ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
МОРДОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМ. Н. П. ОГАРЁВА»**

Институт электроники и светотехники

Кафедра инфокоммуникационных технологий и систем связи

УТВЕРЖДАЮ

Зав. кафедрой
канд. техн. наук, доц.
_____ В. В. Никулин
(подпись)
«06» 06 2020 г.

БАКАЛАВРСКАЯ РАБОТА

ПРОЕКТИРОВАНИЕ И МОНИТОРИНГ КОРПОРАТИВНОЙ СЕТИ ДЕПАРТАМЕНТА СИТУАЦИОННОГО РЕАГИРОВАНИЯ И АНАЛИТИКИ ПАО «РОСТЕЛЕКОМ»

Автор бакалаврской работы _____ 06.06.2020 А.Н. Вишняков
(подпись) (дата)

Обозначение бакалаврской работы БР-02069964-11.03.02-02-20

Направление 11.03.02 Инфокоммуникационные технологии и системы связи

Руководитель работы
канд. культурологии, доц. _____ 06.06.2020г. Е. А. Кошевая
(подпись) (дата)

Нормоконтролер
канд. культурологии, доц. _____ 06.06.2020г. Е. А. Кошевая
(подпись) (дата)

Саранск
2020

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
МОРДОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМ. Н. П. ОГАРЁВА»**

Институт электроники и светотехники

Кафедра инфокоммуникационных технологий и систем связи

УТВЕРЖДАЮ

Зав. кафедрой
канд. техн. наук, доц.

_____ В. В. Никулин
(подпись)

«12» ноября 2019 г.

ЗАДАНИЕ НА БАКАЛАВРСКУЮ РАБОТУ

Студент Вишняков Александр Николаевич

1 Тема Проектирование и мониторинг корпоративной сети Департамента ситуационного реагирования и аналитика ПАО «Ростелеком»

Утверждена приказом № 9008-с от 12 ноября 2019 г.

2 Срок представления работы к защите 6 июня 2020 г.

3 Содержание выпускной квалификационной работы

- 3.1 Обзор систем мониторинга
- 3.2 Выбор программного обеспечения
- 3.3 Выбор оборудования
- 3.4 Постановка на мониторинг систем САПС и База Знаний
- 3.5 Расчет экономической эффективности

4 Приложения

4.1 ПРИЛОЖЕНИЕ А (обязательное) Технические требования для серверов мониторинга

4.2 ПРИЛОЖЕНИЕ Б (обязательное) Спецификация оборудования

4.3 ПРИЛОЖЕНИЕ В (обязательное) Ресурсно-сервисная модель сервиса САСП

4.4 ПРИЛОЖЕНИЕ Г (обязательное) Ресурсно-сервисная модель сервиса База Знаний

Руководитель работы
канд. культурологии, доц. _____ 12.11.19. Е. А. Кошевая
подпись,дата

Задание принял к исполнению 12.11.19 _____

РЕФЕРАТ

Темой бакалаврской работы является проектирование и мониторинг корпоративной сети Департамента ситуационного реагирования и аналитики ПАО «Ростелеком».

МОНИТОРИНГ, СИСТЕМА МОНИТОРИНГА, КОММУТАТОР, КОРПОРАТИВНАЯ СЕТЬ, ПРОЕКТИРОВАНИЕ

Бакалаврская работа содержит 59 страниц, 26 рисунков, 1 таблицу, 8 использованных источников, 4 приложения и 3 формулы.

Цель данной работы состоит в изучении технических и программных средств для построения и мониторинга IT-систем и IT-сервисов.

В проекте осуществлен разбор существующих систем мониторинга, их архитектуры и назначения отдельно взятых компонентов, выбор программного и аппаратного обеспечения для передачи данных по локальной сети, а также для постановки на мониторинг сетевых и ресурсных компонентов. Также рассмотрена технология SMNP-ловушек, с помощью которых ведется наблюдение за работой оборудования.

В результате расчета экономической эффективности было установлено, что проектное решение полностью окупится через 8,2 месяцев.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Мониторинг – это совокупность программного и аппаратного обеспечения для сбора информации о работоспособности систем. При помощи нее возможно собирать данные о работе как отдельно взятых элементов системы, так и функционале системы в целом. В дальнейшем собранная информация может быть проанализирована для выявления недопустимой конфигурации оборудования, времени максимальной нагрузки серверных компонентов и так далее. Также, возможно подключение к системе услуги автоматического оповещения ответственных лиц для своевременного оповещения о проблемах, возникающих при работе.

Сейчас эта мера необходима в любой бизнес-системе, так как это позволяет повысить работоспособность и отказоустойчивость путем обработки информации об ошибках и авариях. При должной скорости реагирования ответственных лиц возможно устранение неполадок в кратчайшие сроки, что позволяет использовать систему бесперебойно.

В данной работе будет рассмотрена замена существующей конфигурации серверного оборудования, а именно – коммутатора и источника бесперебойного питания, добавление серверов мониторинга, а также постановка на мониторинг серверов сервиса САСП и Базы Знаний. Постановка на мониторинг системы обеспечит сбор данных и оповещение ответственных, что увеличит время работы системы без отказов, а значит, позволит использовать ее более эффективно. Замена источника бесперебойного питания даст возможность следить за режимом питания подключенных к нему компонентов, а замена коммутатора – возможность отслеживать его состояние и получать информацию о возможной ошибке. Это будет реализовано с помощью SNMP-ловушек (SNMP trap) – особого широковещательного (UDP) пакета, отправляемого устройством с поддержкой протокола SNMP.

1 Обзор систем мониторинга

Мониторинг IT-сервисов – это процесс, цель которого – соблюдение баланса между количеством имеющихся сетевых ресурсов, поддержанием определенного уровня информационных услуг и затратами на эффективное функционирование вычислительных сетей. В первую очередь он необходим, чтобы администраторы узнавали о проблемах в инфраструктуре раньше пользователей. Это, по сути, комплекс быстрой диагностики, который дает своевременное оповещение о проблемах и точную информацию, где и что случилось конкретно.

Ключевую роль в этом играет система нотификаций – оповещений ответственных лиц путем e-mail и sms рассылок. В тексте письма содержится вся необходимая информация, чтобы начать устранение неполадки – hostname сервера, на котором произошла авария, название процесса, графика использования ресурса, который превысил критическую отметку, его нынешнее состояние и время, когда произошел сбой.

Также системы мониторинга позволяют собирать статистику (метрику) определенных процессов – например, нагрузка на ядра процессора, свободная оперативная память или место на диске и так далее. Следовательно, эти данные пригодны для дальнейшего анализа с целью увеличения эффективности работы сервиса. Так, например, мы можем увеличить объем оперативной памяти или места на диске, если метрики по этим параметрам зачастую превышают допустимое значение.

Существует множество различных систем мониторинга IT-сервисов, но в рамках данной работы будут рассмотрены три основных вида, на которые можно условно разделить любую такую систему. Это системный, прикладной и функциональный мониторинг.

1.1 Системный мониторинг

Системный мониторинг – самый простой вид мониторинга, который нужен для сбора статистики об использовании физических ресурсов сервера. В них, к примеру, входят: свободное место на диске, процент использования оперативной памяти, загруженность ядер процессора и так далее. Такой вид мониторинга необходим для поддержания сервера в рабочем состоянии.

Метрики, собираемые данным видом мониторинга, могут послужить данными для создания различных графиков производительности системы.

Кроме того, некоторые из этих метрик могут иметь ключевое значение при анализе работы сервера. К примеру, при недостаточном количестве дискового пространства на сервере базы данных может возникнуть авария. При постановке на мониторинг такие моменты можно исключить, так как система заранее предупредит о приближении к критической точке.

В компании ПАО «Ростелеком» для этого используется BMC Proactive NET 9.6, SCOM – System Center Operations Manager, а также DynaTrace. Все эти варианты предлагают свой подход для мониторинга, поэтому остановимся на них более детально.

1.1.2 Система мониторинга BMC Proactive NET 9.6

BMC Proactive NET 9.6 – это интегрированная платформа для управления доступностью услуг и производительностью IT-систем и IT-сервисов. Он объединяет управление событиями, управление воздействием на услуги, мониторинг производительности и анализ данных (включая базовые показатели, обнаружение отклонений и алгоритмы анализа первопричин) в едином бесшовном решении для физических, виртуальных и облачных сред [1].

Мониторинг IT-сервисов системой BMC Proactive NET 9.6 имеет несколько рабочих режимов: пассивный, активный, проактивный.

Отличия между ними следующие:

1) активный режим – это периодические опросы IT сервисов, ожидание/получение ответов и реакция на них;

2) пассивный режим – это постоянный режим ожидания системами мониторинга событий в системе;

3) проактивный режим – это прогнозирование поведения инфраструктуры на основании исторических данных за определенный период времени.

BMC Proactive NET 9.6 предоставляет следующие возможности для контроля критических важных IT-систем и IT-сервисов.

Управление событиями – предоставляет решение в режиме реального времени для автоматического обнаружения и решения проблем IT, прежде чем они воздействуют на критические системы IT. Проактивно коррелирует, расставляет приоритеты и разрешает события в бизнес-контексте в реальном времени.

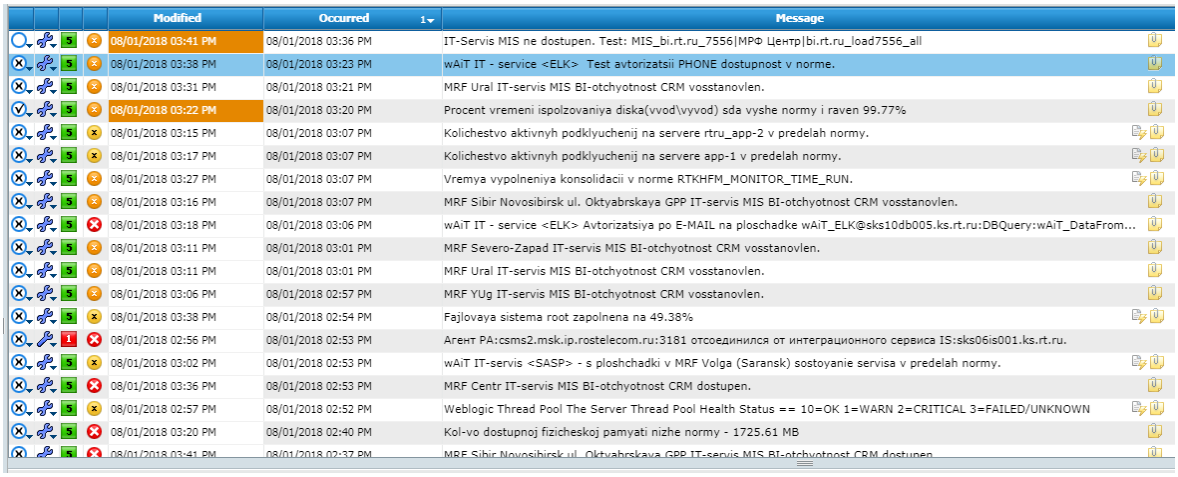
Управление влиянием на сервисы – отображает бизнес-сервисы и IT-инфраструктуру, чтобы помочь управлять приложениями и сервисами, которые важны для управления бизнес-сервисами (BSM), и определять их приоритеты. Управление Service Impact позволяет расставлять приоритеты бизнес-сервисов на основе бизнес-логики, давая возможность быстро определить, какие проблемы наиболее актуальны.

Мониторинг производительности – упреждающее обнаружение, автоматическое прогнозирование и решение проблем производительности IT и неоптимальных конфигураций, прежде чем пользователи и сервисы окажут негативное влияние.

Анализ производительности – позволяет BMC ProactiveNet изучать поведение приложений и IT-инфраструктуры в разных географических зонах, прогнозировать проблемы до их возникновения, автоматически определять вероятную причину в технологических блоках и инициировать стандартизированные процессы сортировки и разрешения проблем. Аналитика производительности сопоставляет и анализирует показатели и события, собранные

в инфраструктуре, для выявления отклонений, прогнозирования сбоев и предоставления подробной диагностической информации.

На рисунке 1 представлен пример коллектора событий системы BMC ProactiveNet 9.6.



