с помощью которого этот элемент можно добавить в информационную панель (Рис. 4.19).

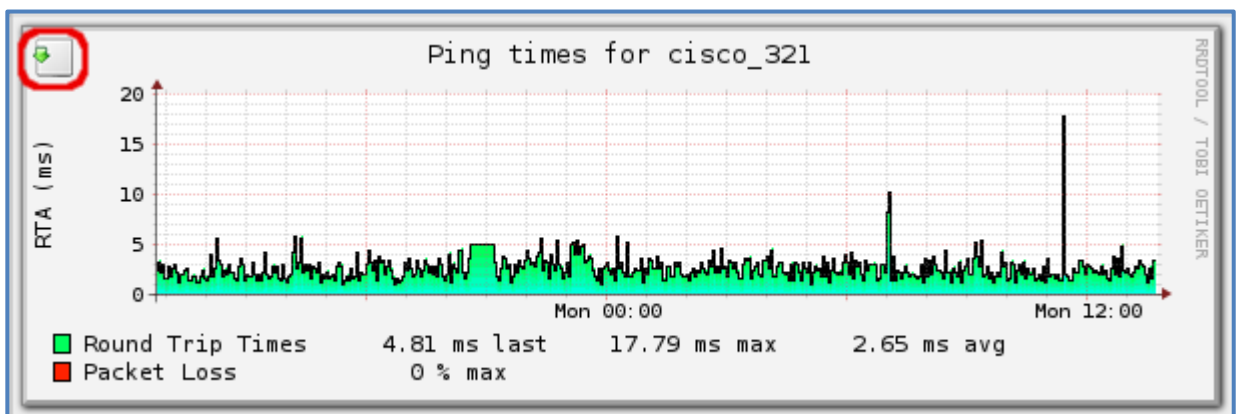


Рис. 4.19 – Пример контекстного меню для добавления элемента на информационную панель

При нажатии на выделенную кнопку (Рис. 4.19) открывается меню выбора информационной панели, на которую будет добавлен текущий элемент (Рис. 4.20).

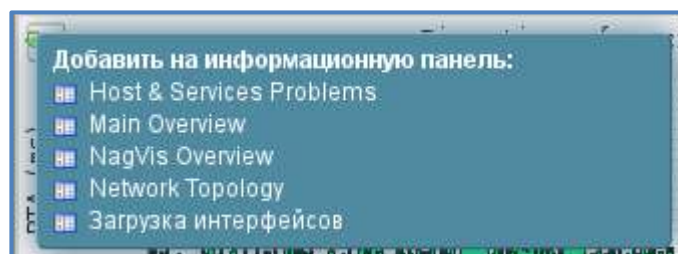


Рис. 4.20 – Меню выбора информационной панели

4.2.3 Создание новой информационной панели

Переход к созданию новой информационной панели осуществляется через блок «Текущее состояние» на боковой панели по нажатию на кнопку «Редактировать». Над списком форм просмотра доступна кнопка «Информационные панели», по нажатию на которую можно осуществить переход к списку информационных панелей для их редактирования или создания (Рис. 4.21).

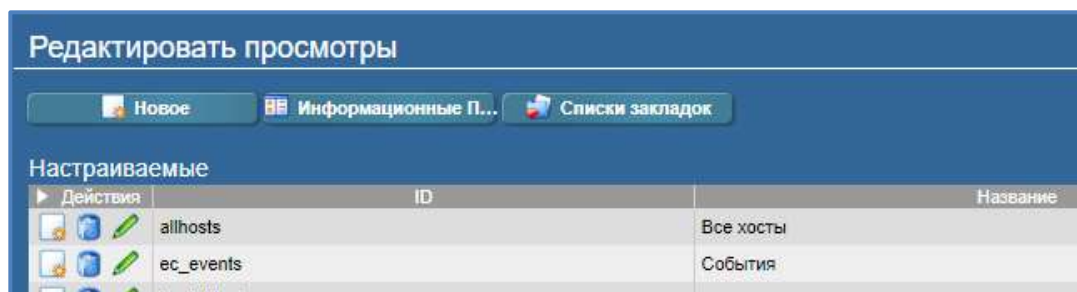


Рис. 4.21 – Меню редактирования просмотров

На форме редактирования просмотров для создания новой панели необходимо нажать на кнопку «Новое» (Рис. 4.22).



Рис. 4.22 – Меню редактирования информационных панелей

При создании новой информационной панели требуется указать источник данных (Рис. 4.23).

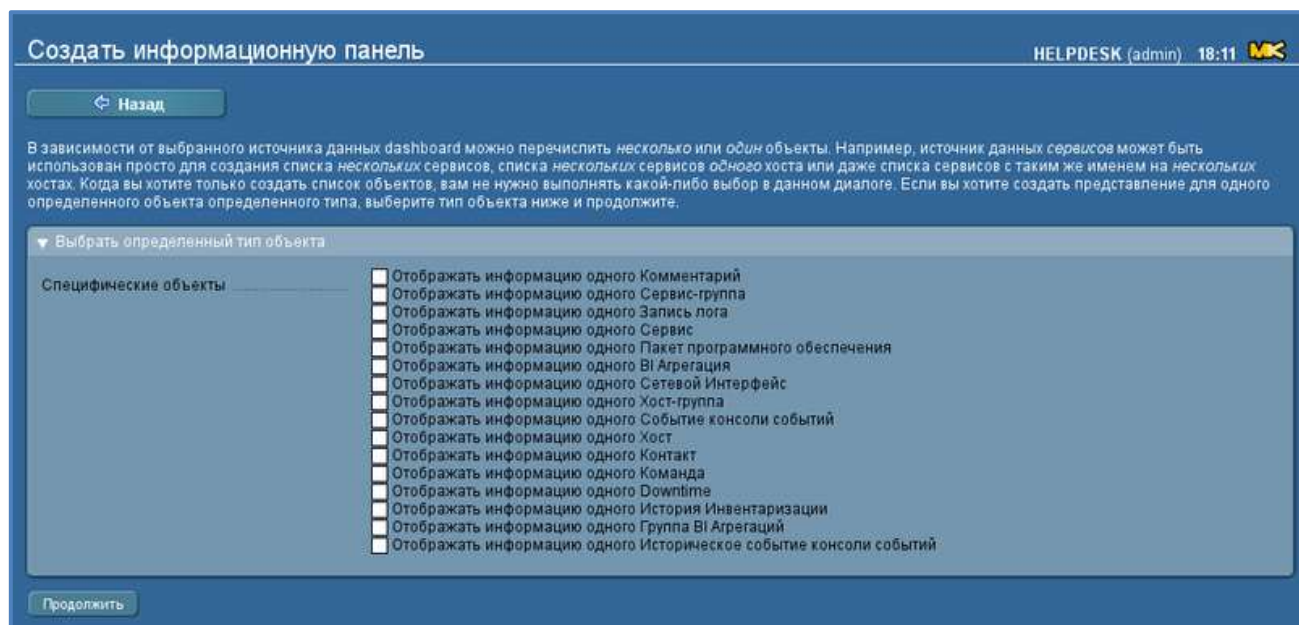


Рис. 4.23 – Форма создания информационной панели – выбор источника данных

Для того, чтобы создать глобальную форму просмотра, данный этап следует пропустить, оставив без выбора.

Создать информационную панель HELPDESK (admin) 18:21

[← Назад](#)

▼ Основные Параметры

Отображать информацию одного Не ограничено для отображения определенного объекта.

Уникальный ID

Название*

Раздел*

Описание*

Текст клавиши*

Иконка клавиши

Видимость Скрывать данный информационную панель из боковой панели
 Не показывать контекстную кнопку для данного информационную панель
 Сделать данный информационную панель доступным для всех пользователей

► Свойства Информационной Панели

► Контекст / Фильтры поиска

Рис. 4.24 – Форма создания информационной панели. Блок «Основные параметры»

Основные параметры (Рис. 4.24) для информационной панели включают в себя такую информацию как уникальный ID, название, раздел, в который будет добавлена новая информационная панель и т.д.

При создании новой информационной панели можно также определить, кто получит доступ к ней. Пользователи, имеющие доступ к новой информационной панели, при входе в систему будут видеть вновь настроенную информационную панель вместо той, что установлена по умолчанию. Для того, чтобы включить доступ, необходимо активировать опцию «Сделать данную информационную панель доступной для всех пользователей».

5 ОПИСАНИЕ ОПЕРАЦИЙ

Для организации мониторинга оборудования необходима корректная настройка его параметров. Хосты представляют собой объекты, описывающие физические или виртуальные устройства в сети, за которыми необходимо вести наблюдение. Для просмотра имеющихся хостов и их настройки необходимо перейти в «WATO-Конфигурация» -> «Хосты» (Рис. 5.1).

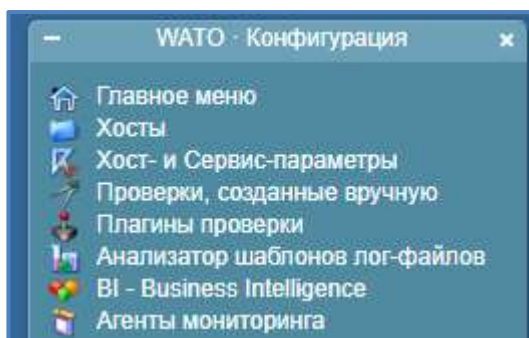


Рис. 5.1 – Блок «WATO конфигурация»

В результате откроется окно вкладки «Хосты» с указанием имеющихся хостов и их основных параметров (Рис. 5.2).









Рис. 5.2 – Экранная форма раздела «Хосты»

Доступные кнопки на экране просмотра перечня хостов:

- «(1,2 и т.д.) Изменений» - по нажатию на кнопку осуществляется переход к экрану просмотра внесенных, но неподтвержденных изменений, которые требуется принять для их активации или отклонить.
- «Главное меню» - по нажатию на кнопку осуществляется переход к главному меню блока WATO.
- «Наборы правил» - по нажатию на кнопку осуществляется переход к экрану «Основанная на правилах конфигурация Хост- & Сервис-параметров», где представлены различные группы правил.
- «Проверки, созданные вручную» - по нажатию на кнопку осуществляется переход к экрану просмотра перечня проверок, доступных для создания вручную.
- «Свойства папки» - по нажатию на кнопку осуществляется переход к экрану просмотра свойств выбранной папки.
- «Новая папка» - по нажатию на кнопку осуществляется переход к экрану создания новой папки.
- «Новый хост» - по нажатию на кнопку осуществляется переход к экрану создания нового хоста, подробное описание представлено в п. 5.1.2 настоящего руководства.


- «Новый кластер» - по нажатию на кнопку осуществляется переход к экрану создания нового кластера, подробное описание представлено в п. 5.1.9 настоящего руководства.
- «Массовый импорт» - по нажатию на кнопку осуществляется переход к экрану ТЕСК, где представлена возможность указать параметры для выполнения импортирования хостов. Подробное описание представлено в п. 5.1.7 настоящего руководства.
- «Массовое обнаружение» - по нажатию на кнопку осуществляется переход к экрану настройки автоматического обнаружения сервисов на выбранных хостах.
- «Родительское сканирование» - по нажатию на кнопку осуществляется переход к экрану поиска родительских хостов.
- «Статус» - по нажатию на кнопку осуществляется переход к экрану просмотра статусов сервисов с разбивкой по хостам.
- «Поиск» - по нажатию на кнопку осуществляется переход к экрану поиска хостов по параметрам, описанным в п. 5.1.5 настоящего руководства.

Доступные действия с хостами:

-  - редактировать свойства данного хоста;
-  - просмотр параметров данного хоста, основанных на правилах;
-  - редактировать сервисы данного хоста;
-  - переместить данный хост в другую папку;
-  - создать клон данного хоста;
-  - удалить данный хост.

5.1 Настройка Хостов

5.1.1 Просмотр свойств хоста

Чтобы перейти к основным свойствам хоста необходимо выбрать на главном экране хост и нажать на кнопку  в строке выбранного хоста. В верхней части открывшегося экрана доступны следующие кнопки:

- «Папка» - по нажатию на кнопку осуществляется переход к папке, в которой расположен хост;
- «Статус» - по нажатию на кнопку происходит переход к экранной форме, описанной подробно в п. 5.1.4 настоящего руководства;
- «Сервисы» - по нажатию на кнопку происходит переход к экранной форме, описанной подробно в п. 5.2.1 настоящего руководства;
- «Параметры» - по нажатию на кнопку происходит переход к экранной форме просмотра параметров для создания правил;
- «Диагностика» - по нажатию на кнопку происходит переход к экранной форме, описанной подробно в п. 5.1.3 настоящего руководства;

- «Обновить DNS кэш» - по нажатию на кнопку происходит удаление весь кэш DNS и запускается процесс разрешения адресов (resolv) при следующей активации изменений.

Открывшееся окно свойств хоста состоит из четырех основных блоков (Рис. 5.3):

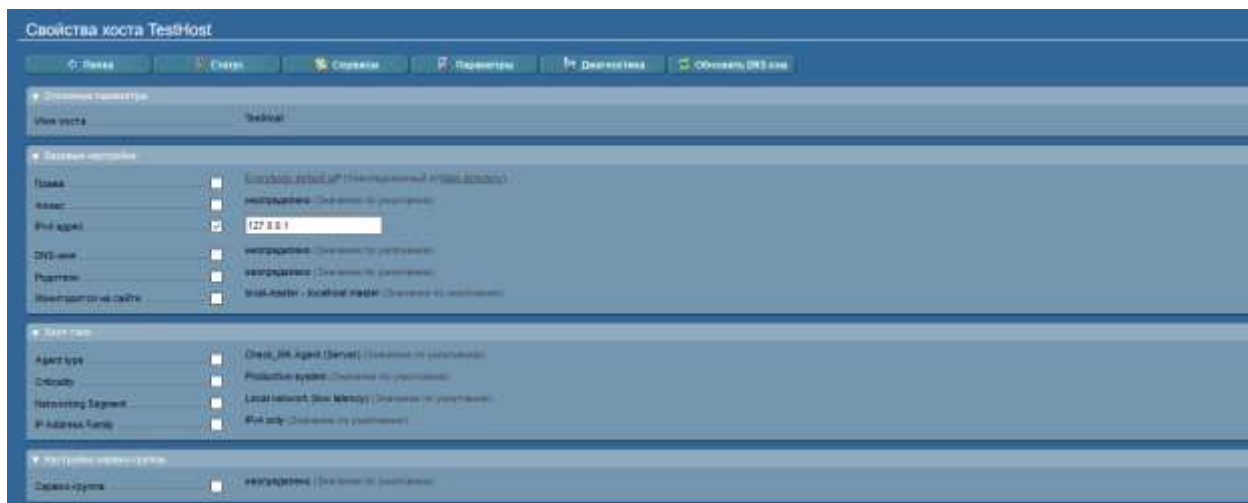



Рис. 5.3 – Экран просмотра «Свойства хоста»


- «основные параметры»: здесь указывается имя хоста;
- «базовые настройки»: в данном блоке указываются:
 - права - содержит список контактов (пользователей), которым разрешено редактирование настроек данного хоста в WATO. Пользователь может автоматически сделать выбранные контактные группы контактами мониторинга путем установки отметки чек-бокса в поле «Добавить данные контактные группы к хосту», в этом случае данные контакты смогут получать уведомления при аварии на оборудовании).
 - алиас - хосту может быть присвоено альтернативное описательное имя, которое будет отображаться во многих местах как в графическом интерфейсе, так и в отчетах. Если алиас не определен, то в качестве алиаса будет использоваться имя хоста.
 - ip-адрес хоста – адрес может быть указан вручную при создании хоста в стандартном виде, в таком случае DNS действие не требуется. Ip-адрес может быть не указан, но в таком случае требуется указание DNS имени хоста.
 - DNS-имя хоста - при указании ip-адреса поле может быть не заполненным.
 - Порт SNMP - поле отображается и становится доступным для редактирования, если выбран тип агента SNMP, указывается порт подключения по протоколу SNMP.
 - SNMP-community – поле отображается и становится доступным для редактирования, если выбран тип агента SNMP.
 - Родители – может указываться как при создании хоста вручную так же может заполняться при сканировании.


- Мониторится на сайте - Указывается сайт, который должен мониторить данный хост, при выполненной настройке распределенного мониторинга.
- «хост-теги»: выбирается значение хост-тега для данного хоста (по умолчанию, всем хостам присваивается первый созданный тег в любой группе тегов).
В блоке «хост-теги» возможные значения тега «Agent type» следующие:
 - Check_MK агент – хост должен отслеживаться с помощью агентов Check_MK, которые должны быть установлены на хосте, который должен быть поставлен на мониторинг. Необходимо выбрать это значение также в случае использования специальных агентов, таких как, например, ESX-Monitoring.
 - SNMP – хост должен проверяться с помощью SNMP. Этот выбор позволяет отображать в «Базовых настройках» поле «SNMP Community», с помощью которого можно определить SNMP Community. Так как это значение, как правило, одинаково для многих хостов, то предпочтительнее, чтобы он был определен в папке. Если значение не указано, то оно автоматически принимается как public.
 - No Agent - отсутствие агента, если требуется проверка только доступности хоста. Такие хосты не имеют агентов и отслеживаются только с помощью Активных проверок. Правила для них находятся в разделе WATO Хост- & Сервис-параметры -> Активные проверки. Если не будет определена ни одна активная проверка, то ТЕСК создаст автоматически сервис PING.
 - Bulkwalk (SNMP v2c) – при выборе «SNMP» «Dual Check_MK+SNMP» доступен выбор команды для проведения инвентаризации хоста «simple walk (like SNMP v1) » или «Bulkwalk (SNMP v2c) » и протокола SNMP (какой протокол SNMP доступен для опроса).
- «Настройки сервис-групп».

5.1.2 Создание хоста

ТЕСК позволяет создать новый хост клонированием одного из существующих в системе хостов либо создать новый хост. Для выполнения клонирования

хоста следует нажать на пиктограмму  в столбце «Действия» в строке хоста на экране просмотра перечня хостов блока WATO. По нажатию на пиктограмму будет осуществлен переход к экранной форме «Свойств хоста», где часть полей формы будет предварительно заполнена и пользователю придется изменить лишь необходимые параметры.

Для создания нового хоста нужно нажать на кнопку  в верхней части экранной формы просмотра перечня хостов блока WATO или

нажать на пиктограмму  в строке хоста. В случае создания нового хоста

потребуется заполнить форму на экранной форме «Свойства хоста» (Рис. 5.4). Описание возможных значений параметров представлено в п. 5.1.1 настоящего руководства.

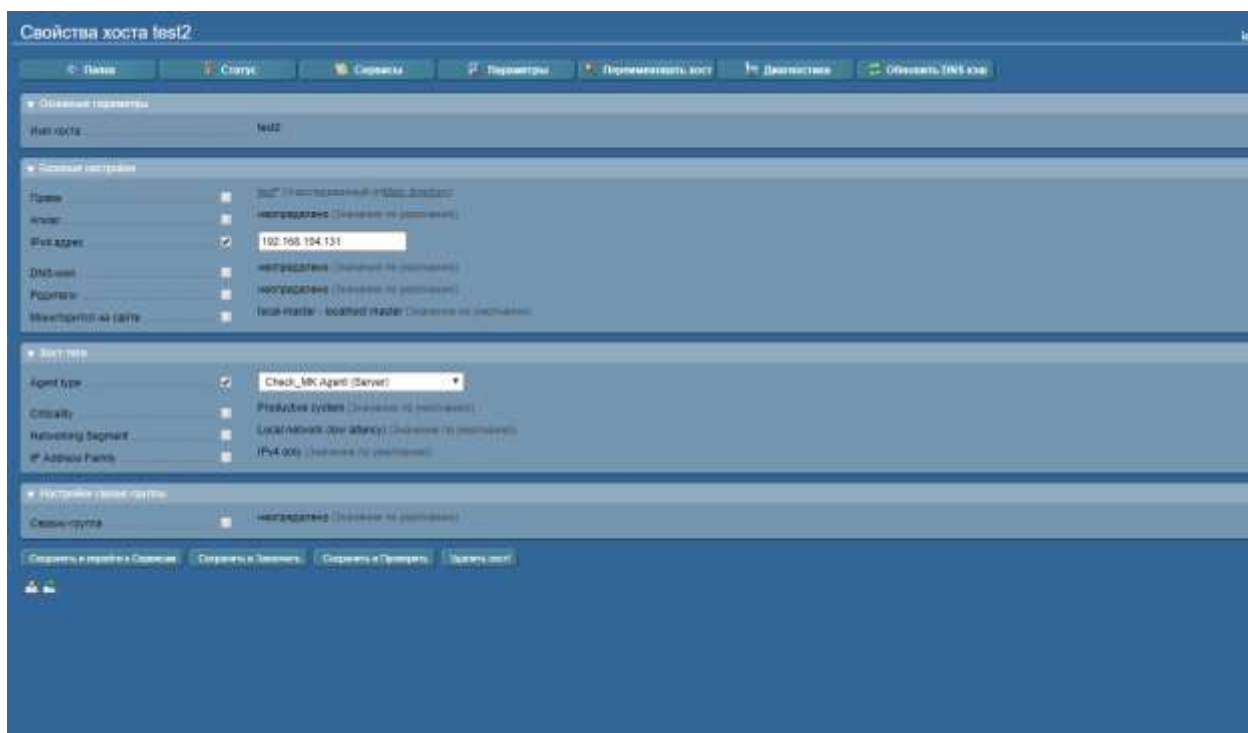



Рис. 5.4 – Свойства хоста

После указания всех параметров хоста требуется выбрать одну из следующих кнопок:

- «сохранить & перейти к сервисам»: данная кнопка позволяет сохранить изменения в свойствах хоста и перейти к результатам поиска сервисов хоста. Аналогично переход может быть осуществлен с помощью кнопки «Сервисы» в верхней части экрана либо через  в строке заданного хоста в общем окне отображения хостов. Данные кнопки также показывают результат инвентаризации сервисов хоста, где можно выбрать найденные сервисы и поставить их на опрос;
- «сохранить & закончить»: данная кнопка завершает редактирование свойств хоста, после сохранения происходит переход к главной странице меню «Хосты»;
- «сохранить & проверить»: данная кнопка переводит на страницу диагностики хоста, автоматически запуская проверку и выдавая ее результаты.

5.1.3 Проверка настроек хоста

Для осуществления проверки корректности настроек хоста необходимо выбрать хост, открыть его свойства и нажать на кнопку «Диагностика». Откроется окно проверки (Рис. 5.5), но для запуска диагностики требуется нажать на кнопку «Проверить» (перед запуском проверки параметры ip-адрес и SNMP- community доступны для изменения).



Рис. 5.5 – Экранная форма «Диагностика хоста»

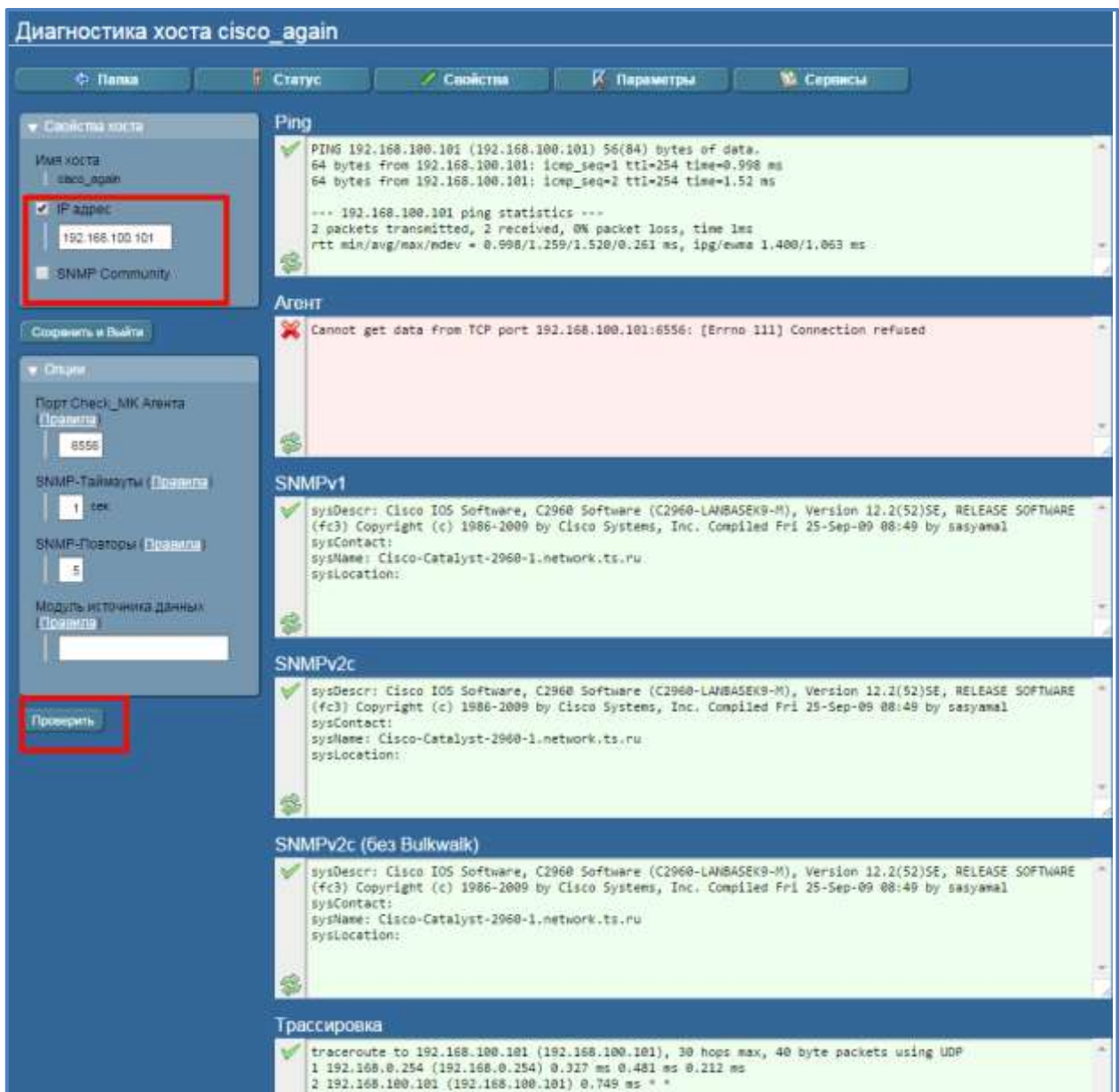


Рис. 5.6 – Выполнение проверки на экранной форме «Диагностика хоста»
 Результаты проверки будут представлены в виде нескольких блоков (Рис. 5.6):

- «ping»: проверка доступности оборудования и качества соединения;
- «агент»: проверка доступности подключения к check_mk-agent, который выполняет роль snmp-агента, собирает данные о работе сервера/ПК и выдает их в одном ответе, порт подключения check_mk-agent 6556;
- «SNMPv1», «SNMPv2c», «SNMPv2c (без Bulkwalk)»: проверка подключения по разным версиям протокола SNMP (какой протокол SNMP доступен для опроса). На примере выше (Рис. 5.6) доступны все три варианта;
- «трассировка»: показывает маршрут (путь) и временные задержки следования пакетов по сети; данная проверка использует трассировку, чтобы определить текущую маршрутизацию от сервера ТЕСК до целевого хоста¹.