Modified	Occurred	Message
08/01/2018 03:41 PM	08/01/2018 03:36 PM	IT-Servis MIS ne dostupen. Test: MIS_bi.rt.ru_7556|МРФ Центр|bi.rt.ru_load7556_all
08/01/2018 03:38 PM	08/01/2018 03:23 PM	wAiT IT - service <ELK> Test avtorizatsii PHONE dostupnost v norme.
08/01/2018 03:31 PM	08/01/2018 03:21 PM	MRF Ural IT-servis MIS BI-otchyotnost CRM vosstanovlen.
08/01/2018 03:22 PM	08/01/2018 03:20 PM	Procent vremeni ispolzovaniya diska(vvod\vyvod) sda vyshe normy i raven 99.77%
08/01/2018 03:15 PM	08/01/2018 03:07 PM	Kolichestvo aktivnyh podklyuchenij na servere rtru_app-2 v predelah normy.
08/01/2018 03:17 PM	08/01/2018 03:07 PM	Kolichestvo aktivnyh podklyuchenij na servere app-1 v predelah normy.
08/01/2018 03:27 PM	08/01/2018 03:07 PM	Vremya vypolneniya konsolidacii v norme RTKHFM_MONITOR_TIME_RUN.
08/01/2018 03:16 PM	08/01/2018 03:07 PM	MRF Sibir Novosibirsk ul. Oktyabrskaya GPP IT-servis MIS BI-otchyotnost CRM vosstanovlen.
08/01/2018 03:18 PM	08/01/2018 03:06 PM	wAiT IT - service <ELK> Avtorizatsiya po E-MAIL na ploschadke wAiT_ELK@sks10db005.ks.rt.ru:DBQuery:wAiT_DataFrom...
08/01/2018 03:11 PM	08/01/2018 03:01 PM	MRF Severo-Zapad IT-servis MIS BI-otchyotnost CRM vosstanovlen.
08/01/2018 03:11 PM	08/01/2018 03:01 PM	MRF Ural IT-servis MIS BI-otchyotnost CRM vosstanovlen.
08/01/2018 03:06 PM	08/01/2018 02:57 PM	MRF YUg IT-servis MIS BI-otchyotnost CRM vosstanovlen.
08/01/2018 03:38 PM	08/01/2018 02:54 PM	Fajlovaya sistema root zapolnena na 49.38%
08/01/2018 02:56 PM	08/01/2018 02:53 PM	Агент PA:csms2.msk.ip.rostelecom.ru:3181 отсоединился от интеграционного сервиса IS:sks06is001.ks.rt.ru.
08/01/2018 03:02 PM	08/01/2018 02:53 PM	wAiT IT-servis <SASP> - s ploshchadki v MRF Volga (Saransk) sostoyanie servisa v predelah normy.
08/01/2018 03:36 PM	08/01/2018 02:53 PM	MRF Centr IT-servis MIS BI-otchyotnost CRM dostupen.
08/01/2018 02:57 PM	08/01/2018 02:52 PM	Weblogic Thread Pool The Server Thread Pool Health Status == 10=OK 1=WARN 2=CRITICAL 3=FAILED/UNKNOWN
08/01/2018 03:20 PM	08/01/2018 02:40 PM	Kol-vo dostupnoj fizicheskoj pamyati nizhe normy - 1725.61 MB
08/01/2018 03:41 PM	08/01/2018 02:37 PM	MRF Sibir Novosibirsk ul. Oktyabrskaya GPP IT-servis MIS BI-otchyotnost CRM dostupen

Рисунок 1 – Коллектор событий

Данная система примечательна не только тем, что имеет заранее заготовленные Knowledge module для разных решений мониторинга, но и позволяет интегрировать в систему различные внештатные решения, разработанные под конкретную задачу и события из других систем мониторинга. Также, она имеет коллектор событий, в котором показаны все недавние аварии; встроенное представление состояния системы в реальном времени (далее – dashboard), на котором видно состояния каждого IT- или бизнес-сервиса; ресурсно-сервисную модель, на которой можно увидеть модель влияния каждого из элементов друг на друга в системе. На рисунке 2 представлен пример dashboard системы BMC ProactiveNet 9.6.

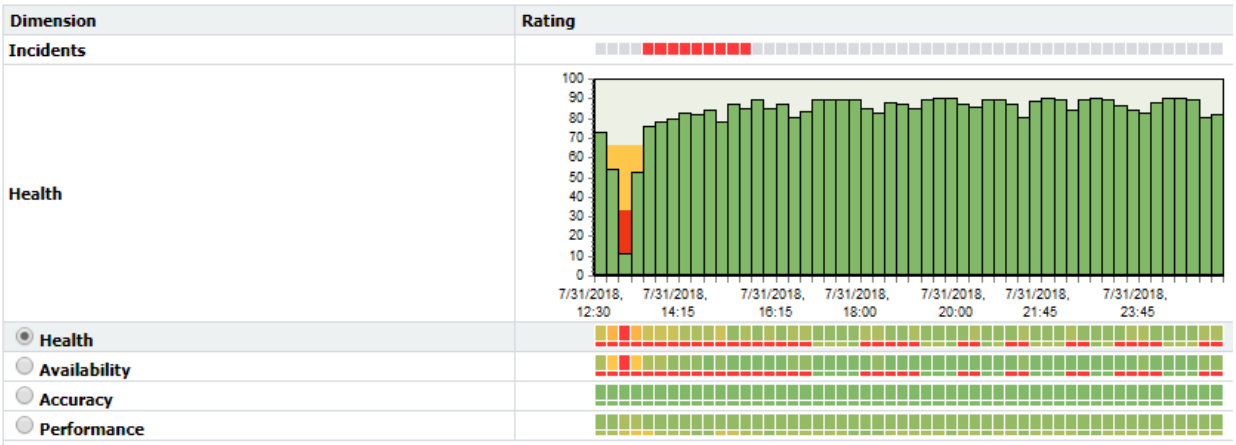


Рисунок 2 – Dashboard BMC

1.1.3 Система мониторинга System Center Operations Manager (SCOM)

System Center Operations Manager (SCOM) (ранее Microsoft Operations Manager, MOM) – программа компании Microsoft для управления и мониторинга IT-сервисов, приложений, серверов в гетерогенной среде Windows, UNIX и Linux. Продукт способен консолидировать информацию о функционировании различных компонентов IT-инфраструктуры, обеспечивая её обобщенное представление в единой консоли.

Существуют инструменты для мониторинга различного системного и прикладного программного обеспечения, однако логика мониторинга может быть определена только самим администратором системы.

SCOM предназначен главным образом для организации с числом компьютеров более 500 и числом серверов более 30. Для меньших организаций существует продукт System Center Essentials [2].

Operations Manager, компонент Microsoft System Center, позволяет отслеживать состояние задач, выполняемых на нескольких компьютерах, в одной консоли. Использование Operations Manager в среде организации упрощает мониторинг большого количества компьютеров, устройств, служб и приложений. Консоль управления, показанная на рисунке 3, позволяет проверить

работоспособность, производительность и доступность всех отслеживаемых объектов в среде, а также помогает обнаруживать и устранять проблемы.

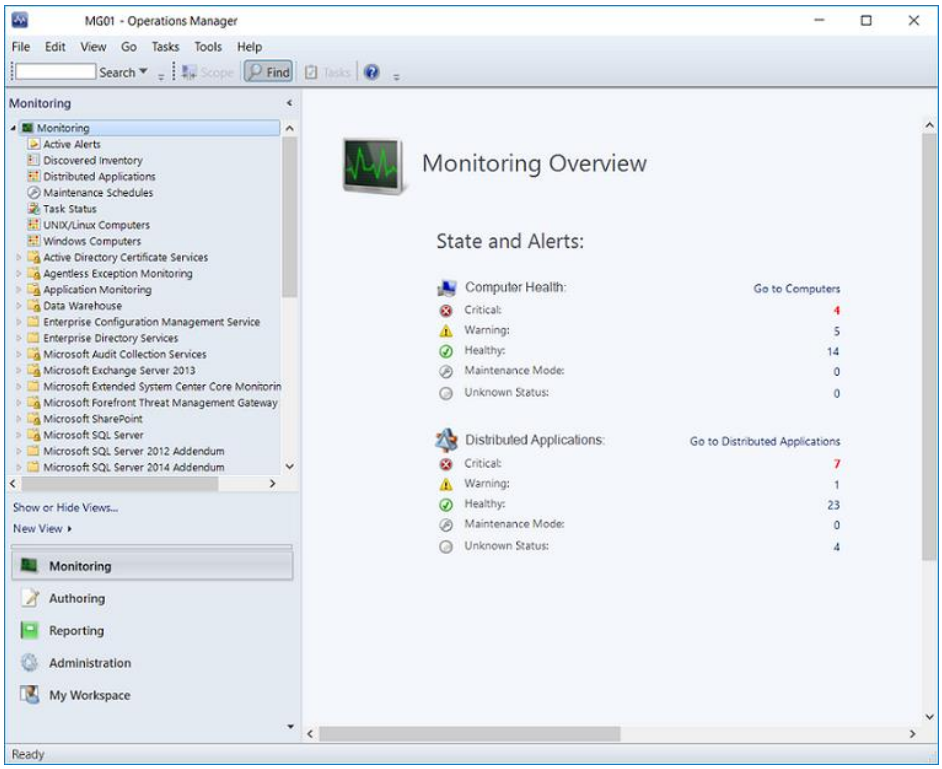


Рисунок 3 – Консоль управления Operations Manager

Operations Manager уведомит, какие отслеживаемые объекты не работают, имеет возможность отправить оповещения при обнаружении проблем и предоставить информацию, которая поможет определить причину проблемы и возможные решения. Администратор устанавливает объекты мониторинга, выбирая компьютеры и устройства и импортируя пакеты управления, которые отслеживают определенные компоненты и приложения.

На рисунке 4 представлен dashboard системы SCOM.

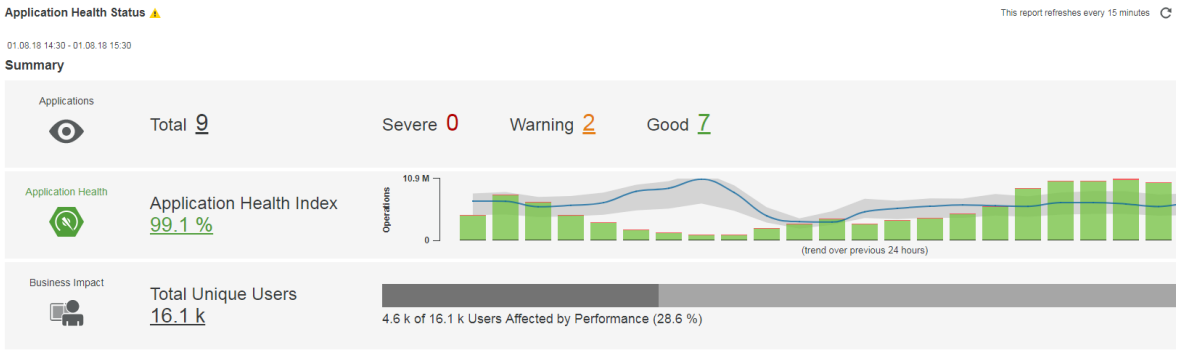


Рисунок 4 – Dashboard SCOM

1.1.4 Система мониторинга DynaTrace

DynaTrace – облачное решение для мониторинга, предназначенное для высокодинамичных сред контейнеров и кластеров. Оно позволяет оптимизировать развертывание контейнеров и выделение памяти с помощью данных об использовании, получаемых в режиме реального времени. Это решение способно автоматически выявлять проблемы приложений и инфраструктуры, обеспечивая автоматизированное задание базовых показателей, обобщение проблем и определение первопричин.

Данное программное обеспечение решает следующие проблемы:

1) мониторинг реальных пользовательских данных, производительности приложений, инфраструктуры и облачных сред;

2) DynaTrace автоматически обнаруживает все зависимости приложений и отслеживает транзакции на всех уровнях;

1) решает проблемы с производительностью или доступностью, прежде чем они повлияют на клиентских устройствах.

На рисунке 5 представлена работа программы DynaTrace.

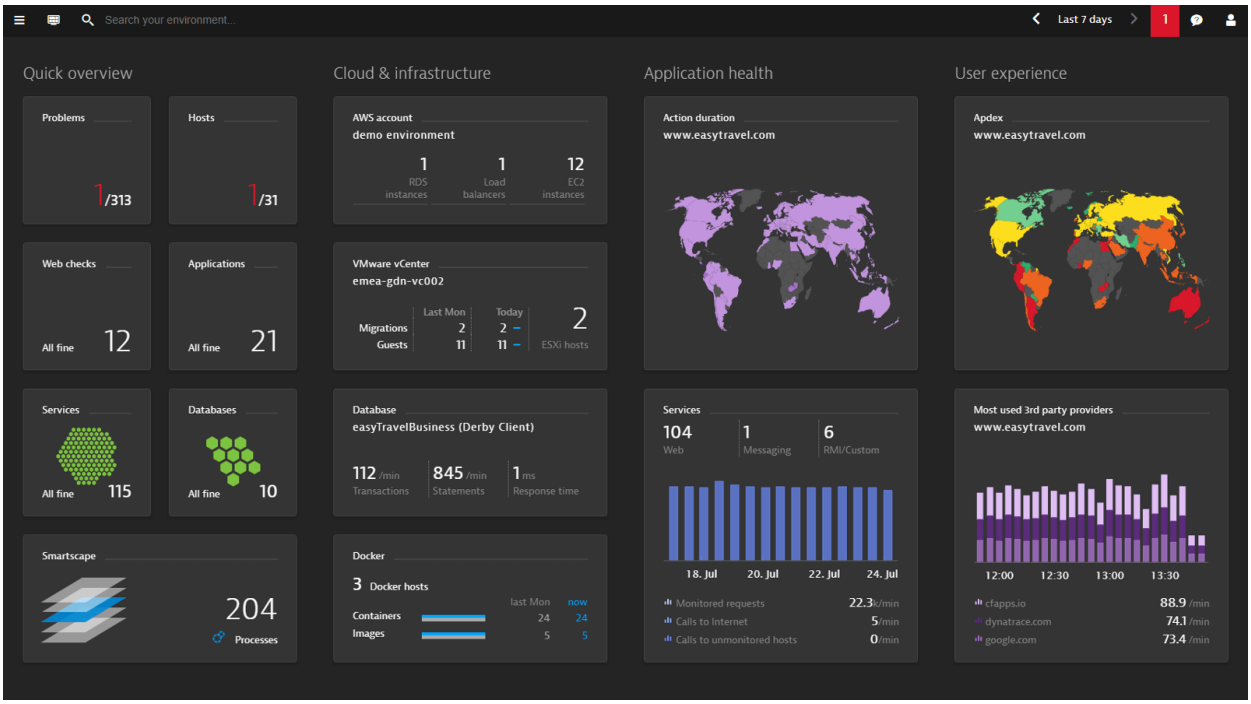


Рисунок 5 – Работа программы Dynatrace

Программа DynaTrace используется в компании “Ростелеком“ исключительно для программистов (разработчиков).