На примере выше (Рис. 5.6) доступны все три версии протокола SNMP. В свойствах данного хоста указан агент «SNMP (Networking device, Appliance)», что соответствует протоколу SNMP v2c. Соответственно, настройка параметров мониторинга хоста выполнены верно.

5.1.4 Просмотр статуса хоста

Чтобы посмотреть текущее состояние хоста в деталях можно нажать кнопку «Статус» в свойствах хоста. В результате откроется окно, подробно отображающее параметры опроса оборудования и информацию о нем (Рис. 5.7), такие как алиас, ip-адрес хоста, хост группы, контактные группы данного хоста, интервал обычной/повторной проверки хоста, тип проверки и т.п.:

¹ При проведении диагностики особо следует обратить внимание не только на доступные версии протокола SNMP, но и на их соответствие типу агентов, указанному в свойствах хоста. Данное соответствие необходимо проверить во избежание проблем с опросом оборудования: в случае, если тип агента и доступная для хоста версия протокола SNMP не совпадают, при постановке на опрос по SNMP, хост будет висеть с сообщением о статусе UNKNOWN для сервиса инвентаризации.

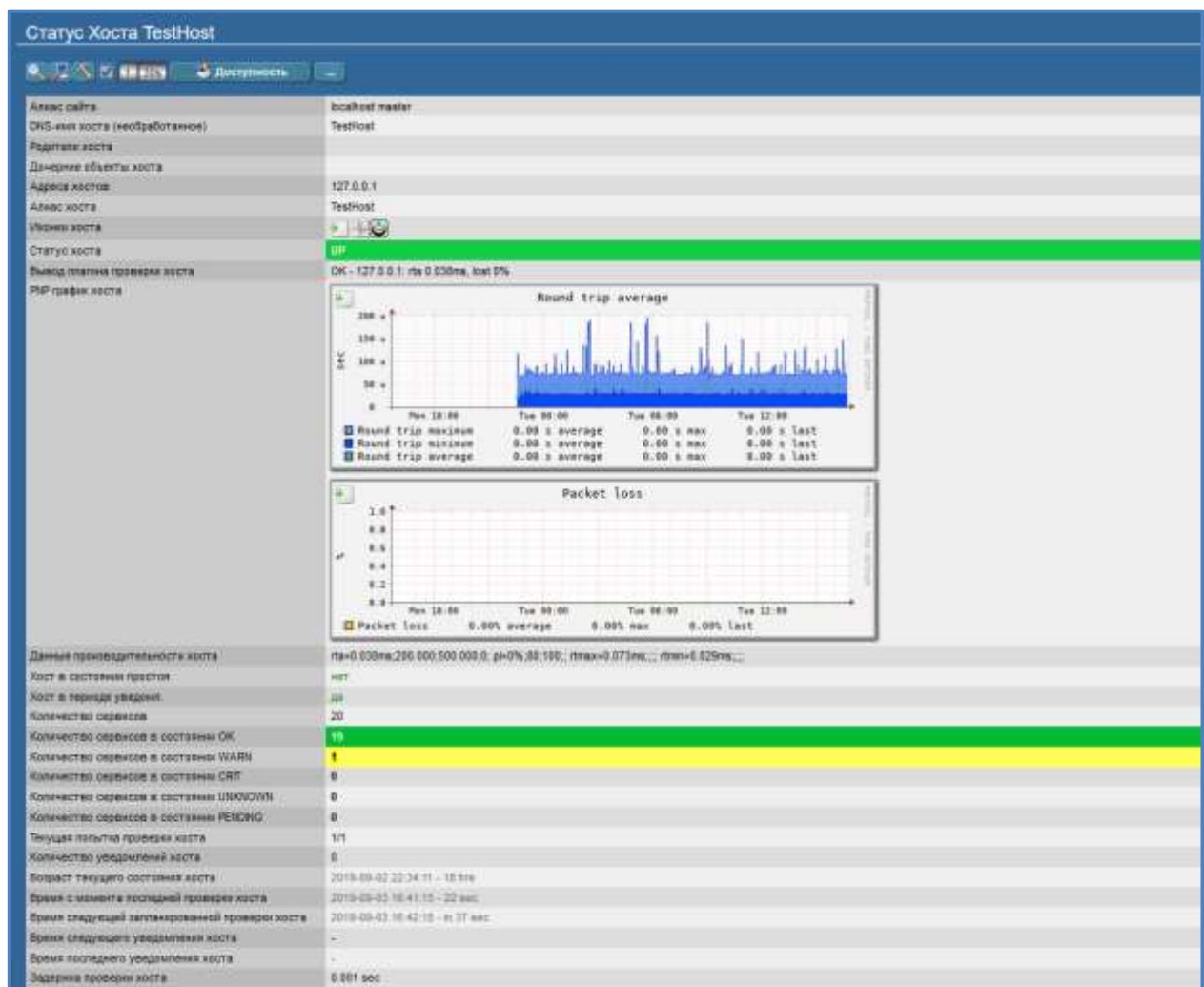


Рис. 5.7 – Просмотр статуса хоста

5.1.5 Поиск хостов по заданным параметрам

Для поиска хостов в заданной папке (или глобально в ТЕСК) по определенным значениям свойств хоста используется кнопка «Поиск» в верхней части окна меню «Хосты». По нажатию на кнопку «Поиск» происходит переход к экранной форме Поиска хостов (Рис. 5.8).

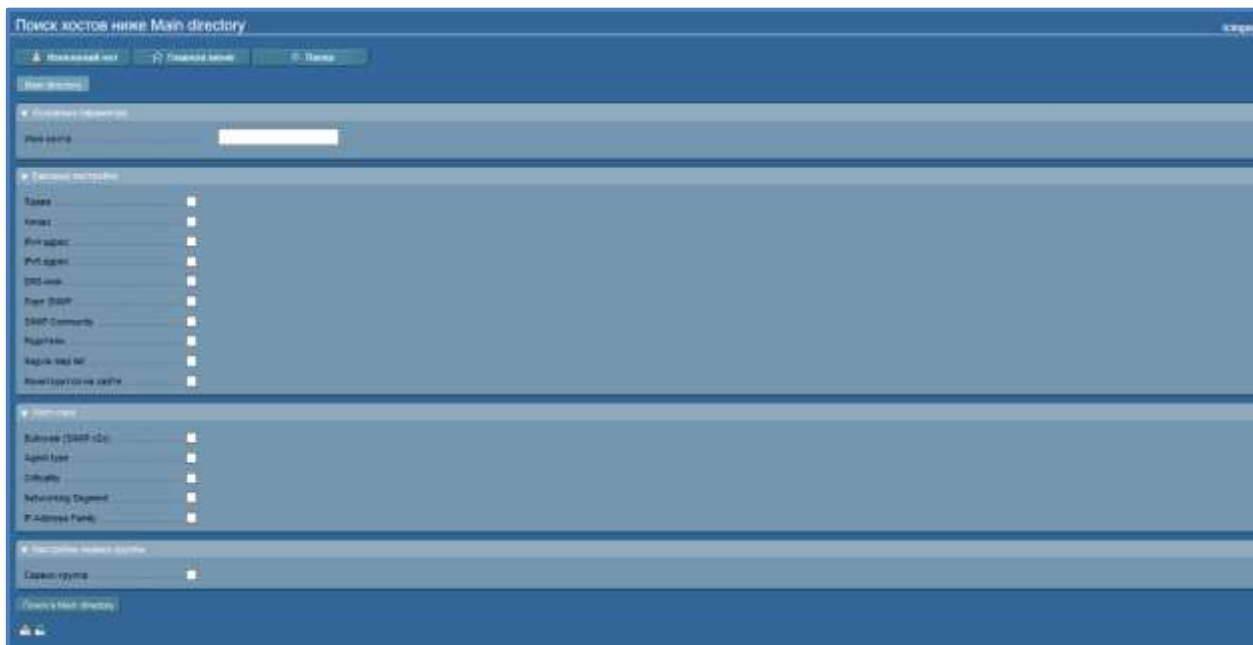


Рис. 5.8 – Экранная форма поиска хоста по указанным параметрам

Экранная форма состоит из следующих блоков:

- «Основные параметры» – поиск осуществляется по имени хоста (если известно);
- «Базовые настройки» – в данном блоке можно указать контактные группы, к которым назначен хост (пункт «права»), алиас, ip-адрес искомого хоста, DNS-имя (это DNS-имя хоста), SNMP-community (если выбран тип агента SNMP), родительский хост, версию прошивки, имя пользователя и пароль для конфигурационных файлов (в случае, когда для хостов включен автоматический сбор конфигурационных файлов). Поиск будет осуществлен по указанному свойству хоста;
- «Хост-теги» – выбирается значение хост-тега для искомого хоста (или хостов). Данный вид поиска наиболее удобен для составления общего списка хостов с заданным хост-тегом. Кроме того, есть возможность организовать поиск хостов с включенным автоматическим сбором конфигурационных файлов по определенному типу протокола (ssh, telnet, snmp). Подробное описание параметров, указанных в этом блоке, описано в главе 5.1.1 настоящего руководства;
- «Настройки сервис-группы» – позволяет осуществить поиск по сервис-группе.

После заполнения необходимых параметров поиска необходимо нажать на кнопку «поиск в Main directory» (может быть указана любая другая папка, из которой инициирован поиск) - поиск в конкретной папке, из которой инициирован поиск.

Результаты поиска по данному хост-тегу «agent type»-> SNMP будут иметь следующий вид (Рис. 5.9).



Рис. 5.9 – Поиск хоста в WATO

Чтобы перейти из окна результатов поиска к нужному хосту, необходимо кликнуть левой кнопкой мышки на его имени. В результате откроются свойства искомого хоста.

5.1.6 Массовое редактирование хостов

Массовое редактирование хостов доступно на экранной форме просмотра перечня хостов блока WATO после выбора перечня хостов отметками в чек-боксе, которые становятся доступными по нажатию на пиктограмму , которая находится под списком всего перечня хостов, и последующем нажатии на кнопку «Редактировать» , которая расположена под перечнем всех хостов (Рис. 5.10).

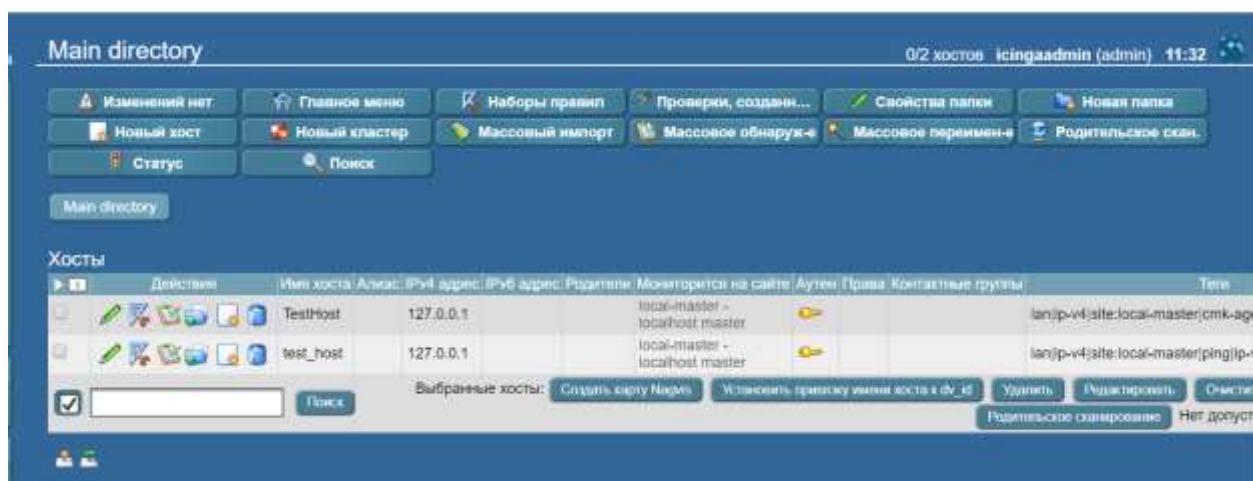


Рис. 5.10 – Просмотр хостов в WATO

Для массового редактирования найденных по заданному признаку хостов необходимо использовать кнопку «Массовое Редактирование» в верхней части экранной формы (подробное описание выполнения поиска хостов описано в п. 5.1.5 настоящего руководства) (Рис. 5.11).

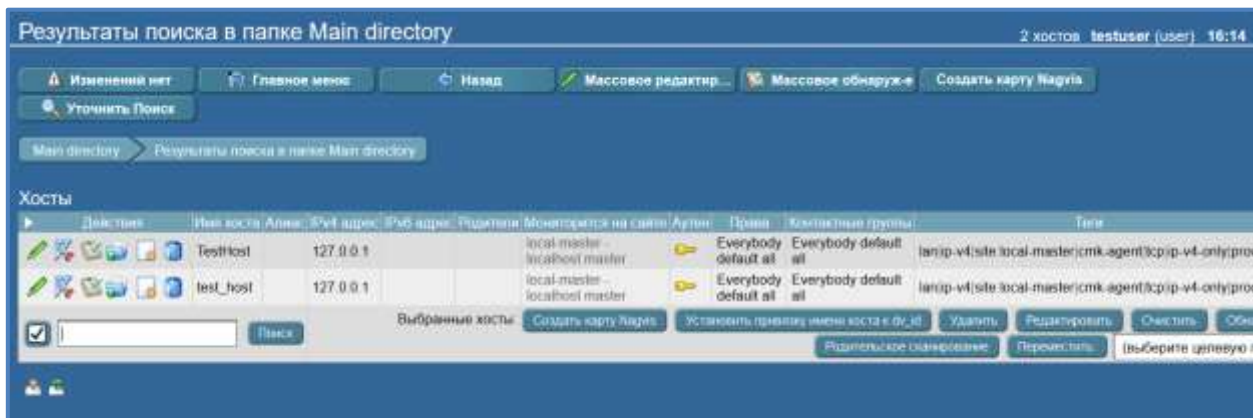


Рис. 5.11 – Просмотр результатов поиска хостов в WATO

По нажатию на кнопку откроется окно с параметрами для массового редактирования хостов (Рис. 5.12). Например, с помощью массового редактирования можно присвоить всем хостам один и тот же хост-тег.

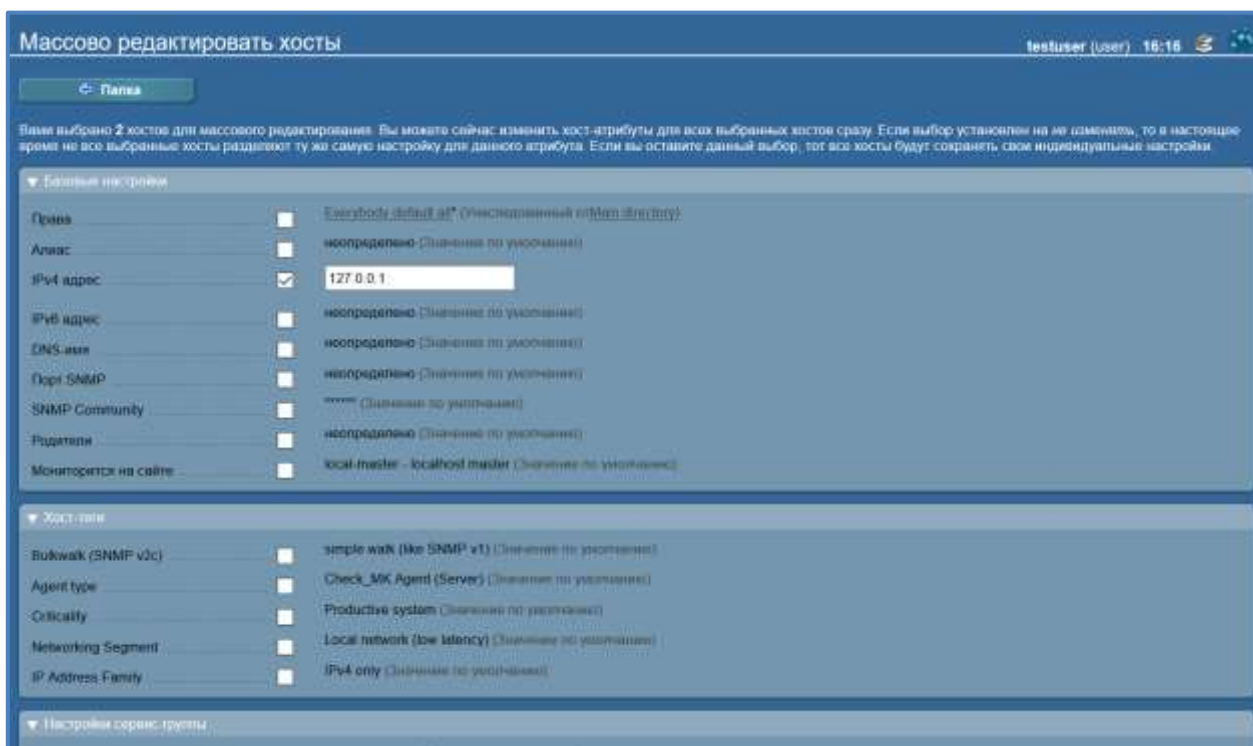


Рис. 5.12 – Экранная форма массового редактирования параметров хостов

В случае, когда те или иные значения параметров отличаются между хостами, в окне массового редактирования высвечивается соответствующее предупреждение. Параметр, общий для всех найденных хостов (по которому производился поиск), также указан в окне массового редактирования (Рис. 5.13).



Рис. 5.13 – Экранная форма массового редактирования параметров хостов 2

После выбора и установки соответствующих параметров для массового редактирования хостов необходимо нажать кнопку «Сохранить & Закончить» в нижней части экранной формы. В результате в левом верхнем углу фрейма «Хосты» будут отображены произведенные изменения в виде надписи «(1,2 и т.д.) Изменений». Количество изменений равно количеству хостов, массово отредактированных после поиска. Данные изменения, как и любые изменения в интерфейсе Check_MK, необходимо активировать либо отменить, если по каким-либо причинам необходимость присвоения выбранных параметров отпала.

5.1.7 Импорт и экспорт хостов в CSV

Импорт CSV данных можно использовать при необходимости загрузить большое количество хостов из другой системы мониторинга или из таблицы Excel. TECK имеет очень гибкий алгоритм чтения файлов подобного формата. Для использования данной функции пользователю потребуется файл, в каждой строке которого есть имя хоста, которое может быть разрешено (распознано) через DNS, пример представлен на рисунке ниже (Рис. 5.14).

```
import.csv
myserver01
myserver02
myserver03
```


Рис. 5.14 – Пример импортируемого CSV файла

Во время импорта также можно принять дополнительные атрибуты. Если в CSV данных имена атрибутов находятся в первой строке, ТЕСК может их автоматически назначить. При импорте данных, пример которых приведен на рисунке ниже (Рис. 5.15), ТЕСК может корректно соотнести все четыре столбца автоматически.²

```
import.csv
hostname;ip address;alias;agent
srvlnx17;10.0.0.10;web99;cmk-agent
srvlnx18;10.0.0.32;Backupserver;cmk-agent
switch47-11;;Backpserver23;snmp-only
```

Рис. 5.15 – Пример импортируемого CSV файла с заголовком

Процедура импорта содержит следующие шаги:

- создать или выбрать целевую папку для импорта;
- перейти в папку и нажать кнопку ;
- в открывшемся диалоговом окне загрузить файл, либо выбрать поле «Content of CSV File» и скопировать содержимое файла в открывшееся поле ввода.
- в диалоговом окне, открывшемся для загрузки данных, отметкой чек-бокса рядом с параметром «Выполнить автоматическое обнаружение сервисов» (Рис. 5.16) можно выполнить автоматическое обнаружение сервисов на вновь импортируемых хостах.

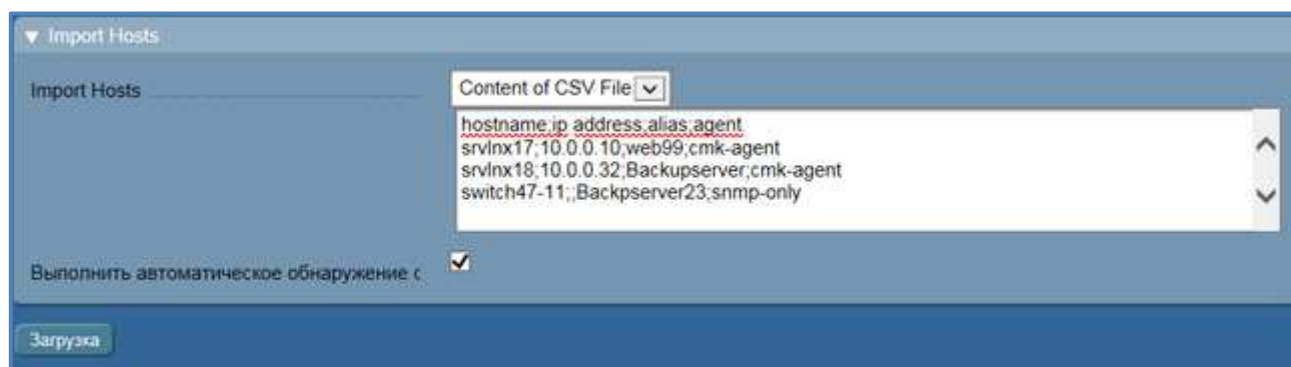


Рис. 5.16 – Массовый импорт хостов

Разделитель полей будет распознан автоматически или его можно ввести вручную (Рис. 5.17). Также в зависимости от содержания файла можно подтвердить опцию – «Имеет строку заголовка».

² Могут быть ситуации, в которых дополнительно потребуется внесение исправлений вручную. Например, идентификаторы (ID) тегов являются компонентами URL-адресов, которые вызывают просмотры, фильтрующие по тегам. WATO не сможет изменить эти URL-адреса. Аналогично, конфигурации фильтров в отчетах и информационных панелях не смогут обновиться автоматически.

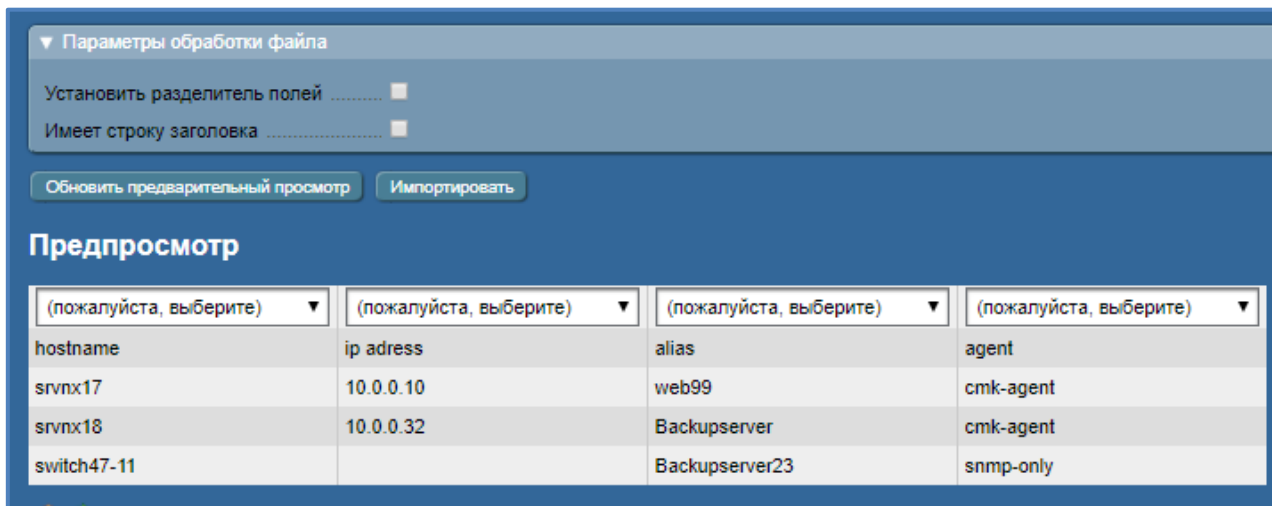


Рис. 5.17 – Разбор CSV файла

Далее необходимо «Обновить предварительный просмотр» для разбора заголовка и автоматического определения типа данных для каждой колонки (Рис. 5.18).

hostname	ip address	alias	agent
Имя хоста	IPv4 Адрес	Алиас	Tag: /Agent type
srvlnx17	10.0.0.10	web99	cmk-agent
srvlnx18	10.0.0.32	Backupserver	cmk-agent
switch47-11		Backupserver23	snmp-only

Рис. 5.18 –Разбор CSV файла с использованием строки заголовка

Если автоматическое распознавание столбцов не работает, ТЕСК позволяет выбрать атрибут, который нужно назначить. В атрибутах хоста в CSV данных важно, чтобы использовалось внутреннее имя атрибута.