1.2 Прикладной мониторинг

Прикладной мониторинг необходим для сбора статистики о наличии определенных процессов, доступности портов и нескольких других решений. К такому мониторингу, например, относится: проверка наличия процесса, доступность/недоступность порта, проверка отклика сервера по протоколу ICMP (ping), выгрузка данных из баз данных по предоставленным командам SELECT, и последующий их анализ на соответствие.

Также этот вид мониторинга позволяет проводить проверки доступности web-страниц, а также поиска контента на них. При невыполнении условий проверки будет создано аварийное событие, которое будет переправлено ответственным лицам.

Этот вид мониторинга примечателен тем, что дает более показательную оценку работоспособности сервиса, и, обычно, события от прикладного мониторинга имеют намного больший приоритет. К примеру, если на сервере базы данных загруженность памяти достигает отметки в 90%, это не означает, что он недоступен. Но, если же этот сервер не будет доступен по ICMP, это даст весомые основания полагать, что в данный момент сервер неработоспособен.

Обычно в системах, которые предоставляют системный мониторинг, также предоставляют и прикладной. BMC ProactiveNET 9.6 также может выполнять обе эти функции одновременно, так как имеет множество Knowledge Module, в том числе и для прикладного мониторинга.

1.3 Функциональный мониторинг

Функциональный мониторинг – самый сложный для интеграции в системы и постановки их на контроль. При этом, сама разработка метода мониторинга весьма трудоемка, так как для него необходимо написать программу с определенной последовательностью действий.

Функциональный мониторинг в общем случае воссоздает действия пользователя в каком-либо сервисе, чтобы проверить работоспособность его функционально – отсюда и пошло название. Такой вид мониторинга очень показателен, так как может засечь ошибки, которые невозможно выявить программно. К примеру, у пользователя может не отображаться кнопка на сайте, либо недоступно для скачивания какое-либо приложение, либо может не прогрузиться элемент.

Для такой проверки пишется робот с определенной последовательностью шагов. Каждый шаг проверяет какой-либо элемент, и после положительного результата переходит к следующему этапу. Если на одном из шагов робот не смог выполнить действие, то он возвращает ошибку и появляется уведомление об ошибках в работе сервиса.

Для такого вида мониторинга также есть различные системы, но в данной работе будет рассмотрена система функционального тестирования ATOM. Она была создана сотрудником Ростелеком для выполнения операций функционального мониторинга, с последующей передачей состояния каждой площадки на dashboard. Рассмотрим принцип ее работы.

Имеются площадки тестирования – серверы, на которых установлены клиенты ATOM. На них запускаются с заданной периодичностью тесты определенного сервиса. Тесты состоят из шагов – упорядоченных действий, каждый из которых формирует «здоровье» сервиса. При невыполненном шаге тестирования остальные шаги пропускаются. «Здоровье» одной площадки тестирования формируется как среднее арифметическое успешно выполненных шагов от количества всех шагов в тесте.

Далее идет расчет «здоровья» сервиса в целом. Он также рассчитывается как среднее арифметическое всех площадок тестирования, которые проверяют данный сервис. Далее показатель здоровья в виде цветового индикатора (зеленый – 100% «здоровье», желтый – 50%, красный – 0%, полная недоступность сервиса) выводится на dashboard ATOM в соответствующий временной промежуток.

На рисунке 6 представлен dashboard системы ATOM.

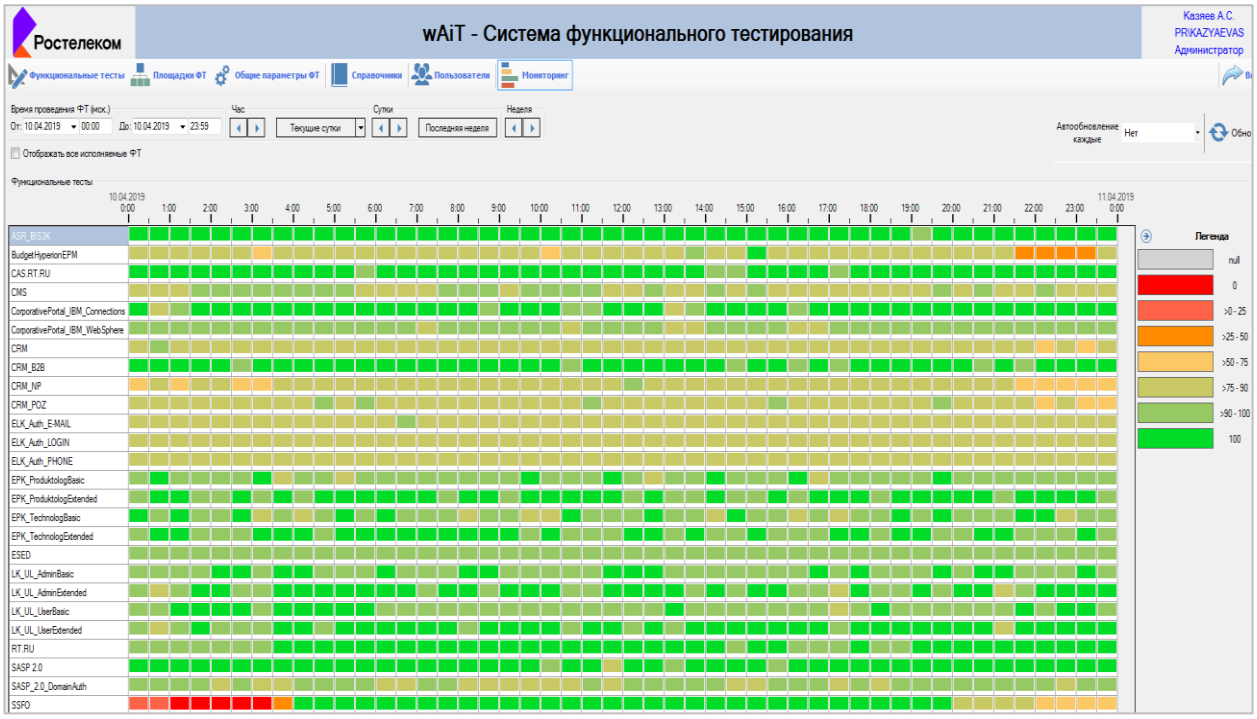


Рисунок 6 – Dashboard системы ATOM

Также, к преимуществам данной системы можно отнести легкое выяснение причины ошибки в тестировании. При возникновении неполадок, клиент ATOM на площадке тестирования делает скриншот, и он сохраняется в базу данных системы. Далее это может быть применено для устранения ошибки в работе контролируемой системы, теста или же в работе самой площадки функционального тестирования.

1.4 Принцип работы системы мониторинга BMC Proactive NET 9.6

Для ознакомления с принципом работы системы ознакомимся с рисунком 7.

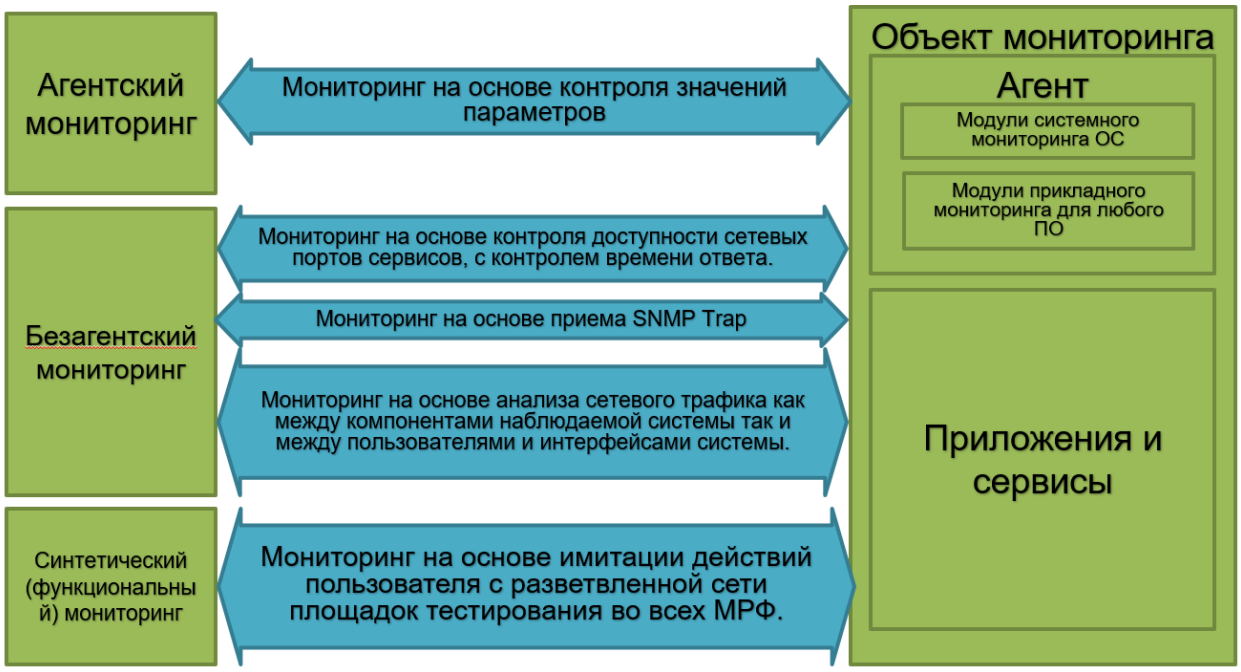


Рисунок 7 – Принцип работы системы мониторинга BMC ProactiveNet 9.6

Исходя из рисунка 7, мы видим, что существует агентский мониторинг, безагентский мониторинг, синтетический мониторинг. Каждый из этих вариант подразумевает различные подходы к сбору данных, необходимых для составления метрики, которая будет отобрать работоспособность сервиса. Рассмотрим подробнее каждый из подходов.

Агентский мониторинг – для такого вида мониторинга необходимо подготовить пакет инсталляции с необходимыми по техническому заданию модулями (агент мониторинга). Агент устанавливается на целевой сервер, где в фоновом режиме собирает данные о всех процессах, которые были указаны модулями. Далее эти данные отправляются на сервер интеграции, после чего переправляются на ProactiveNet сервер.

Безагентский мониторинг – в этом случае в агенте мониторинга нет необходимости, сервер системы мониторинга самостоятельно опрашивает целевой сервер, после чего получает необходимые данные для создания метрики.

Синтетический мониторинг – это функциональный мониторинг, предоставленный компанией BMC. Работает по тому же принципу, что и система АТОМ – заранее написанные программы проверок (робот) выполняют ряд действий, который симулируют действия пользователя. По сравнению с описанной ранее системой функционального мониторинга, коррелирует не с таким большим количеством методов проверок, а также имеет более неудобный dashboard.

Рассмотрим общий вариант постановки площадки на мониторинг. Вначале идет договоренность между заказчиком мониторинга (администратор сервиса) и отдела мониторинга. На этом этапе обговариваются параметры, которые должны состоять на мониторинге. Также на этом этапе решается, какой из видов мониторинга (или их совокупности) будет инсталлирован. После того, как будут обговорены общие аспекты метрик, которые будут собираться, составляется карточка мониторинга. Карточка мониторинга – техническое задание на постановку IT-сервиса на мониторинг с указанием всей информации об IT-сервисе, объектах мониторинга, контролируемых параметрах, списках оповещений и ресурсно-сервисной моделью.

На рисунке 8 представлен пример карточки мониторинга.

Назначение		
Данный документ представляет собой карточку мониторинга услуги CRM предоставляемую ЦИТ МФ ОЦО ОАО «Ростелеком» структурным подразделениям ОАО «Ростелеком». В карточке мониторинга услуги CRM:		
-	перечисляются ее характеристики и состав услуги;	
-	описываются роли, отвечающие за события, возникающие в процессе мониторинга услуги;	
-	указываются параметры, определяющие качество предоставляемой услуги.	
Используемые термины и сокращения		
СМИТС	-	Система мониторинга ИТ-Сервисов Ростелекома
CRM	-	Система управления взаимоотношениями с клиентами на базе программного обеспечения CRM Amdocs

Описание ИТ-услуги для мониторинга		
N/N	Название	Значение
1	Наименование услуги	CRM
2	Описание услуги	правления взаимоотношениями с клиентами на базе программного обеспечения CR
3	Критичность услуги	Business Critical
4	Предметный администратор	Крылов Андрей Владимирович
5	Специалист технической поддержки	Смоляной Роман Васильевич
6	Куратор системы	Крылов Андрей Владимирович
7	Ключевые пользователи (Подразделения, использующие у	Сотрудники ОАО «Ростелеком»
8	Количество пользователей	Все
9	Тип услуги	Клиент-сервер
10	Используется при составлении финансовой отчётности	Да
11	Список рассылки email «Общий»	SMITS_Support <smits_support@RT.RU>
12	Список рассылки sms «Общий»	
13	Список рассылки email «Кураторы системы»	
14	Список рассылки sms «Кураторы системы»	

Параметр	Тип монитора	Атрибут	Шаблон текста события	Имя объекта СМ	Критичность	Длит. (мин)	Условие	Значение	e-mail оповещение (группа)	SMS уведомления (группа)	Звонок от группы поддержки мониторинга	
											(ДА/нет)	Примечание
Доступность по ICMP (%)	Ping	Availability	Сервер <имя> не доступен по ICMP.	Все ОСМ	critical	5	«=»	0	CRM_SYS_CRIT	CRM_SYS_CRIT1	нет	
Утилизация процессора (%)	UNIX OS/CPU/	% CPU Utilization	Процессоры загружены на <значение>%	Все ОСМ	minor	5	>	80	CRM_SYS_MINOR		нет	
					major	5	>	90	CRM_SYS_MAJOR		нет	
					critical	5	>	95	CRM_SYS_CRIT	CRM_SYS_CRIT1	ДА	Опощения голосом только по основным серверам
Утилизация процессора в пользовательском режиме	UNIX OS/CPU/	% CPU Utilization In User Mode	Процессоры загружены на <значение>%	sks06crdb001.ks.rt.ru	minor	5	>	50	CRM_DBPROD_CPU1		нет	
					major	5	>	60	CRM_DBPROD_CPU2	CRM_DBPROD_CPU2	нет	
					critical	5	>	70	CRM_DBPROD_CPU3	CRM_DBPROD_CPU3	ДА	Опощения голосом

Рисунок 8 – Карточка мониторинга

Далее идет непосредственно постановка на мониторинг. Для того, чтобы сервер мог отсылать данные серверу-ядру системы мониторинга, на площадку необходимо инсталлировать агента мониторинга. После инсталляции, необходимо создать политику, по которой будет опрашиваться площадка. В этой политике прописаны метрики, которые будут собираться, с какой частотой, а также самая важная часть – threshold и оповещение на ответственных лиц.