Если ранее была выбрана опция «Выполнить автоматическое обнаружение сервисов», то отобразится та же форма, что и при массовом обнаружении (подробное описание представлено в п. 5.1.6 настоящего руководства). После импортирования и завершения автоматического обнаружения сервисов необходимо активировать изменения.

5.1.8 Настройка хостов при распределенном мониторинге

В данном руководстве термин «распределенный мониторинг» применяется, когда система состоит из более чем одного экземпляра.

Для работы с распределенным мониторингом потребуется указать в настройках хоста, каким экземпляром он должен отслеживаться, Master указан по умолчанию.

Обязательный атрибут для этого "Мониторится на сайте". Пользователь может установить его индивидуально для каждого хоста или на уровне папок (Рис. 5.19).

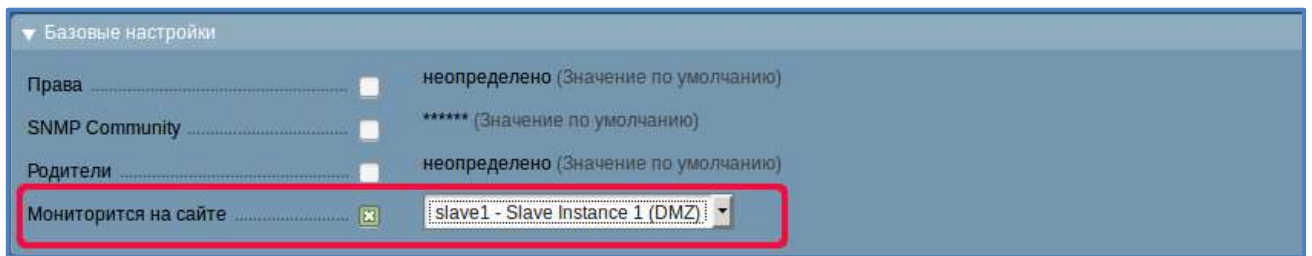


Рис. 5.19 – Параметр в настройках хоста «Мониторится на сайте»

Обнаружение хостов и сервисов не требует дополнительных настроек: наблюдение, а также обнаружение сервисов будут выполняться из соответствующего slave-экземпляра.

5.1.9 Создание нового кластера

ТЕСК позволяет создать новый кластер на экранной форме просмотра созданных хостов. При переходе из WATO Конфигурация в меню «Хосты» по нажатию на кнопку «Новый кластер» открывается экранная форма создания нового кластера (Рис. 5.20).

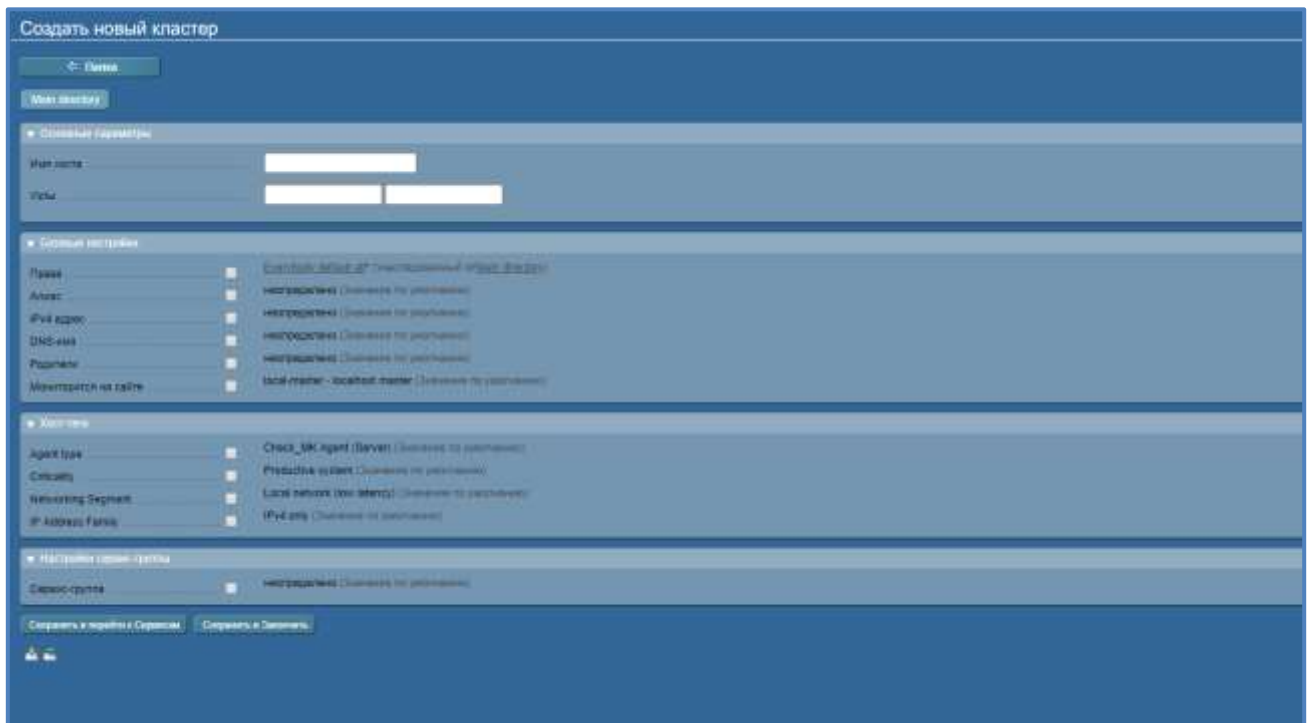


Рис. 5.20 – Экранная форма создания нового кластера

Перечень блоков экранной формы создания нового кластера совпадает с перечнем при создании нового хоста, подробно описанного в п. 5.1.1 настоящего руководства.

В блоке «Основные параметры» требуется указать хосты, которые представлены в WATO и содержат сервисы, которые должны быть включены в кластер при настройке мониторинга.

- «Статус» - по нажатию на кнопку осуществляется переход к экрану просмотра статусов сервисов по выбранному хосту;
- «Свойства» - по нажатию на кнопку осуществляется переход к экрану просмотра свойств хоста с возможностью внесения изменений;
- «Параметры» - по нажатию на кнопку осуществляется переход к экрану параметров заданного хоста;
- «Диагностика» - по нажатию на кнопку осуществляется переход к экрану Диагностики хоста. Подробное описание представлено в п.5.1.3 настоящего руководства;
- «Полное сканирование» - по нажатию на кнопку осуществляется переход к экрану поиска сервисов.

5.2.2 Конфигурирование сервисов

Следующим шагом после создания хоста (описание представлено в п. 5.1.2 настоящего руководства) является конфигурирование его сервисов, подлежащих мониторингу. Для конфигурации сервисов сразу после создания хоста необходимо выбрать опцию «Полное сканирование» в верхней части экрана или нажать кнопку «сохранить & перейти к сервисам» в нижней части экрана, после чего осуществится переход к экрану, где представлены все сервисы хоста, доступные для мониторинга (Рис. 5.23).

Имя сервиса	Статус	Параметры	Детали	Действия
hw_cpu0	OK	HW CPU 0	CPU0 'realtime' in 100.0% in 100% '0'	[OK] [Refresh] [Delete]
hw_cpu1	OK	HW CPU 1	CPU1 'realtime' in 100.0% in 100% '0'	[OK] [Refresh] [Delete]
hw_cpu0m0	OK	HW CPU0M 0	CacheM: ok, Speed:Constant ok, Speed:Status: ok, (Proc:0)ok, (Model:7) ok, (0:0)ok, (PSM:0)ok, (PVE:0)ok	[OK] [Refresh] [Delete]
hw_cpu0m1	OK	HW CPU0M 1	CacheM: ok, Speed:Constant ok, Speed:Status: ok, (Proc:0)ok, (Model:7) ok, (0:0)ok, (PSM:0)ok, (PVE:0)ok	[OK] [Refresh] [Delete]
hw_cpu0m2	OK	HW CPU0M 2	CacheM: ok, Speed:Constant ok, Speed:Status: ok, (Proc:0)ok, (Model:7) ok, (0:0)ok, (PSM:0)ok, (PVE:0)ok	[OK] [Refresh] [Delete]
hw_cpu0m3	OK	HW CPU0M 3	CacheM: ok, Speed:Constant ok, Speed:Status: ok, (Proc:0)ok, (Model:7) ok, (0:0)ok, (PSM:0)ok, (PVE:0)ok	[OK] [Refresh] [Delete]
hw_cpu0m4	OK	HW CPU0M 4	CacheM: ok, Speed:Constant ok, Speed:Status: ok, (Proc:0)ok, (Model:7) ok, (0:0)ok, (PSM:0)ok, (PVE:0)ok	[OK] [Refresh] [Delete]
hw_cpu0m5	OK	HW CPU0M 5	CacheM: ok, Speed:Constant ok, Speed:Status: ok, (Proc:0)ok, (Model:7) ok, (0:0)ok, (PSM:0)ok, (PVE:0)ok	[OK] [Refresh] [Delete]
hw_cpu0m6	OK	HW CPU0M 6	CacheM: ok, Speed:Constant ok, Speed:Status: ok, (Proc:0)ok, (Model:7) ok, (0:0)ok, (PSM:0)ok, (PVE:0)ok	[OK] [Refresh] [Delete]
hw_cpu0m7	OK	HW CPU0M 7	CacheM: ok, Speed:Constant ok, Speed:Status: ok, (Proc:0)ok, (Model:7) ok, (0:0)ok, (PSM:0)ok, (PVE:0)ok	[OK] [Refresh] [Delete]
hw_cpu0m8	OK	HW CPU0M 8	CacheM: ok, Speed:Constant ok, Speed:Status: ok, (Proc:0)ok, (Model:7) ok, (0:0)ok, (PSM:0)ok, (PVE:0)ok	[OK] [Refresh] [Delete]
hw_cpu0m9	OK	HW CPU0M 9	CacheM: ok, Speed:Constant ok, Speed:Status: ok, (Proc:0)ok, (Model:7) ok, (0:0)ok, (PSM:0)ok, (PVE:0)ok	[OK] [Refresh] [Delete]
hw_cpu0m10	OK	HW CPU0M 10	CacheM: ok, Speed:Constant ok, Speed:Status: ok, (Proc:0)ok, (Model:7) ok, (0:0)ok, (PSM:0)ok, (PVE:0)ok	[OK] [Refresh] [Delete]
hw_cpu0m11	OK	HW CPU0M 11	CacheM: ok, Speed:Constant ok, Speed:Status: ok, (Proc:0)ok, (Model:7) ok, (0:0)ok, (PSM:0)ok, (PVE:0)ok	[OK] [Refresh] [Delete]
hw_cpu0m12	OK	HW CPU0M 12	CacheM: ok, Speed:Constant ok, Speed:Status: ok, (Proc:0)ok, (Model:7) ok, (0:0)ok, (PSM:0)ok, (PVE:0)ok	[OK] [Refresh] [Delete]
hw_cpu0m13	OK	HW CPU0M 13	CacheM: ok, Speed:Constant ok, Speed:Status: ok, (Proc:0)ok, (Model:7) ok, (0:0)ok, (PSM:0)ok, (PVE:0)ok	[OK] [Refresh] [Delete]
hw_cpu0m14	OK	HW CPU0M 14	CacheM: ok, Speed:Constant ok, Speed:Status: ok, (Proc:0)ok, (Model:7) ok, (0:0)ok, (PSM:0)ok, (PVE:0)ok	[OK] [Refresh] [Delete]
hw_cpu0m15	OK	HW CPU0M 15	CacheM: ok, Speed:Constant ok, Speed:Status: ok, (Proc:0)ok, (Model:7) ok, (0:0)ok, (PSM:0)ok, (PVE:0)ok	[OK] [Refresh] [Delete]

Рис. 5.23 – Перечень доступных сервисов хоста

Когда хост включен впервые и его сервисы еще не настроены или на хосте обнаружен сервис, неконтролируемый в настоящее время, все обнаруженные сервисы отображаются в категории «Имеющиеся (отсутствующие) сервисы» (Рис. 5.24):

Статус	Плагин проверки	Часть имени	Имя Сервиса	Вывод плагина	Параметры Проверки		
OK	disco_cpu	None	CPU utilization	42.0% utilization in the last 5 minutes	80.0%, 90.0%	✘	☑
OK	disco_fan	Switch 1 Fan 1	FAN Switch 1 Fan 1	State is: normal (1)		✘	☑
OK	disco_mem	Driver text	Mem used Driver text	0.0% (40.00 B) of 1.00 MB used	80.0%, 90.0%	✘	☑
WARN	disco_mem	I/O	Mem used I/O	83.6% (11.71 MB) of 14.00 MB used (warning at 80%)	80.0%, 90.0%	✘	☑
OK	disco_mem	Processor	Mem used Processor	36.9% (26.04 MB) of 70.49 MB used	80.0%, 90.0%	✘	☑
OK	disco_power	Sw1 1006	Power Sw1 1006	state: normal, source: AC		✘	☑
OK	disco_temperature	SW 1 Sensor 1	Temperature SW 1 Sensor 1	24 °C	(нет параметров)	✘	☑

Рис. 5.24 – Блок «Имеющиеся сервисы»

Обычный способ добавления их к мониторингу - сохранить полученный список сервисов с помощью кнопки **Сохранить ручную конфигурацию проверки**, затем «Применить изменения», и хост с перечнем сервисов будет находиться в режиме мониторинга.

Для подтверждения игнорирования данного сервиса необходимо нажать кнопку «Сохранить ручную конфигурацию проверки» в окне общего списка сервисов хоста. Чтобы вернуть уже найденные и настроенные сервисы, но отмеченные для временного игнорирования, в общий список сервисов хоста, необходимо нажать кнопку «Полное сканирование» (Рис. 5.24). В этом случае информация по сервисам хоста будет взята не из кэш-файла, из результата реального сканирования. Затем снять отметку в чек-боксе для исключения сервисов из мониторинга и сохранить ручную конфигурацию (либо выбрать кнопку «Активировать отсутствующие» - тогда сервисы автоматически будут добавлены на опрос); активировать исключенные из мониторинга сервисы можно также с помощью кнопки «Автоматическое обновление (tabula rasa)»³.

При сохранении конфигурации для опроса нажатием на кнопку «Сохранить ручную конфигурацию проверки» данная конфигурация сервисов будет задана статически, и опрос будет производиться только по указанным сервисам. Настройка периодов обнаружения новых сервисов хоста выполняется в блоке параметрах хоста блок «Конфигурация мониторинга». По умолчанию период обнаружения сервисов – 2 часа, конфигурация сервисов обновляется с помощью сервиса `check_mk inventory`.

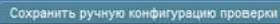
Использование кнопки «Сохранить ручную конфигурацию проверки» чаще всего используется для устройств, имеющих стабильное количество сервисов, обнаруженных в основном при первой инвентаризации и практически не меняющихся с течением времени.

5.2.3 Удаление нежелательных сервисов

ТЕСК позволяет исключить сервисы объектов, которые не требуется отслеживать следующими способами:

- временное отключение сервисов

³ В случае использования «Автоматическое обновление (tabula rasa)» конфигурация *всех* сервисов хоста будет выполнена заново

Для временного исключения сервиса из мониторинга требуется снять чек-боксы тех сервисов, мониторинг которых не требуется, а затем сохранить изменения, нажав на кнопку . После исключения сервисов из мониторинга необходимо так же применить изменения либо отклонить. Этот способ предназначен только для временных и мелких действий, поскольку отмененные таким образом сервисы будут отмечены ТЕСКом как отсутствующие, а проверка обнаружения будет неудачной.

- постоянное отключение сервисов




Постоянно игнорировать определенные сервисы можно с помощью набора правил «Отключенные сервисы». Метод постоянного отключения сервисов позволяет не только исключить отдельные сервисы из мониторинга, но и сформулировать правила такого типа, как: «файловые системы на тестовых системах, которые начинаются с /mnt / dsk, не должны мониториться». По нажатию на пиктограмму  на панели строки сервиса (Рис. 5.25) происходит переход к странице параметров сервисов (так же переход может быть осуществлен через боковую панель WATO-Конфигурация меню « Хост- & Сервис-параметры модуля WATO»).



Рис. 5.25 – Панель строки сервиса

При нажатии на кнопку  в строке сервиса осуществляется переход непосредственно к созданию нового правила, которое будет предварительно заполнено для текущей папки, хоста и сервиса (Рис. 5.26).

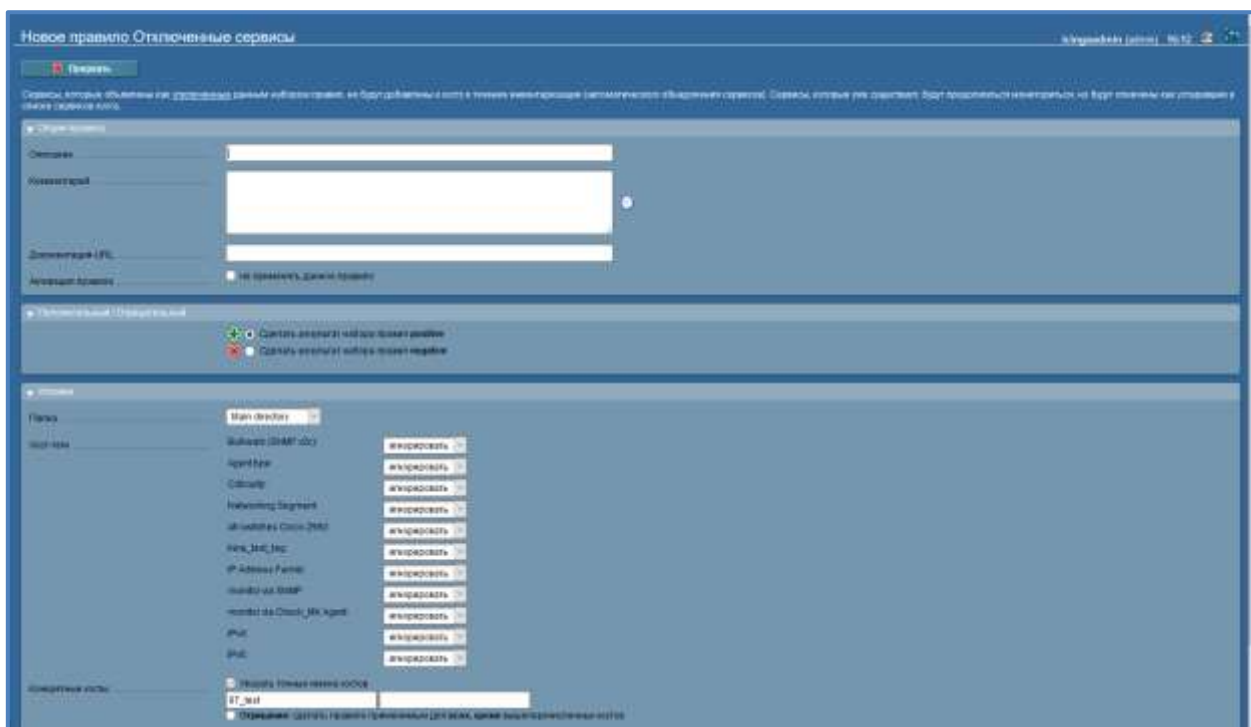



Рис. 5.26 – Форма создания правила

5.2.4 Настройка сервисов вручную

ТЕСК предоставляет возможность создания сервисов вручную. Для этого необходимо перейти в меню  - «Проверки, созданные вручную» в модуле WATO-конфигурация. В основе данного раздела лежит коллекция наборов правил, которые полностью соответствуют набору правил, используемых для настройки параметров этих проверок.

Проверки создаются для хостов, а не для сервисов. Сервисы будут созданы автоматически в результате отработки этих правил.

При настройке правил потребуется выбрать плагин, который будет использоваться для проверки, поскольку автоматического обнаружения сервисов производиться не будет.

Следующий пример показывает основную часть правила – «Состояние синхронизации времени NTP» в разделе «Проверки, созданные вручную» (Рис. 5.27). При создании правила необходимо вручную указать плагин проверки, его параметры, если требуется, и пороговые значения.

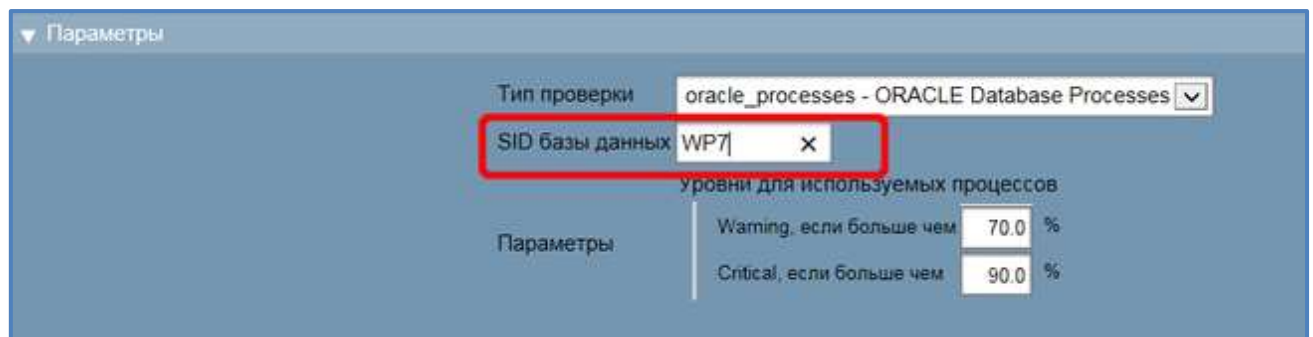


Рис. 5.27 – Создание ручной проверки



Сервис, определенный таким образом, будет установлен на всех хостах, к которым применяется это правило.

Если после запуска такого сервиса агент уведомляет, что запрошенный сервис не запускается или имеет проблемы, то сервис помечается как CRIT или UNKNOWN. Если агент вообще не предоставляет никакой информации, например, потому что не может получить никаких результатов проверки, сервис, созданный в результате настройки ручной проверки, остается в состоянии PEND, а сервис Check_MK переходит в состояние WARN с уведомлением о том, что отсутствует соответствующий раздел в данных агента.

5.2.5 Пассивные сервисы

Пассивные сервисы - это те сервисы, которые активно не иницируются ТЕСКом, результаты проверки регулярно направляются из внешних источников в ТЕСК. Обычно это происходит через командный канал ядра.

В интерфейсе ТЕСК представлены 2 вида значков прохождения проверок для сервисов:

-  - сервисы являются «активными проверками», которые выполняются непосредственно ТЕСКом;
-  - сервисы, для которых результаты проверки получены из общей активной проверки «Check_MK».


Данное разделение значков сделано для повышения производительности и является особенностью ТЕСК.

5.3 Обработка аварий

Для проблем DOWN, UNREACH, WARN, CRIT или UNKNOWN ТЕСК различает два возможных состояния: необработанная и обработанная проблема.

Понятие обработанные (подтвержденные) проблемы подразумевает, что решением проблем уже занимается оператор.

Если проблема была подтверждена, то:

- она будет идентифицирована с помощью символа ;
- проблема будет исключена из списка новых (необработанных) проблем в Тактическом обзоре;
- никаких дальнейших уведомлений по ней отправлено не будет.

5.3.1 Процедура подтверждения

Просмотр перечня проблем на хостах доступен в перечне обзоров, представленных в боковой панели меню «Текущее состояние» -> «Проблемы». Проблемы хоста/сервиса доступны на формах просмотра «Проблемы хоста» и «Проблемы сервиса». Для подтверждения проблемы хоста/сервиса на экранных формах «Проблемы хоста» и «Проблемы сервиса» необходимо



нажать на иконку  в строке хоста/сервиса (Рис. 5.28) либо с помощью команд на затронутых хостах/сервисах (Рис. 5.29) на экранных формах, где отображается меню «команды» . Так же через меню команды Пользователь может удалить подтверждения, по нажатию на кнопку «Удалить подтверждение» в развернутой форме «Команды» (Рис. 5.29).



Рис. 5.28 – Подтверждение проблемы сервиса в статусе хоста

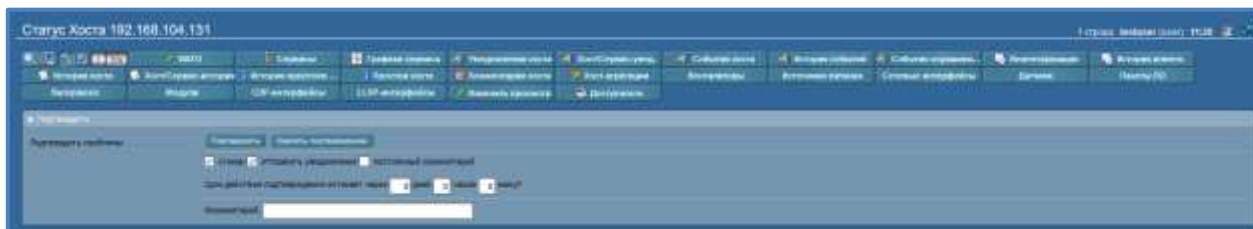


Рис. 5.29 – Подтверждение проблемы сервиса через команду

В меню, доступном при нажатии на пиктограмму «Команды» доступен следующий перечень опций, представленный в таблице ниже (см. Табл. 5.1).