Threshold – это пороги срабатывания, после пересечения которых метрикой будет вызвано определенное событие:

1) INFO – событие информативное, используется в общем случае для оповещения об успешной итерации, инсталляции и так далее;

2) Warning – также информативное событие, но оно уже несет в себе предупреждение;

3) Minor – аварийное событие с самым низким приоритетом, означает, что какая-то метрика незначительно превысила допустимый порог, либо произошла какая-то авария, которая возможно затронет сервис;

4) Major – аварийное событие с средним приоритетом, означает частичную недоступность сервиса (зависания, недоступность некоторых элементов);

5) Critical – аварийное событие с высоким приоритетом, означает либо полную недоступность сервиса, либо сильное отклонение метрики от ее заданного параметра.

При настройке возможно выбрать любое количество необходимых порогов срабатывания. При этом, каждое событие, открытое превышением графика контролируемого процесса по определенному порогу, будет уникальным, поэтому его можно будет однозначно определить, к примеру, для настройки нотификации.

Нотификация – ключевой параметр системы мониторинга, поскольку именно он определяет ее как систему для оповещения ответственных лиц, которые должны следить за ее работоспособностью. У каждого события есть определенный ряд параметров, по которым его можно однозначно определить. Это может быть как критичность события (уровень порога, который превысил график контролируемого процесса), так и название контролируемого сервиса, hostname сервера, название самого контролируемого процесса (загрузка процессора, количество свободного места на диске, к примеру) и многое другое. По ним создается политика нотификации, в которой прописано, кому именно будет отправлено данное событие.

Для этого существует специальные конфигурационные файлы, в которые прописываются контакты ответственных лиц. Сначала создаются группы рассылки – e-mail или sms. Далее в эти группы добавляются контакты. После этого в конфигурационном файле политики нотификации прописывается, на какое

событие должна среагировать политика, и какой группе рассылки переслать сообщение об аварии.

1.5 Обзор технологии SNMP-ловушек

SNMP (англ. Simple Network Management Protocol – простой протокол сетевого управления) – это стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP. Устройства с поддержкой SNMP включают в себя маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и другие. Протокол обычно используется в системе управления сетью. SNMP определен Инженерным советом Интернета (IETF) как компонент TCP/IP. Он состоит из набора стандартов для управления сетью, включая протокол прикладного уровня.

SNMP-traps (SNMP-ловушки) – это особый широковещательный UDP пакет, отправляемый удаленным устройством с поддержкой протокола SNMP. Подобные сообщения оповещают администратора о ошибке в функционировании устройства. Включает в себя текущее значение sysUpTime, OID, определяющий тип trap (ловушки), и необязательные связанные переменные. Адресация получателя для ловушек определяется с помощью переменных trap-конфигурации.

В данной главе были рассмотрены основные виды мониторинга, программы для обеспечения мониторинга IT-систем и IT-сервисов, принцип работы системы мониторинга BMC ProactiveNet 9.6, а также выполнен обзор технологий SNMP-ловушек. Весь мониторинг можно условно поделить на системный, прикладной, функциональный. Каждый из этих видов контролирует различные области системы, что позволяет в полной мере следить за ее работоспособностью.

1.6 Обоснование необходимости мониторинга

Департамент ситуационного реагирования и аналитики состоит из 4 отделов:

1) отдел мониторинга;
2) отдел аналитики;
3) первая линия (техподдержка внутренних пользователей);
4) отдел доступов.

В рамках данной работы будет рассмотрено проектное решение для решения проблемы недоступности ключевых сервисов отдела техподдержки. Предложено:

1) добавить серверы, необходимые для реализации мониторинга;
2) заменить текущие коммутатор и источник бесперебойного питания;
3) поставить на мониторинг серверы систем САСП и База Знаний.

Работоспособность отдела техподдержки напрямую зависит от функционирования основных программ, необходимых им для выполнения ряда задач. Это САСП – программа, показывающая текущие задачи для выполнения, а также их статус, и База Знаний – это база данных о возможных решениях определенных задач, шаблонов, информации о различных системах и их работе, отделах и так далее. При недоступности хотя бы одного из этих приложений функциональность отдела техподдержки существенно снизится.

Мониторинг данных систем позволит не только оперативно реагировать на всевозможные аварии и ошибки, но и собирать статистику об использовании отдельных элементов, графики загруженности серверных компонентов, времени дня, в которое нагрузка наиболее большая. При таком подходе возможно значительное увеличение времени безаварийной работы.

2 Выбор программного обеспечения и оборудования

Для предлагаемого проектного решения необходимо выбрать соответствующее оборудование, а именно: программное обеспечение – систему мониторинга, с помощью которой будет производиться отслеживание работы системы и сбор данных, сервер системы мониторинга, на который будет установлено соответствующее программное обеспечение, коммутатор второго уровня для мониторинга UDP пакетов (SNMP-ловушки), а также источник бесперебойного питания для мониторинга состояния питания элементов системы.

2.1 Выбор программного обеспечения

В качестве основной системы мониторинга была выбрана BMC Proactive NET 9.6, так как дежурная смена и администраторы системы уже ознакомлены с ней, а также она имеет множество преимуществ, которые были описаны ранее. Эта система уже внедрена в большое количество IT-сервисов компании Ростелеком и собирает статистику о работе ключевых сегментов. Таким образом, постановка на мониторинг систем САСП и Базы Знаний добавит две новые системы в каталог уже существующих, и сложность наблюдения за состояниям данными системами, как и сложность в их обслуживании заметно снизится для дежурной смены, администраторов сети и разработчиков приложений.

2.1.1 Архитектура системы мониторинга

Для того, чтобы все компоненты системы мониторинга могли быть использованы, необходимы серверы, выполняющие определенные роли.

Архитектура системы представлена на рисунке 9.

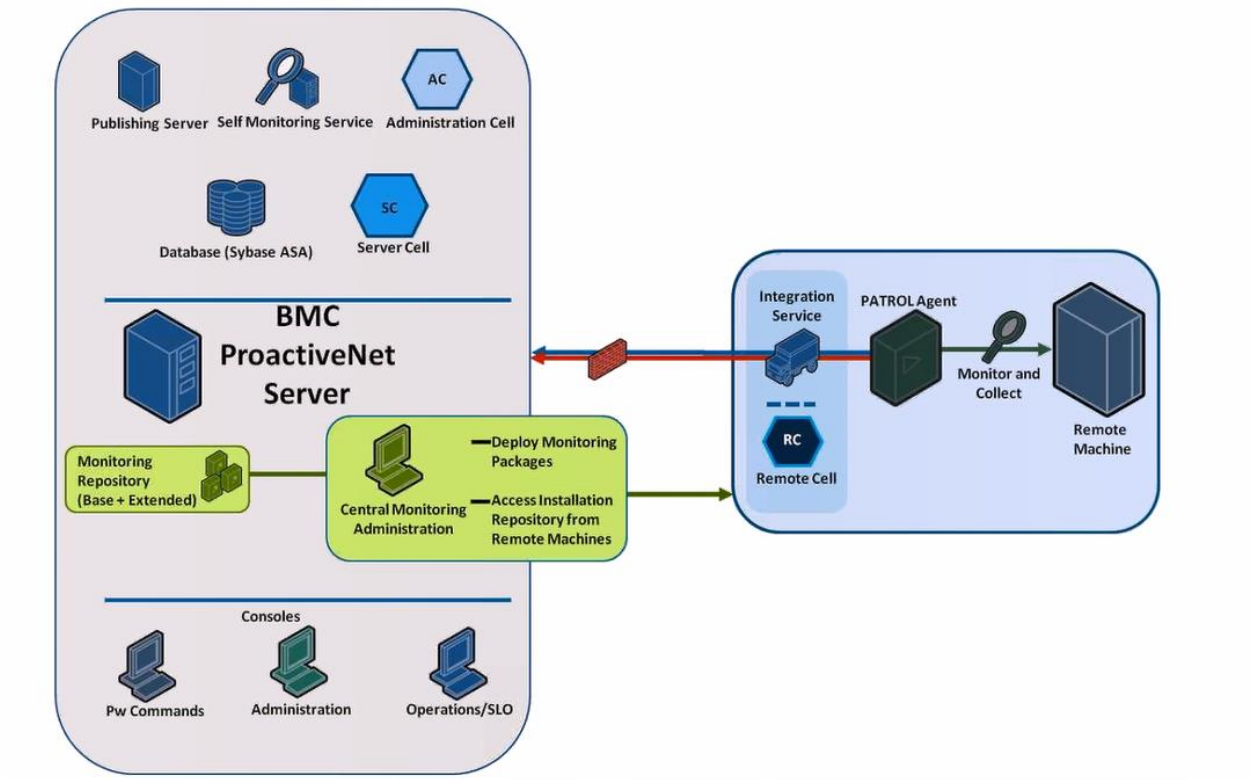


Рисунок 9 – Архитектура BMC

Подробнее рассмотрим каждый элемент представленной схемы.

Слева представлена серверная составляющая. Она состоит из нескольких частей – сам сервер системы мониторинга, его репозиторий и центральная консоль администрирования, с которой производится управление системой. Репозиторий – это хранилище для набора компонентов мониторинга, которые включены в ProactiveNet-сервер. В репозитории хранятся собранные индивидуально для каждой системы пакеты – агенты мониторинга, которые при последующей инсталляции на целевой сервер начинают собирать данные о его работе. На агента мониторинга можно поставить различные модули мониторинга, то есть указать, какие данные должны собираться: данные производительности операционной системы, данные о каком-либо конкретном программном обеспечении, серверные роли, производить удаленный мониторинг и так далее. Это позволяет подобрать оптимальную сборку для любой задачи, которая встает на стадии планирования наблюдения за работой сервера.

BMC ProactiveNet сервер необходим для сбора пакетов (агентов мониторинга) и дальнейшего их распространения. Также служит web-интерфейсом для операторов и администраторов системы мониторинга.

Система имеет три пользовательских консоли:

1) Pw commands – командная консоль;

2) Administration – консоль администрирования системы, ее программное обеспечение подключается к ProactiveNet серверу и служит для его настройки;

3) Operations/LSO – консоль оператора. Она расположена внутри web-интерфейса внутри ProactiveNet сервера. Это консоль, в которой работают операторы системы мониторинга, также в ней приведены все события, влияющие на контролируемые устройства, метрики.

Консоль операторов системы мониторинга имеет коллектор событий, в котором отображаются все аварийные события. Также в нем показан статус этих событий – они открыты (проблема актуальна на сервере действительно имеются проблемы), ознакомлены (с проблемой ознакомился оператор и оповестил о ней ответственных лиц, если этого не сделала система нотификаций), закрыты (проблема была решена). На рисунке 10 показана консоль оператора.

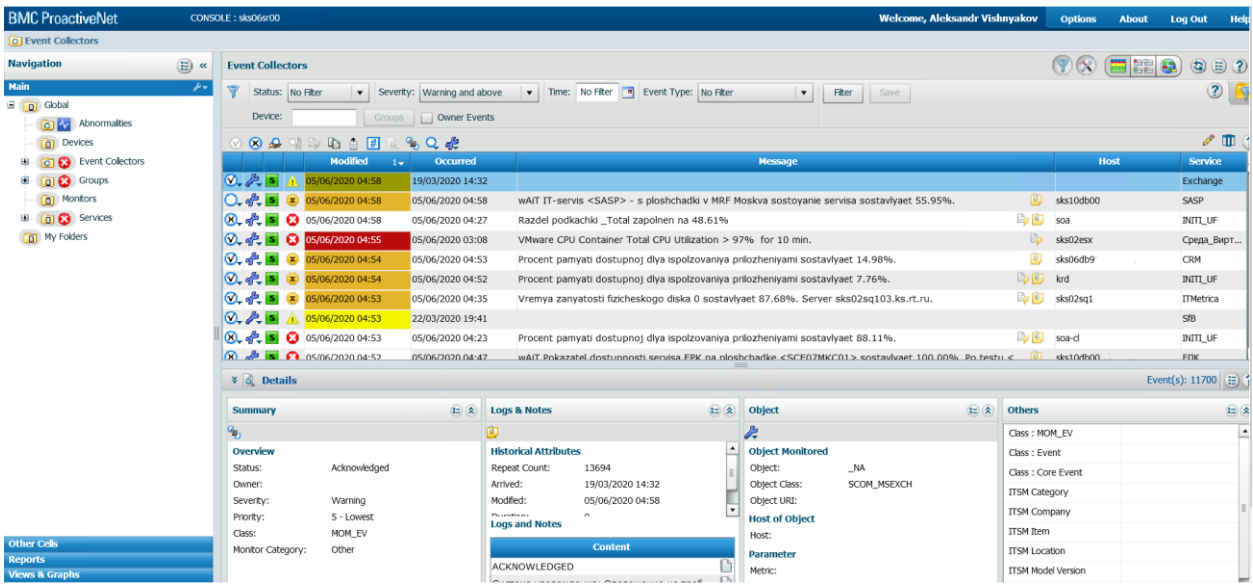


Рисунок 10 – Консоль оператора

Также, в этой консоли есть возможность просмотреть активных агентов мониторинга (вкладка Devices), а также ресурсно-сервисные модели всех сервисов, поставленных на мониторинг (вкладка Services). На агентах мониторинга можно увидеть все графики состояния, собираемые ими.