Табл. 5.1 – Описание процедуры подтверждения

Название	Описание
Стикер	Подтверждение действует до следующего изменения статуса . Если, например, сервис был подтвержден со статусом WARN, и позже статус изменился на CRIT, подтверждение будет автоматически удалено. Отметка в чек-боксе рядом с параметром стикер сохранит подтверждение до тех пор, пока не будут достигнуты статусы OK или UP .
Отправить уведомление	Всем контактам, привязанным к хосту/сервису, для которых настроено оповещение о подтверждении проблемы хоста/сервиса, отправляется уведомление: «Подтверждение проблемы хоста/сервиса».
Постоянный комментарий	С помощью этой опции комментарий не будет автоматически удален, если подтверждение исчезнет или будет удалено. Комментарии, введенные таким образом, могут быть удалены только вручную.
Срок действия подтверждения истекает через ...	С помощью этой опции может быть установлен лимит времени для сохранения подтверждения. Когда срок истекает, подтверждение автоматически удаляется, даже если хост/сервис еще не достигли статуса OK или UP.

5.3.2 Отображение подтверждения в ТЕСК


В веб-интерфейсе ТЕСК есть несколько возможностей для отображения подтверждений.

Во всех просмотрах хостов и сервисов подтвержденные проблемы обозначаются двумя символами:

-  - символ обозначает подтверждение (Рис. 5.30);



Рис. 5.30 – Отображение подтверждения

-  - при нажатии на этот символ отображается список с комментариями подтверждения (Рис. 5.31).

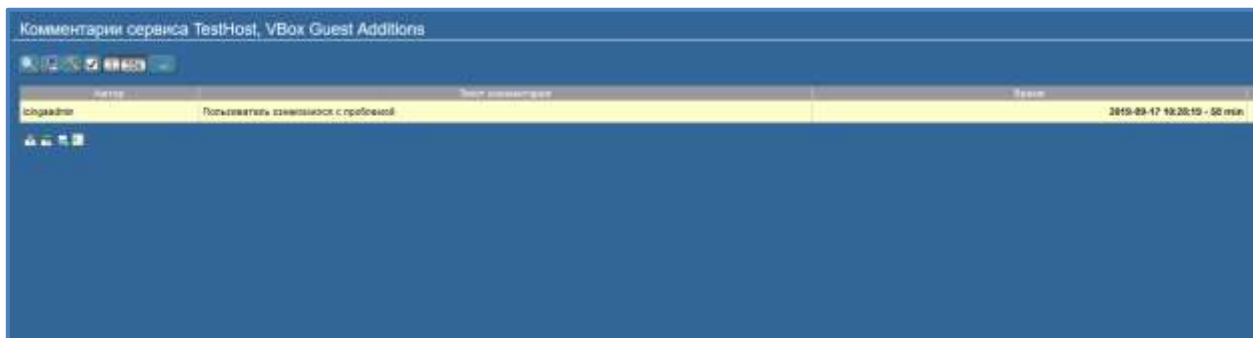


Рис. 5.31 – Комментарии подтвержденной проблемы

В разделе «Комментарии» («Текущее состояние» -> «Другое» -> «Комментарии») отображается список всех комментариев для хостов и сервисов, в том числе те, которые создаются с помощью подтверждений. Комментарии могут быть удалены с помощью команд. Удаление комментария не оказывает никакого влияния на зарегистрированные подтверждения.

5.4 НАСТРОЙКА КОНСОЛИ СОБЫТИЙ

5.4.1 Просмотры событий

Доступ к этому отображению осуществляется через просмотр «Текущее состояние» -> «Консоль Событий» -> «События». Этот просмотр можно настроить, как и все остальные просмотры. Отображаемые события могут быть отфильтрованы, выполнены команды по ним и т.д. (Рис. 5.32).

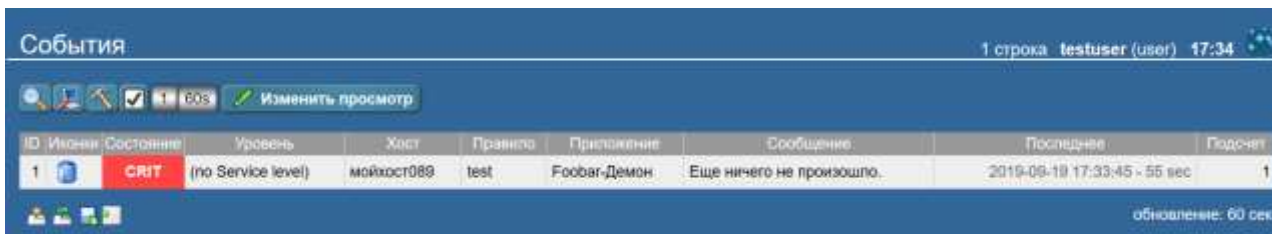




Рис. 5.32 – Просмотр событий

При нажатии на ID события откроются подробные сведения о нем (Рис. 5.33).

помощью иконки «Команды» . С помощью  чекбоксов можно также выполнять команды с несколькими событиями одновременно (Рис. 5.34).

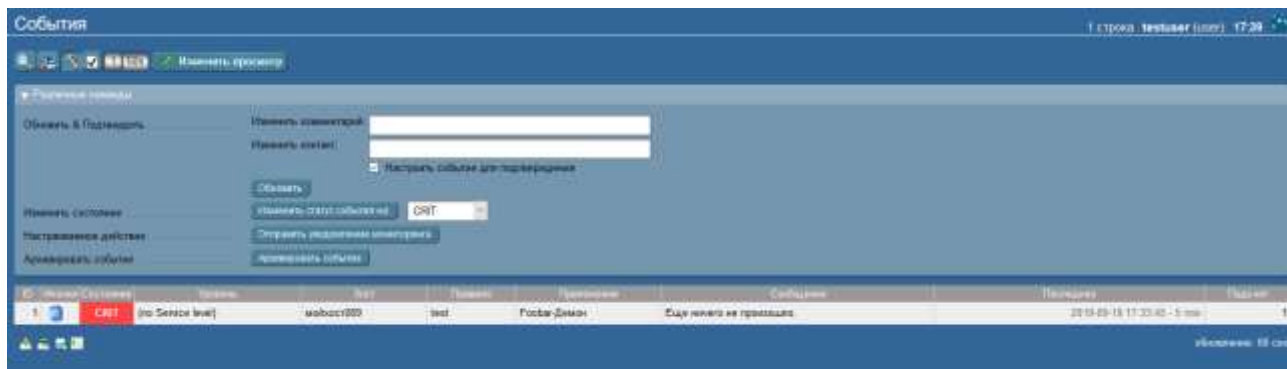


Рис. 5.34 – Команды блока просмотра событий

Доступны следующие команды:

- «Обновить & Подтвердить»;

Используя кнопку «Обновить», одним действием может быть добавлен комментарий к событию, назначено контактное лицо и подтверждено событие.

Чекбокс «Настроить событие для подтверждения» переводит событие в статус подтвержденного, и с этого момента событие считается обработанным. Это аналог подтверждения проблем хостов и сервисов.

Более позднее выполнение команды без выбора чекбокса удаляет подтверждение.

- «Изменение состояния» - кнопка «Изменить состояние» позволяет переклассифицировать событие вручную, например, с CRIT на WARN;
- «Выполнение действий» - с помощью «Настраиваемых действий» можно разрешить выполнение свободно определяемых действий над событиями.

По умолчанию доступно только действие «Отправить уведомление мониторинга». Оно отправляет уведомление модуля мониторинга, которое будет обработано точно так же, как уведомление от активно отслеживаемого сервиса. Уведомление проходит через правила уведомлений и, при необходимости, генерирует электронные письма, SMS или иное уведомление, которое было настроено. Более подробная информация об уведомлениях через Консоль событий будет предоставлена ниже.

- Кнопка «Архивировать событие» окончательно удаляет событие из списка открытых событий;

Архивирование отдельных событий также легко выполняется из списка

событий с помощью символа .

5.4.3 Видимость событий

В Консоли событий ситуация такова, что сначала не существует назначения событий контактными группам – так как заранее фактически неизвестно, какие сообщения можно получить. Неизвестен список хостов, поскольку сокет для Syslog и SNMP доступен извне. По этой причине существует несколько особенностей, связанных с видимостью в Консоли событий:

Изначально всем пользователям разрешено видеть все события, если предварительно пользователем с ролью «Администратор» не изменены настройки роли.

Назначение хоста в «Консоли событий» обрабатывается в следующем порядке:

- если в событии не было идентифицировано имя хоста, в качестве имени хоста будет использоваться его IP-адрес;
- затем имя хоста события будет без учета регистра сравниваться всеми именами хостов, алиасами хостов и IP-адресами хостов в мониторинге;
- если такой хост найден, его контактные группы будут приняты для события и использованы для контроля видимости;
- если хост не найден, контактные группы, если они настроены, будут приняты из правила, которое сгенерировало событие;
- если группы там также не были назначены, Пользователю будет разрешено видеть событие только в том случае, если у него есть право «Видеть события, не связанные с известным хостом», доступное к настройке Администратору (подробное описание представлено в документе «Руководство пользователя с правами Администратор» в п. 4.8).

Пользователь может повлиять на назначение при одной возможности: если контактные группы были определены в наборе правил и хост может быть назначен.

5.4.4 Просмотр состояний событий в активном мониторинге

Для отображения в активном мониторинге хостов, которые имеют открытые проблемные события, на каждом хосте требуется добавить активную проверку, которая суммирует текущие состояния событий. Для хоста, не имеющего открытых событий, она будет выглядеть так, как представлено на Рис. 5.35.

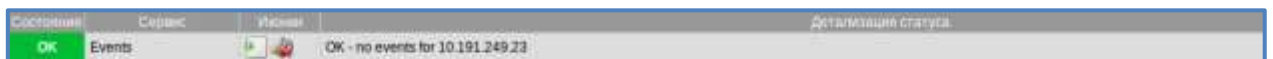


Рис. 5.35 – Сервис просмотра состояний событий

Если присутствуют только события с состоянием **OK**, проверка покажет количество событий, но останется в статусе **OK**.

На рисунке ниже приведена ситуация с открытыми событиями в состоянии **CRIT** (Рис. 5.36):

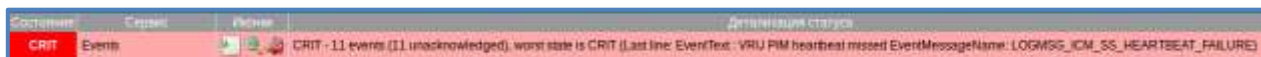


Рис. 5.36 – Сервис просмотра состояний событий CRIT

Данная активная проверка создается с помощью правила в меню «Хост-& Сервис-параметры» - «Консоль Событий» - набор правил «Проверить статус события в консоли событий». При использовании этого правила можно также указать, следует ли добавлять в статус уже подтвержденные события (Рис. 5.37).

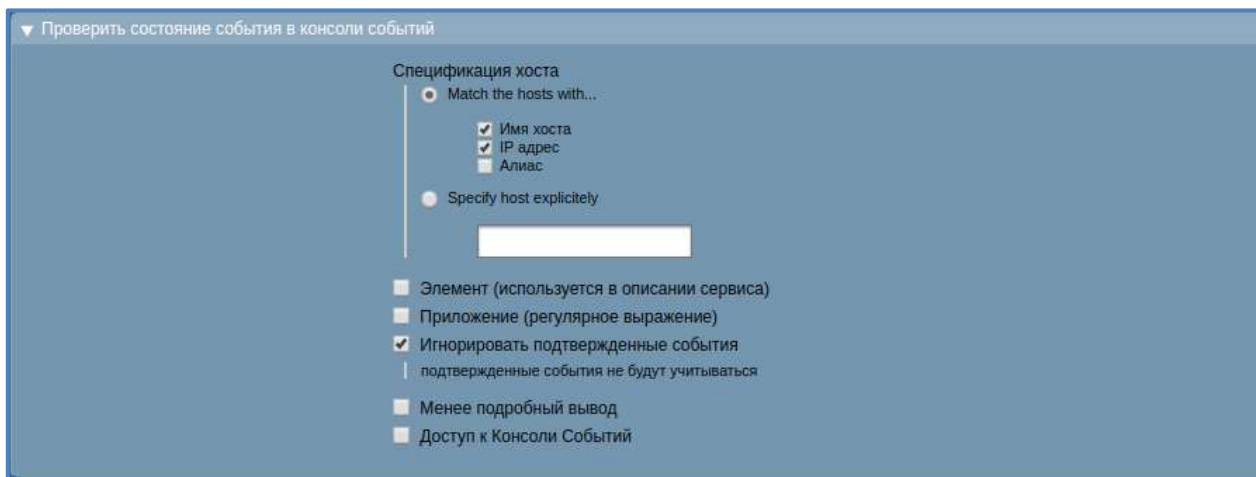


Рис. 5.37 – Создание правила «Проверить статус события в консоли событий»

Если консоль событий запущена не на том же экземпляре ТЕСК, который отслеживает состояние хоста, потребуется удаленный доступ по протоколу TCP через настройку параметра «Доступ к Консоли Событий» (Рис. 5.38), который доступен в блоке «Проверить статус события в консоли событий» настраиваемого правила.

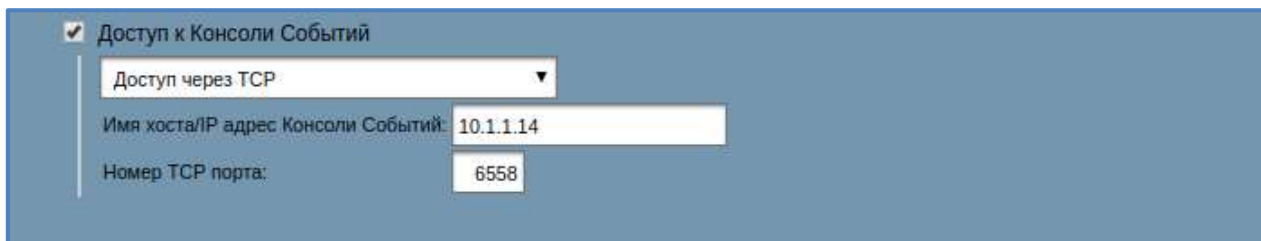


Рис. 5.38 – Настройка доступа к консоли событий

Для того, чтобы это работало, консоль событий должна разрешать доступ по протоколу TCP. Этот доступ может настроить в параметрах настройки консоли событий пользователь с ролью «Администратор» (Подробное описание представлено в документе «Руководство пользователя с правами Администратор» в п. 4.10).

5.4.5 Переадресация Консоли Событий «Logwatch»

Чтобы сообщения, обнаруженные плагинами, больше не мониторились обычной проверкой Logwatch, а передавались один за другим на консоль событий для обработки требуется настроить правило в меню «Хост- & Сервис-Параметры» - «Параметры обнаруженных Сервисов» - «Приложения,



Рис. 5.40 – Блок переадресация

Пользователю доступны следующие параметры для настройки:

- При установке отметки в чек-боксе «Ограничить лог-файлы (префикс, соответствующий регулярному выражению)» - Поле для указания имени элементов лог-файлов становится доступно, например, «System\$», чтобы выбрать сервис «LOG System». При заполнении поля возможно использование регулярных выражений, которые должны соответствовать началу имени лог-файла.
- В подблоке «Способ переадресации» можно выбрать «Отправить события на локальную консоль событий» или «Отправлять события на другой syslog-сервер». При выборе опции «Отправлять события на другой syslog-сервер» потребуется указать Протокол, Адрес сервера и порт. При распределенном мониторинге, в котором не каждый экземпляр запускает свою собственную консоль событий и удаленные экземпляры должны перенаправлять сообщения на центральную консоль через syslog. Протокол UDP является значением по умолчанию для этой процедуры, в связи с тем, что этот протокол не является безопасным, рекомендуется использовать syslog-сервер через TCP-протокол.
- В подблоке «Syslog категория переадресованных сообщений» требуется указать категорию, которая будет использована в случаях, когда категория не может быть извлечена из сообщения при переадресации сообщений.
- При установке отметки чек-бокса в подблоке «Мониторинг перенаправленных лог-файлов» проверка будет мониторить список переадресованных лог-файлов и будет направлять предупреждения, если в какое-либо время лог-файл будет отсутствовать или будет превышен по сравнению с первоначальным списком, который был зафиксирован во время обнаружения сервисов. Требуется провести повторную инвентаризацию данной проверки, чтобы перевести ее снова в состояние ОК.
- При установке отметки чек-бокса в подблоке «Список ожидаемых лог-файлов» проверка будет сверять, чтобы все лог-файлы, перечисленные в этом пункте, были сообщены с помощью отслеживаемой системы.

- При установке отметки чек-бокса в подблоке «Переклассифицировать сообщения до отправки их на Консоль Событий», строки logwatch переклассифицируются с помощью шаблонов logwatch прежде чем будут отправлены на консоль событий. Если в соответствии с шаблоном logwatch отдельные строки будут классифицированы со статусом IGNORE, то они не будут перенаправлены на консоль событий. Переклассификация каждой строки учитывает, от какого лог-файла возникает сообщение.
- При установке отметки чек-бокса в подблоке «Создать отдельную проверку для каждого лог-файла» будет создана одна отдельная проверка для каждого лог-файла, созданного во время обнаружения сервисов. Данная опция также изменяет поведение для неизвестных лог-файлов. По умолчанию, проверка logwatch перенаправляет все лог-файлы на консоль событий, даже лог-файлы, которые не были известны во время обнаружения сервисов. Эта созданная проверка по лог-файлу изменяет данное поведение так, что любые данные из неизвестных лог-файлов сбрасываются.

Блок «Условия»

В этом блоке можно определить, к каким хостам или сервисам должны применяться правила (Рис. 5.41). Здесь есть три различных условия, все из которых должны быть выполнены, чтобы правило применялось. Условия связаны между собой логическим И.

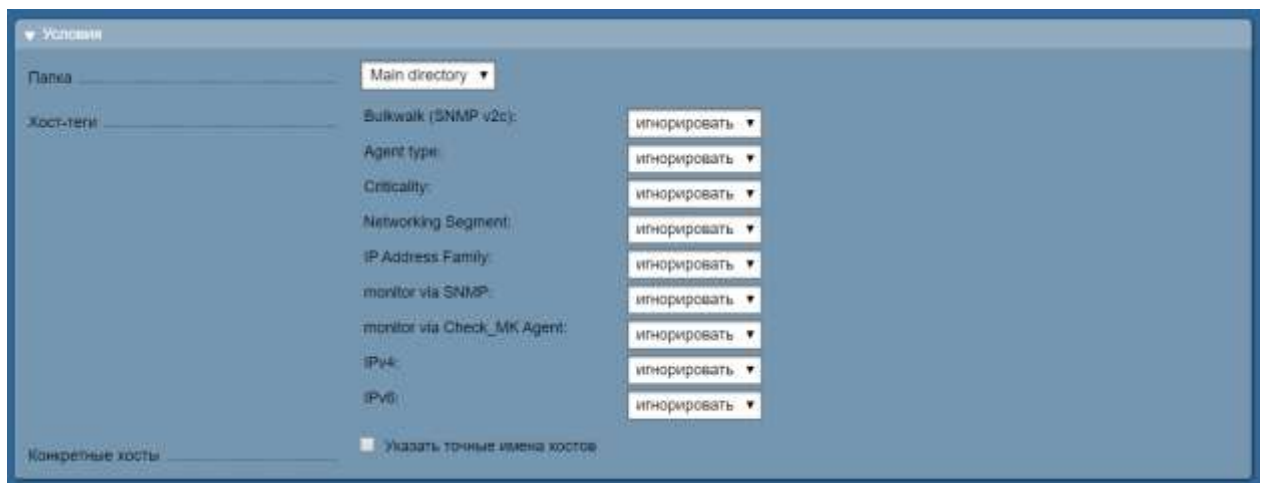


Рис. 5.41 – Блок «Условия»

- Папка Правило должно применяться только к хостам указанной в этом пункте папки.
- «Хост-теги» - Ограничивают правила хостами в зависимости от того, имеют ли они - или не имеют - конкретные хост-теги. Здесь также всегда используется связь через логическое И.
- «Конкретные хосты» - Этот тип условия предназначен для правил исключений. При указании конкретных хостов правило будет применено только к выбранным хостам. Через опцию «Отрицание» может быть определено обратное исключение. С помощью него можно исключить из этого правила конкретно названные хосты.

При завершении заполнения формы требуется сохранить все внесенные изменения нажатием на кнопку «Сохранить» в нижней части экранной формы.

Правило становится активным только через обнаружение сервисов. Пока не будет выполнено обнаружение сервисов, существующие сервисы logwatch будут удалены и заменены на каждом хосте недавно созданным сервисом с именем Переадресация журнала (Log Forwarding) (Рис. 5.42).

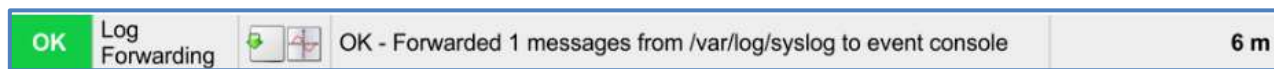


Рис. 5.42 – Сервис с именем «Переадресация журнала (Log Forwarding)»

ПЕРЕЧЕНЬ РИСУНКОВ

Рис. 2.1 – Ядро мониторинга Nagios	11
Рис. 2.2 – Архитектурное решение ТЕСК	13
Рис. 3.1 – Форма авторизации.....	14
Рис. 3.2 – Экранная форма «Главный обзор».....	15
Рис. 4.1 – Боковая панель	16
Рис. 4.2 – Блок боковой панели «Тактический обзор».....	17
Рис. 4.3 – Быстрый поиск	17
Рис. 4.4 – Блок боковой панели «Текущее состояние»	17
Рис. 4.5 – Блок «Закладки».....	18
Рис. 4.6 – Блок «WATO конфигурация»	19
Рис. 4.7 – Главное меню	19
Рис. 4.8 – Экранная форма раздела «Хосты»	19
Рис. 4.9 – Экранная форма раздела «Хост- и Сервис-параметры»	20
Рис. 4.10 – Экранная форма блока «Проверки, созданные вручную».....	21
Рис. 4.11 – Каталог плагинов проверки	21
Рис. 4.12 – Экранная форма «Анализатор шаблонов лог-файлов».....	21
Рис. 4.13 – Экранная форма блока «Business Intelligence»	22
Рис. 4.14 – Экранная форма «Агенты и плагины».....	22
Рис. 4.15 – Информационная панель «Главный обзор».....	23
Рис. 4.16 – Режим редактирования дашборда	23
Рис. 4.17 – Редактирование информационной панели. Меню «Добавить dashlet».....	24
Рис. 4.18 – Редактирование информационной панели. Добавление нового элемента	25
Рис. 4.19 – Пример контекстного меню для добавления элемента на информационную панель	25
Рис. 4.20 – Меню выбора информационной панели.....	25
Рис. 4.21 – Меню редактирования просмотров.....	26
Рис. 4.22 – Меню редактирования информационных панелей	26
Рис. 4.23 – Форма создания информационной панели – выбор источника данных	26
Рис. 4.24 – Форма создания информационной панели. Блок «Основные параметры»	27

Рис. 5.1 – Блок «WATO конфигурация»	28
Рис. 5.2 – Экранная форма раздела «Хосты»	28
Рис. 5.3 – Экран просмотра «Свойства хоста».....	30
Рис. 5.4 – Свойства хоста	32
Рис. 5.5 – Экранная форма «Диагностика хоста»	33
Рис. 5.6 – Выполнение проверки на экранной форме «Диагностика хоста» ...	33
Рис. 5.7 – Просмотр статуса хоста.....	35
Рис. 5.8 – Экранная форма поиска хоста по указанным параметрам	36
Рис. 5.9 – Поиск хоста в WATO.....	37
Рис. 5.10 – Просмотр хостов в WATO	37
Рис. 5.11 – Просмотр результатов поиска хостов в WATO	38
Рис. 5.12 – Экранная форма массового редактирования параметров хостов ..	38
Рис. 5.13 – Экранная форма массового редактирования параметров хостов	239
Рис. 5.14 – Пример импортируемого CSV файла	39
Рис. 5.15 – Пример импортируемого CSV файла с заголовком	40
Рис. 5.16 – Массовый импорт хостов.....	40
Рис. 5.17 – Разбор CSV файла	41
Рис. 5.18 –Разбор CSV файла с использованием строки заголовка.....	41
Рис. 5.19 – Параметр в настройках хоста «Мониторится на сайте»	42
Рис. 5.20 – Экранная форма создания нового кластера	42
Рис. 5.21 – Просмотр перечня сервисов через Check_MK inventory	43
Рис. 5.22 – Сервисы хоста	43
Рис. 5.23 – Перечень доступных сервисов хоста	44
Рис. 5.24 – Блок «Имеющиеся сервисы»	45
Рис. 5.25 – Панель строки сервиса	46
Рис. 5.26 – Форма создания правила	46
Рис. 5.27 – Создание ручной проверки	47
Рис. 5.28 – Подтверждение проблемы сервиса в статусе хоста	48
Рис. 5.29 – Подтверждение проблемы сервиса через команду	49
Рис. 5.30 – Отображение подтверждения	49
Рис. 5.31 – Комментарии подтвержденной проблемы	50
Рис. 5.32 – Просмотр событий	50
Рис. 5.33 – Детали события	51
Рис. 5.34 – Команды блока просмотра событий	52

Рис. 5.35 – Сервис просмотра состояний событий	53
Рис. 5.36 – Сервис просмотра состояний событий CRIT	54
Рис. 5.37 – Создание правила «Проверить статус события в консоли событий»	54
Рис. 5.38 – Настройка доступа к консоли событий	54
Рис. 5.39 – Новое правило «Переадресация Консоли Событий Logwatch».....	55
Рис. 5.40 – Блок переадресация	56
Рис. 5.41 – Блок «Условия»	57
Рис. 5.42 – Сервис с именем «Переадресация журнала (Log Forwarding)»	58

ПЕРЕЧЕНЬ ТАБЛИЦ

Табл. 1.1 - Термины и сокращения.....	5
Табл. 5.1 – Описание процедуры подтверждения	49
Табл. 5.2 – Основные данные событий консоли событий	51