Консоль для администраторов позволяет полностью конфигурировать системы сбора информации, пороги критичности, добавлять и удалять агентов мониторинга и многое другое. Доступ к ней предоставляется отдельно, так что у операторов системы нет доступа к конфигурациям сервисов, поставленных на мониторинг. На рисунке 11 представлена консоль администратора.

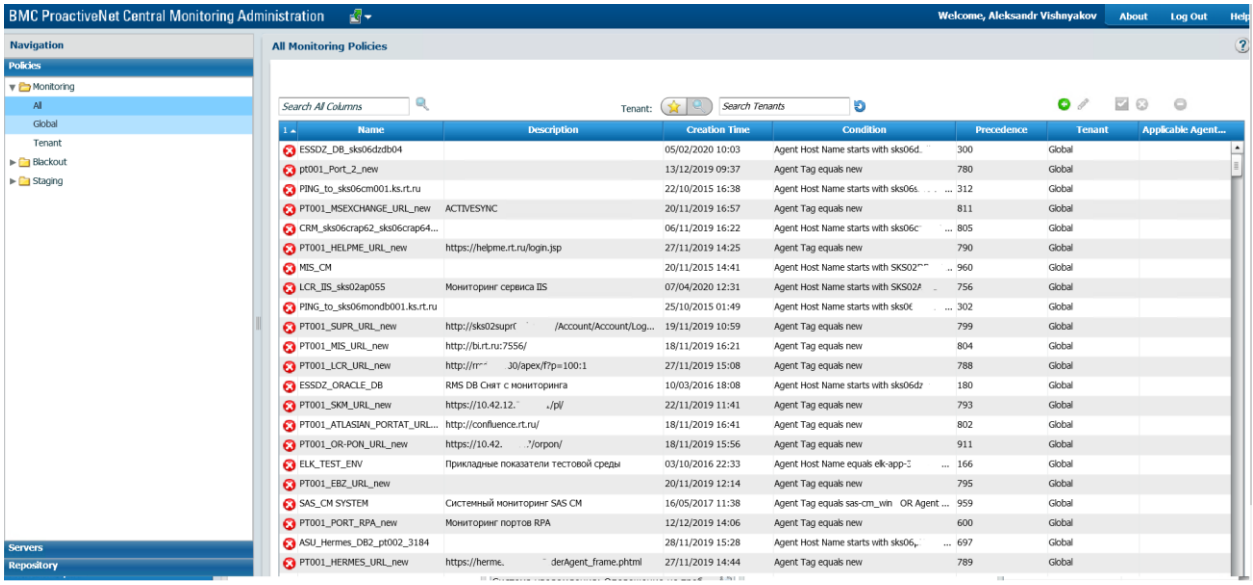


Рисунок 11 – Консоль администратора

На рисунке 11 на данный момент показаны групповые политики сервисов, поставленных на мониторинг. Каждая политика по определенным параметрам (соответствие по hostname сервера, тэгу, ip-адресу и так далее) применяется к агентам мониторинга. После этого их можно сконфигурировать по своему усмотрению.

Во вкладке «Servers» показаны серверы, на которых в данный момент установлены агенты мониторинга. Также там отображаются их статусы: отключен

или подключен. При нескольких серверах интеграции возможно переназначать место отправление собранных данных агентами, переустанавливать агентов мониторинга для обновления модулей, по которым собираются данные и тому подобное.

Вкладка «Repository» открывает вкладку с репозиторием сервера ProactiveNet. В нем находятся сконфигурированные пакеты инсталляции, которые можно при желании изменить по своему усмотрению.

Publishing server – это компонент, осуществляющий публикацию ресурсно-сервисных моделей систем, поставленных на мониторинг, из других продуктов. В данном случае, это BMC CMDB Atrium.

Self-monitoring server является очень важным элементом системы мониторинга. Это сервис самомониторинга, который контролирует свои процессы и сигнализирует о неисправностях, которые возникают в компонентах системы. Без этого элемента, при аварии в самой системе мониторинга невозможно было бы понять ее причину. Также это помогает увеличить время бесперебойной работы системы, так как сервер предупреждает о возможных ошибках, которые могут произойти в будущем, анализируя графики процессов.

Administration cell и Server Cell – это программные компоненты, их функция состоит в том, что они позволяют обрабатывать события, которые возникают в системе, хранят динамические данные, политики обработки этих событий, настройки по обработке, ресурсно-сервисные модели и так далее.

С правой стороны схемы показана контролируемая системой мониторинга структура. При установке на целевой сервер (Remote Server) агента мониторинга (PATROL Agent), начинают собираться данные, которые были настроены политикой обработки. Название агента PATROL является таким, потому что это отдельный продукт компании BMC, изначально разработанный не для этой системы. Но так как он был многофункционален и предоставлял больше простора для выбора контролируемых процессов, он был добавлен в данную систему.

Исходя из вышесказанного, для обеспечения функциональности необходим сервер, позволяющий интегрировать этот продукт в систему – Integration Server.

2.2 Выбор оборудования

Исходя из предлагаемого проектного решения, изложенного ранее, необходимо выбрать коммутатор второго уровня и источник бесперебойного питания для того, чтобы можно было организовать мониторинг. С предыдущим оборудованием нет возможности организовать мониторинг SNMP-ловушек и режима питания оборудования, что может привести к несвоевременному информированию ответственных как о критичных ошибках, так и состояния, предшествующему ему. Также необходимо выбрать серверы для организации системы мониторинга, под заданные технические требования каждого из компонентов.

2.2.1 Выбор коммутатора

В рамках текущего технического проекта нужно заменить устаревший коммутатор на более современный. Он должен быть второго уровня, иметь 24 медных порта и 4 1G SFP или 10G SFP+ специальных порта.

Коммутатор уровня 2 (Layer2 или L2) предназначен для соединения нескольких устройств локальной вычислительной сети (LAN) или нескольких сегментов данной сети. Коммутатор уровня 2 обрабатывает и регистрирует MAC-адреса поступающих фреймов, осуществляет физическую адресацию и управления потоком данных (VLAN, мультикаст фильтрация, QoS).

Уровень 2 обеспечивает прямую передачу данных между двумя устройствами в локальной сети. При работе коммутатор уровня 2 сохраняет таблицу MAC-адресов, в которой обрабатываются и регистрируются MAC-адреса поступающих фреймов и запоминается оборудование, подключаемое через порт.

Массивы данных переключаются в MAC-адресах только внутри локальной сети, что позволяет сохранять данные только в пределах сети. При использовании коммутатора уровня 2 возможно выбрать определенные порты коммутатора для управления потоком данных (VLAN). Порты, в свою очередь, находятся в разных подсетях уровня 3.

Для решения данной задачи был выбран коммутатор FS S3900-24T4S. Он показан на рисунке 12.

Рисунок 12 – Коммутатор FS S3900-24T4S

Данный коммутатор – это усовершенствованный гигабитный стекируемый коммутатор Layer 2 Plus (Layer 3 Lite) с восходящей линией связи 1/10Gb, поддерживает возможность стекирования с возможностью подключения 1 и 10 Gigabit и улучшенным QoS на границе сети.

Технические характеристики коммутатора FS S3900-24T4S представлены в таблице 1.

Таблица 1 – Технические характеристики коммутатора FS S3900-24T4S

Интерфейсы	24x 10/100/1000BASE-T RJ45, 4x 10G SFP+	**Тип уровня**	Уровень 2+

Окончание таблицы 1

Макс. 10G Интерфейсы	4	**Коммутационная способность**	128 Gbps
Макс. 1G Интерфейсы	28	**Скорость переадресации**	95 Mpps
Таблица MAC-адресов	16K	**Количество VLAN**	4K
Jumbo-фреймы	9KB	**MTBF (Часы)**	>100,000
Flash-память	64MB	**RAM**	128MB
Память пакетного буфера	1.5MB	**Емкость DDRIII**	512MB
Штабелирования	До 6 Единиц (Те же модели)	**Макс. потребляемая мощность**	21W
Устройство питания	2x Источники питания - Внутренние	**Входное напряжение**	100-240VAC, 50-60Hz, 0.8A
Воздушный поток	Безвентиляторный	**Акустический шум**	0dB
Методы аутентификации	802.1X, AAA	**Протокол удаленного управления**	SNMP, RMON, HTTP, Telnet, SSH
Размеры (Ш x Г x В)	1.73"x11.02"x17.05" (44x280x440mm)	**Вес**	9.41 lbs (4.27кг)
Диапазон рабочих температур	32°F ~ 122°F (0º ~ 50ºC)	**Температура хранения**	-40°F ~ 158°F (-40º ~ 70ºC)
Диапазон рабочей влажности	5% ~ 90% (Без конденсата)	**Влажность Хранения**	10% ~ 90% (Без конденсата)
Индикаторы состояния	System, LINK activity, PWR	**Гарантия**	4 Года
Тип корпуса	Монтируемые в стойку	**Монтажный комплект**	Включены

2.2.2 Выбор серверов мониторинга

Как было написано ранее, для организации системы мониторинга необходимо выбрать серверы согласно их рекомендуемым техническим требованиям. Всего необходимо подобрать 4 сервера согласно их ролям, а именно:

1) ProactiveNet server;
2) Integration server;
3) Publishing server;
4) Database server.

Исходя из приложения А, и того, что система мониторинга будет развернута для не более чем 100 агентов мониторинга, будет выбрана Минимальная» конфигурация. Используя данные из приложения А, выберем соответствующие серверы для каждого элемента системы мониторинга.

За основу будет взят сервер HPE ProLiant dl20 Gen10 (1U). Он показан на рисунке 13. Для разных серверов системы мониторинга он будет сконфигурирован различно.

Рисунок 13 – Сервер HPE ProLiant dl20 Gen10 (1U)

Так, для ProactiveNet сервера необходим четырехъядерный процессор, 8 Gb оперативной памяти и 100 Gb дискового пространства. Для Integration сервера необходим двухъядерный процессор, 2 Gb оперативной памяти и 30 Gb дискового пространства. Для Publishing сервера (Atrium CMDB) необходим четырехъядерный процессор, 8 Gb оперативной памяти и 100 Gb дискового пространства. Для

Database сервера необходим четырехъядерный процессор, 16 Gb оперативной памяти и 170 Gb дискового пространства.

2.2.3 Расчет и выбор источника бесперебойного питания

Для бесперебойного питания оборудования шкафа необходим источник бесперебойного питания, который будет поддерживать систему в рабочем состоянии в случае аварии не менее чем на 15 минут. Также необходимо, чтобы в комплект источника бесперебойного питания входила SNMP-карта – это необходимо для того, чтобы он мог отправлять ошибки в режиме питания устройств.

Для того, чтобы рассчитать необходимую емкость источника бесперебойного питания, воспользуемся следующей формулой:

$$Ah = 100 * t * W, \quad (1)$$

где Ah – емкость источника бесперебойного питания,

t – расчетное время бесперебойной работы,

W – максимальное потребление.

Время автономной работы выражается в часах, емкость источника бесперебойного питания измеряется в А · ч, а мощность нагрузки в киловаттах. Суммарная мощность всех устройств составляет 350 Вт, то есть 0,35 кВт. Необходимое минимальное время работы – 15 минут, то есть 0,25 часа. Подставим данные значения в формулу 1:

$$100 * 0{,}25 * 0{,}35 = 8{,}75 \text{ А} \cdot \text{ч}$$

Значит, нам необходим источник бесперебойного питания с емкостью не менее 8,75 А · ч.

Тогда в качестве источника бесперебойного питания выбираем ИБП APC Smart-UPS SMT1500RMI2U, 1500BA. Имеет аккумулятор емкостью 9 А · ч, типоразмер 2U. Он представлен на рисунке 14.

Рисунок 14 – ИБП APC Smart-UPS SMT1500RMI2U, 1500BA

Для расчета времени, которое проработает данный источник бесперебойного питания, воспользуемся формулой 1. Подставляя значение емкости источника бесперебойного питания в формулу 2, получим:

$$t = \frac{Ah}{100 * W}, \quad (2)$$

$$\frac{9\ \text{А} \cdot \text{ч}}{100 * 0{,}35\ \text{кВт}} = 0{,}26\ \text{ч}.$$

В результате работа источника бесперебойного питания в автономном режиме будет 0,26 часа, что равно 15,6 минутам.

В данной главе был выполнен выбор оборудования и программного обеспечения для проектирования мониторинга для систем САСП и База Знаний, а также представлена архитектура системы мониторинга BMC ProactiveNet 9.6,

которая была выбрана как основная программа для контроля работоспособности систем.

3 Установка компонентов системы и постановка на мониторинг

Для постановки сервисов САСП и База Знаний на системный мониторинг необходимо добавить серверы системы мониторинга в шкаф, а также заменить коммутатор и источник бесперебойного питания в шкафу.

Изначально заменим источник бесперебойного питания на ИБП APC Smart-UPS SMT1500RMI2U, 1500BA. Он имеет типоразмер 2U, элементы для крепления в стойку приложены в комплекте. Устанавливаем его в нижнюю часть шкафа для повышения его устойчивости.

Далее добавляем четыре сервера мониторинга, которые были заранее сконфигурированы под цели компонентов мониторинга. Они имеют типоразмер 1U, элементы для крепления в стойку поставляются в комплекте. Устанавливаем их в свободные места в шкафу.

После этого заменяем устаревший коммутатор и заменяем его на коммутатор FS S3900-24T4S. Предыдущие подключения к коммутатору подключаем в нынешний, также в него будут подключены серверы мониторинга.

Непосредственно постановка на мониторинг режима питания источника бесперебойного питания, SNMP-ловушек, а также серверов систем САСП и База Знаний. Она проходит в несколько этапов.

3.1 Создание агента мониторинга

Изначально, исходя из требуемых по карточке мониторинга параметров, которые будут состоять на мониторинге, создадим агента мониторинга. Для этого заходим на web-страницу ProactiveNet сервера. Она показана на рисунке 15.

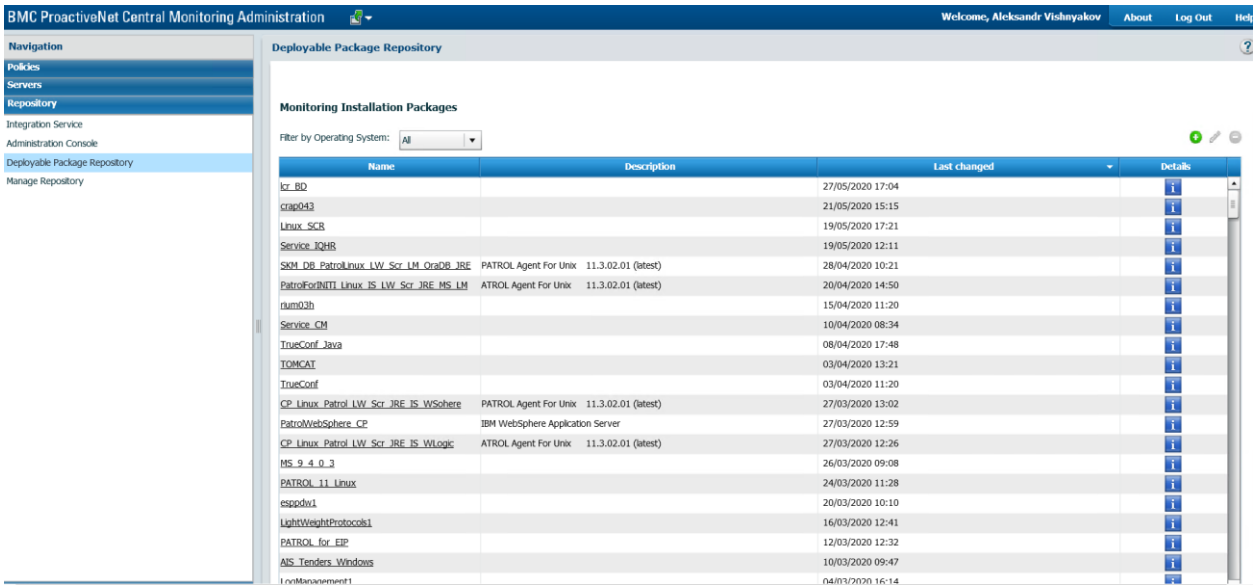


Рисунок 15 – Web-страница ProactiveNet сервера

Далее создаем непосредственно агента мониторинга. Для этого переходим в «Создать новый пакет инсталляции». По техническому заданию, взятому из карточки мониторинга, нам необходимы модули для контроля системных ресурсов сервера, таких как: процент использования процессора, процент использования оперативной памяти, количество свободного дискового пространства. За это отвечает модуль «Unix and Linux – HP-UX and Linux». Также необходим модуль для мониторинга доступности по команде ping. За это отвечает модуль «Light weight protocol». Модуль «Patrol agent for Unix» необходим для того, чтобы программа сбора метрик (агент мониторинга) была постоянно запущена в фоновом режиме. Эти модули будут добавлены в пакет инсталляции, впоследствии установленный на целевые серверы. На рисунке 16 показаны выбранные модули.

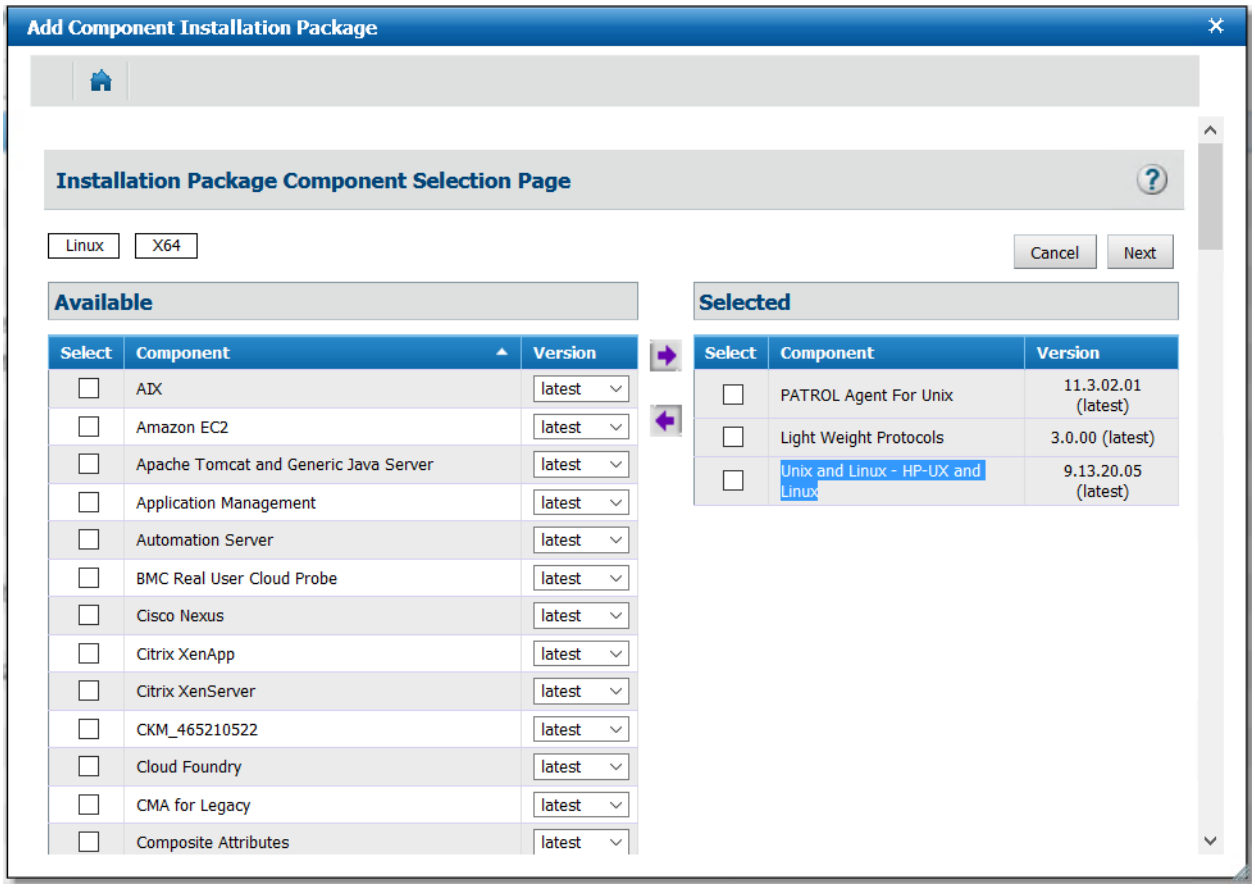


Рисунок 16 – Список выбранных модулей, необходимых для агента мониторинга

После этого необходимо указать директорию, в которую будет установлен агент мониторинга. По умолчанию это /opt/bmc/. Необходимо учитывать, что при инсталляции данная папка не создается автоматически.

Для корректной работы агента мониторинга ему необходим пользователь, под учетной записью которого он будет посылать данные на сервер интеграции. Далее открывается диалоговое окно, в котором предлагается ввести логин и пароль, под которым будет работать агент мониторинга. Ему необходим пользователь с администраторскими правами.

Следующим шагом необходимо выбрать номер порта, который будет использовать агент мониторинга для коммуникации с консолью. Здесь следует указать порт, на который была настроена конфигурация оборудования ранее. На рисунке 17 показано окно выбора порта.

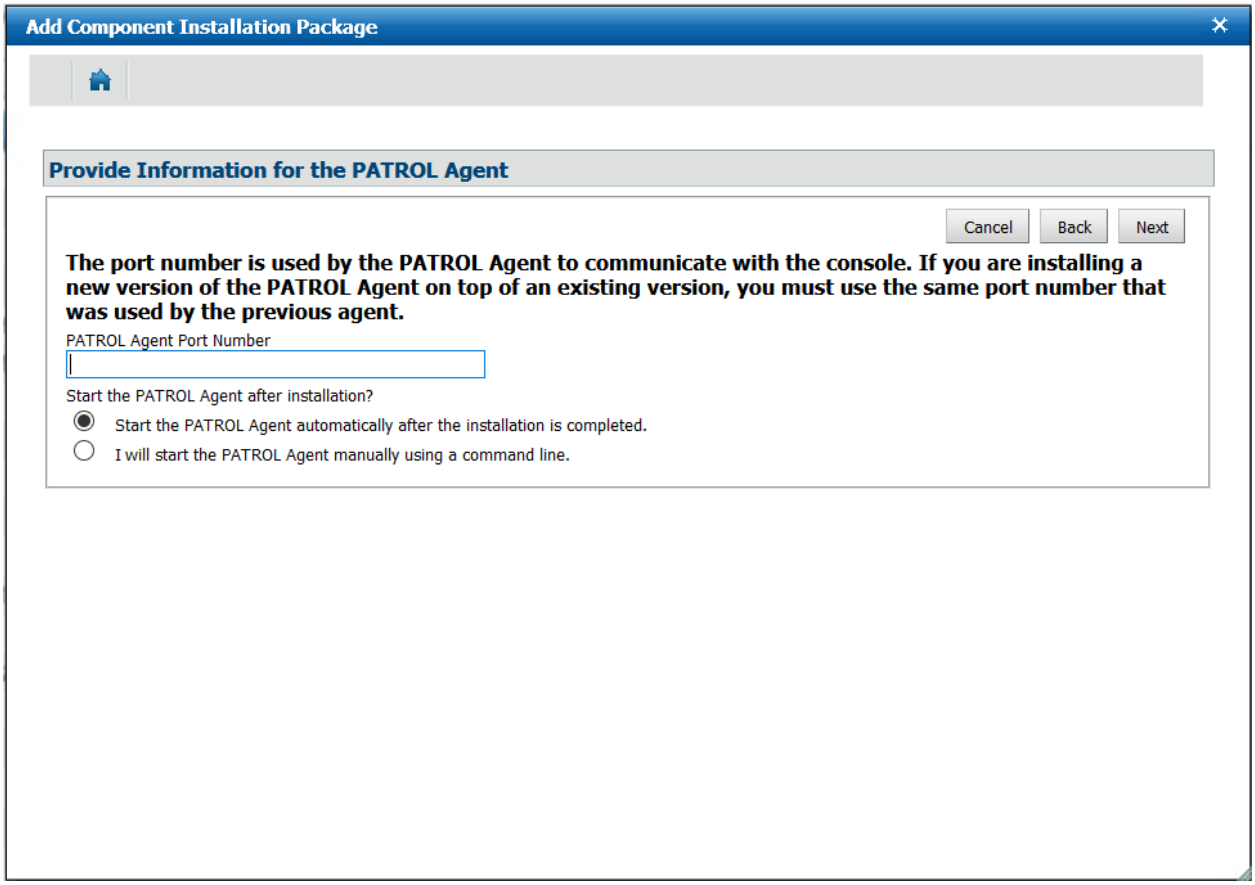


Рисунок 17 – Выбор порта для коммуникации с консолью

Далее следует настройка коммуникации с Integration сервером. В первом поле, «INTEGRATIONSERVICES Variable» указывается действующий адрес Integration сервера. В следующем поле «Central Monitoring Administration Tag(s)» указывается тег, который будет присвоен установленному на сервер агенту мониторинга. С помощью него можно сделать агента мониторинга специально для отельной системы, и, позже, по нему легко собрать их в единую ресурсно-сервисную модель. На рисунке 18 – настройка коммутации с Integration сервером.

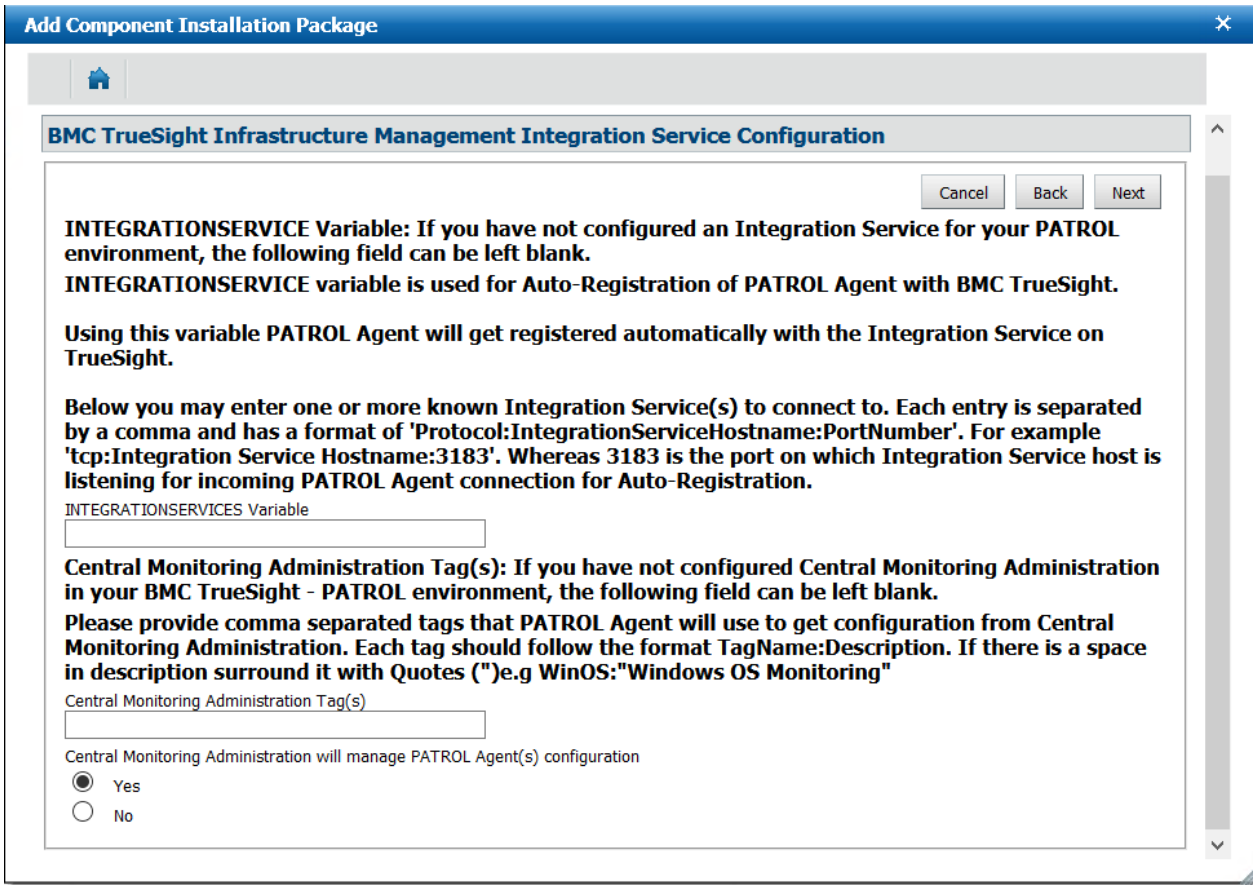


Рисунок 18 – Настройка коммутации с Integration сервером

Заключительным этапом является название для агента мониторинга, выбор его расширения, а также выбора – сохранить его в память рабочего компьютера, с которого был осуществлен доступ к web-странице ProactiveNet сервера, либо сохранить его в репозиторий системы мониторинга. При выборе опции «Сохранить», пакет инсталляции невозможно будет в дальнейшем конфигурировать и он будет удален из памяти ProactiveNet сервера. При выборе опции «Сохранить в репозиторий», возможно будет изменять его параметры, к примеру, можно будет добавить дополнительные модули мониторинга для сбора метрик, изменить назначенный тэг и так далее. На рисунке 19 мы можем наблюдать заключительный этап создания агента мониторинга.

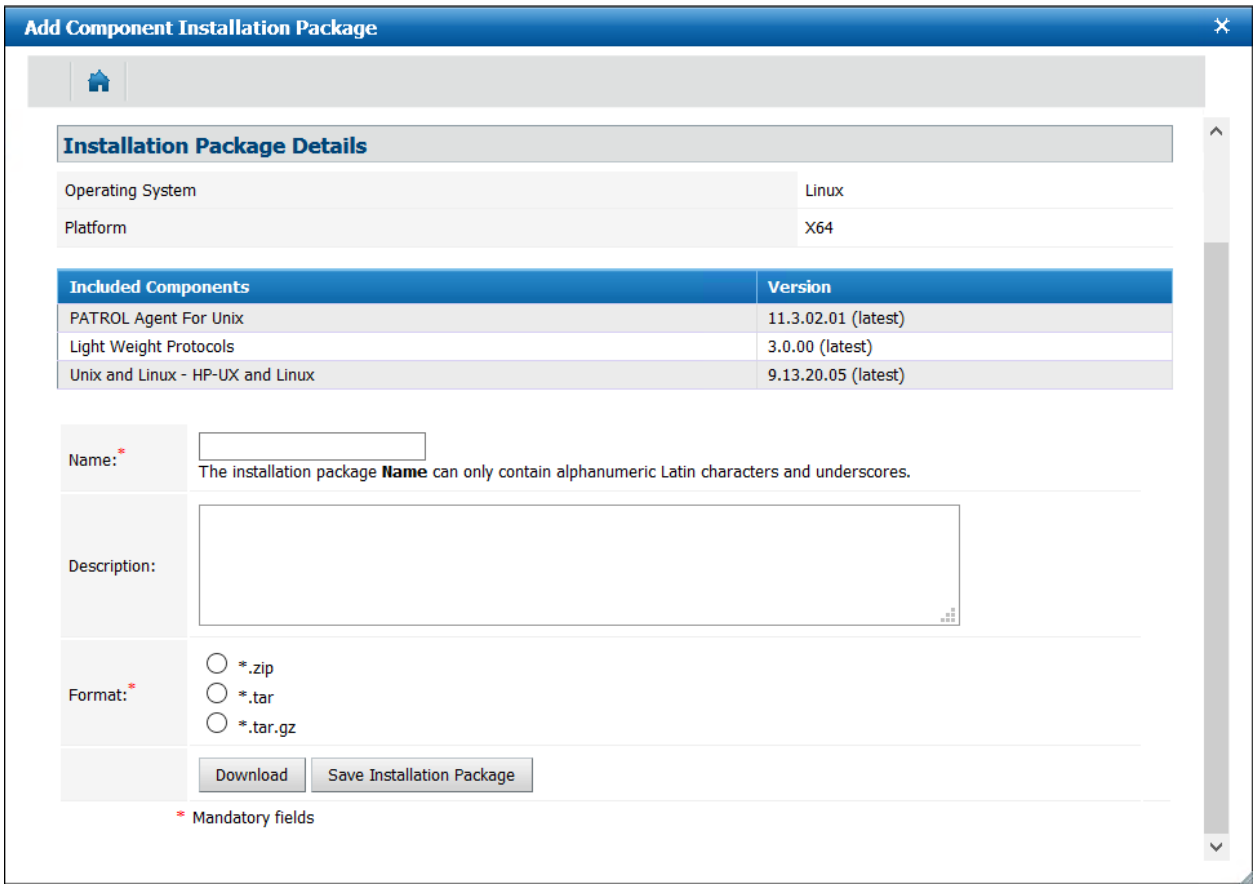


Рисунок 19 – Заключительный этап создания агента мониторинга

3.2 Подготовка серверов к постановке на мониторинг и установка агентов мониторинга

Для корректной работы агента мониторинга на целевом сервере необходимо произвести подготовительные мероприятия. Они будут разниться от выбора портов, имен серверов мониторинга, выбора оборудования для серверов мониторинга. Рассмотрим общий случай:

1) на сервере должен быть создан пользователь с администраторскими правами, логин и пароль должны совпадать с таковыми в конфигурации пакета инсталляции;

2) должны быть открыты порты, по которым агент обращается к Integration серверу и ProactiveNet серверу;

3) необходимо вручную создать папку «/opt/bmc/», в нее агент будет устанавливать свои компоненты;

4) пользователь должен получить права на запись, чтение и редактирование данной папки;

5) в файл «/etc/hosts/» необходимо прописать соответствие ip-адреса и hostname сервера, так как агент берет информацию именно оттуда.

После выполнения всех предшествующих условий, можно приступать к инсталляции агента мониторинга. Порядок действий следующий:

1) загружается пакет инсталляции с репозитория либо с памяти устройства (в зависимости от того, куда он был сохранен);

2) пакет инсталляции копируется в папку пользователя, созданного ранее;

3) запускается приложение инсталляции.

После завершения установки агент будет показан в администраторской консоли как активный. Если этого не произошло, возможно, были совершены ошибки в предыдущих шагах – конфигурировании инсталляционного пакета либо в подготовительных мероприятиях.

3.3 Создание политики проверки

После того, как агенты были успешно установлены на целевые серверы, можно приступать к созданию политики проверки. Для этого заходим в консоль администратора и нажимаем «Создать новую политику». На рисунке 20 показано начальное окно создания политики проверки.

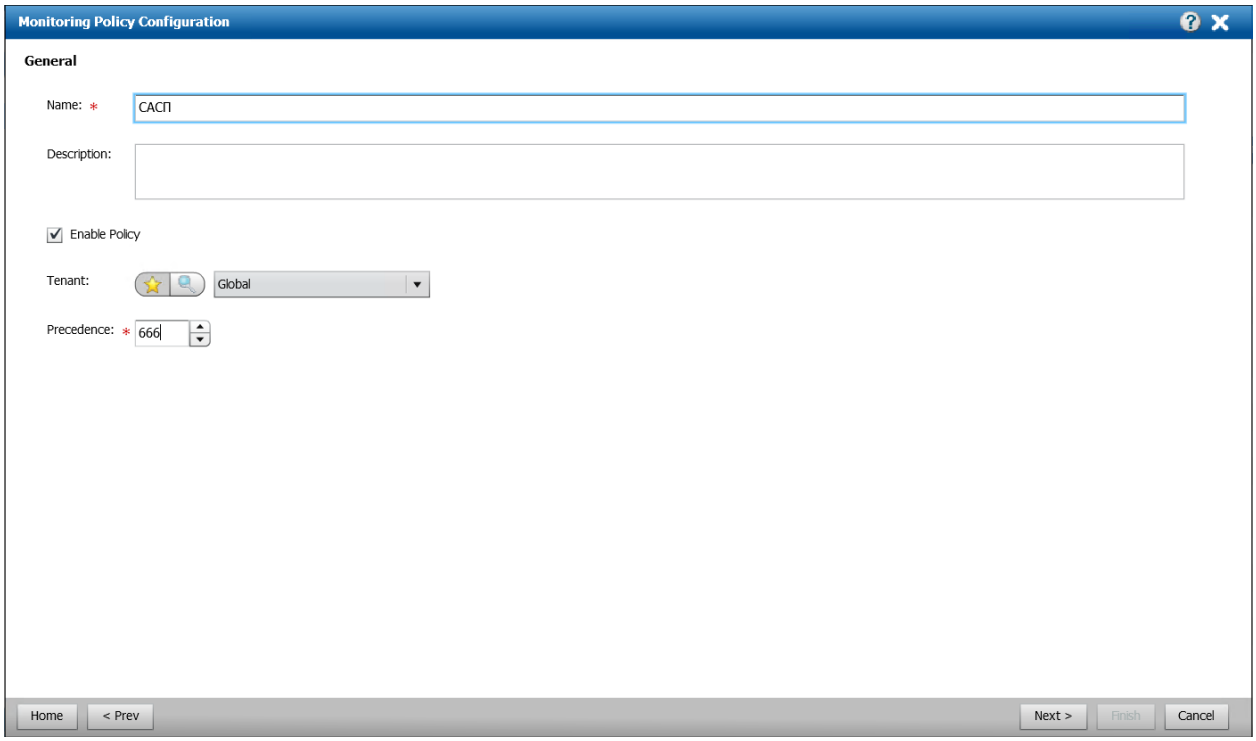


Рисунок 20 – Создание политики

В этом окне есть поле «Name» – имя политики, «Description» – описание политики, а также поле «Precedence» – это порядок политики в иерархии. Политика с числом ниже будет обрабатываться в первую очередь по сравнению с политикой с высшим числом. Также сразу нажимаем «Enable policy» – если этого не сделать, то политика будет неактивной.

Следующим шагом необходимо указать политике, на какие серверы она должна распространяться. Это можно сделать в следующем окне, которое представлено на рисунке 21.

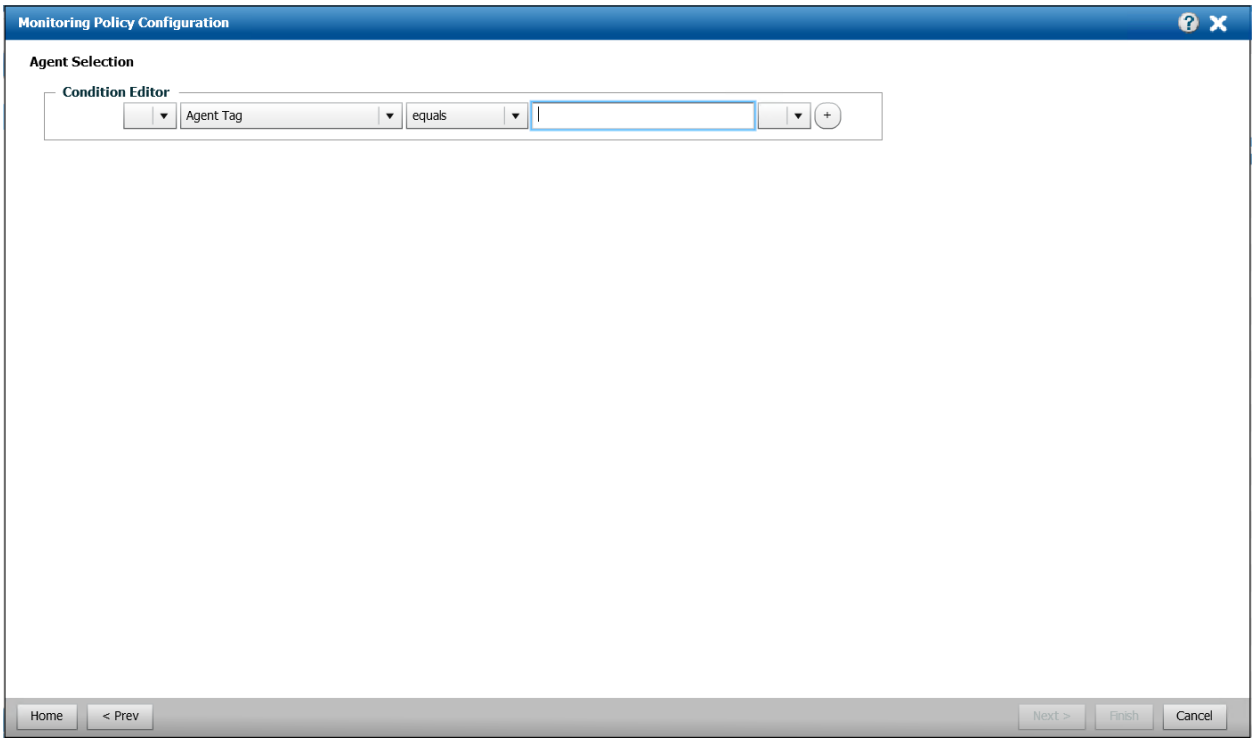


Рисунок 21 – Окно выбора серверов

В данном окне необходимо указать параметр, по которому будут отбираться серверы, на которые будет действовать политика. Если при создании пакета инсталляции был указан тэг, то есть возможность по отобрать серверы только лишь по нему. Намного труднее дело обстоит, когда тэг не был указан – тогда собрать все серверы в одну политику можно лишь по hostname. Так как при создании пакета инсталляции был указан тэг, вводим его в поле «Condition Editor».

Далее необходимо выбрать, какие данные будут собираться. Для этого в следующем окне выбираем модули, которые были указаны при конфигурировании пакета инсталляции. На рисунке 22 показано окно для настройки модулей.

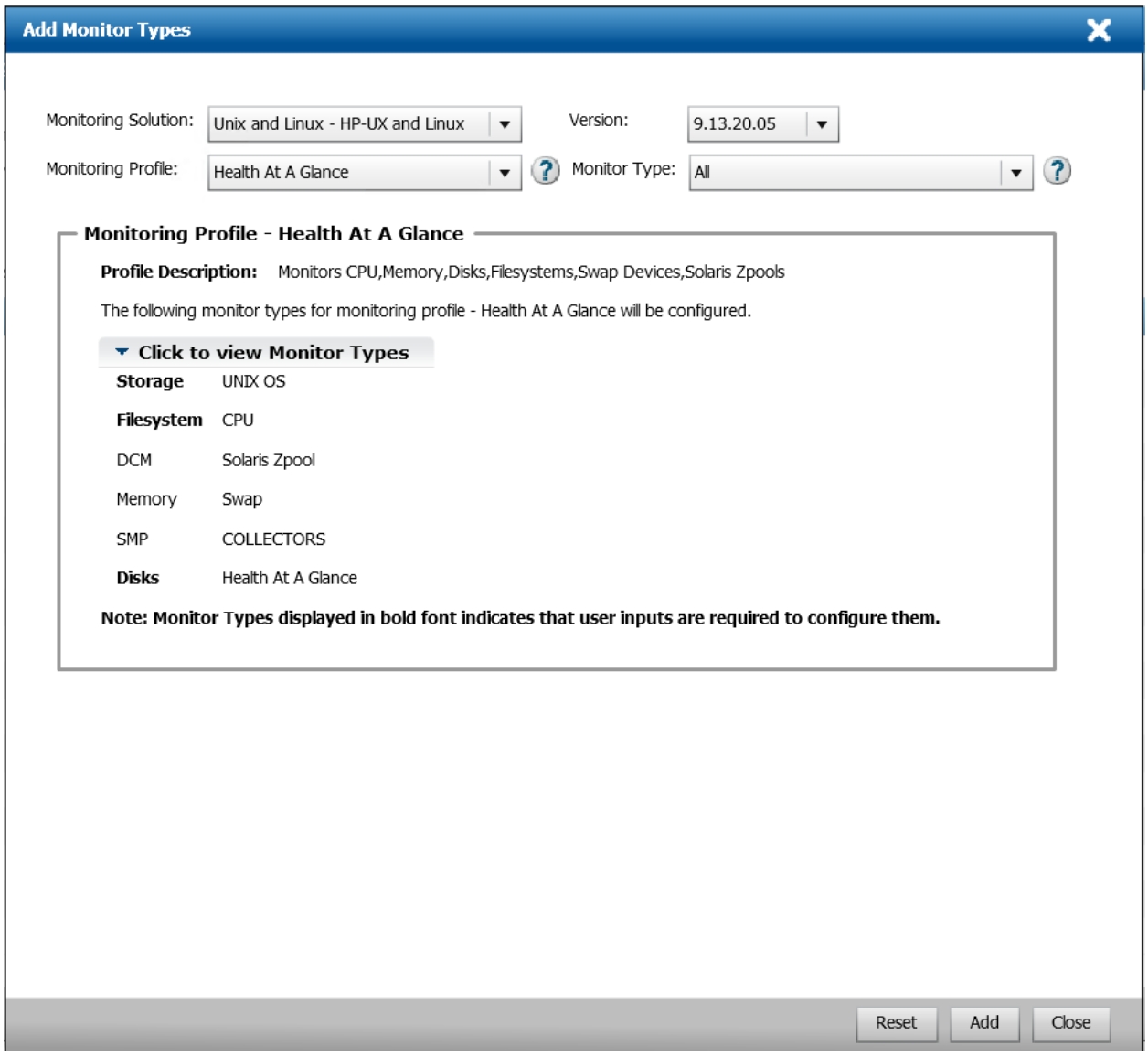


Рисунок 22 – Выбор собираемых данных

На рисунке 22 видно, что на данный момент выбран модуль «Unix and Linux – HP-UX and Linux». Он включает в себя необходимые проверки процессора, дискового пространства, оперативной памяти, а также Swap. Также нам понадобится добавить модуль «Light Weight Protocols», чтобы организовать проверку по команде ping.

Следующим шагом будет установка порогов срабатывания для метрик, которые будут собираться с помощью политики. Для этого, в следующем окне,

выберем интересующий нас модуль, в нем выберем проверку, и настроим вид критичности: MINOR, MAJOR или CRITICAL. Это можно увидеть на рисунке 23.

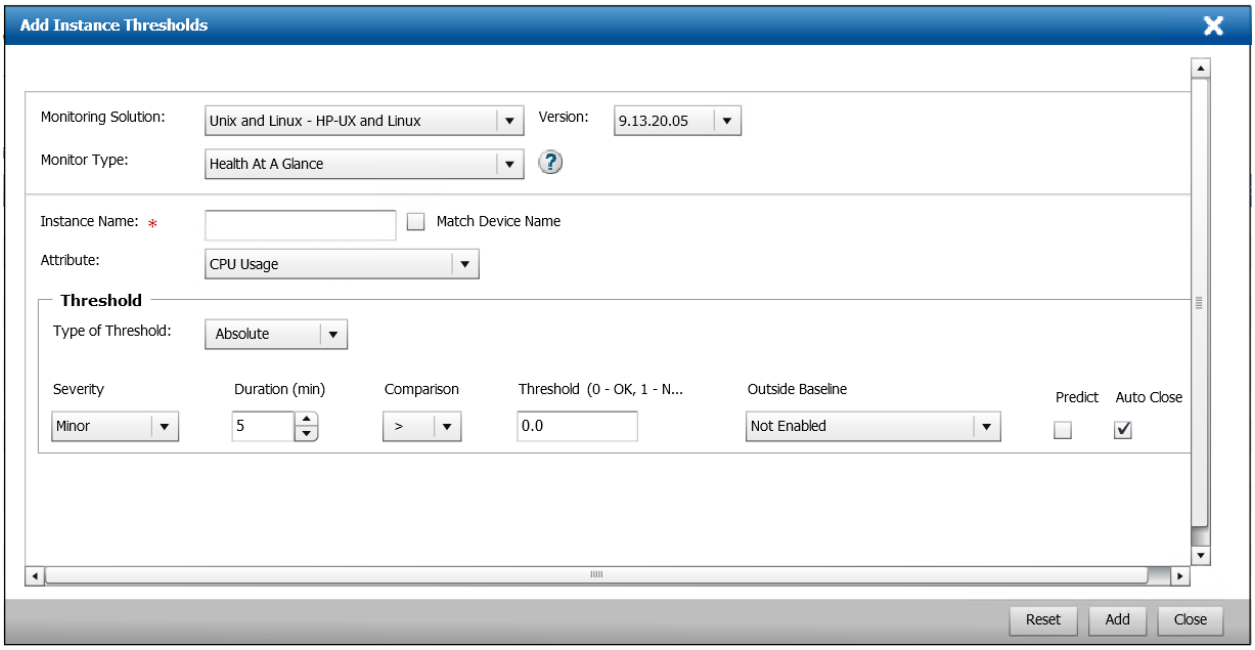


Рисунок 23 – Выбор порогов срабатывания аварийных событий

В данный момент на рисунке 24 можно увидеть, что выбран параметр «CPU Usage» – использование процессора. Установлена критичность Minor, длительность – 5 минут. Длительность – важный параметр системы, так как она работает по следующему принципу: один раз в заданную длительность выполняется проверка указанного параметра. При провале проверки аварийное событие не генерируется. Оно создается только после второй проваленной подряд проверки. Также это работает и с закрытием события – после двух успешных проверок система считает работоспособность восстановленной. «Comparsion» – это параметр, который определяет, будет ли событие генерироваться при превышении заданной линии на графике, или же, наоборот, при ее снижении. Выставим условие как «больше». «Threshold» – это значение, после превышения или понижения которого сработает аварийное событие. После настройки данного параметра

настроим остальные согласно техническому заданию, взятому из карточки мониторинга.

После этого достаточно проверить окно подключенных агентов к политике, чтобы убедиться, что политика успешно на них применилась. Для того, чтобы убедиться, что данные настройки – модули проверок и пороги срабатывания настроены правильно, зайдем в консоль оператора. Введем в поисковую строку название сервера, который находится под влиянием политики. Это показано на рисунке 24.

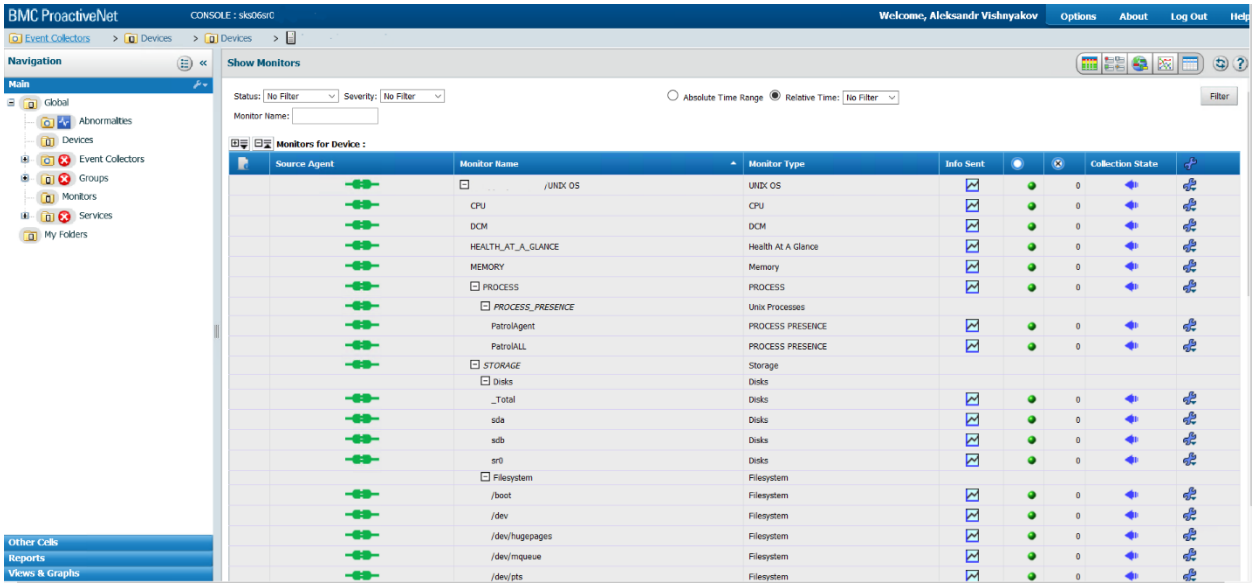


Рисунок 24 – Параметры проверок на сервере

Как видно на рисунке 24, сервер виден в списке устройств, и политика применилась к нему корректно. Все необходимы модули состоят на мониторинге.

3.4 Создание ресурсно-сервисной модели

Для того, чтобы операторы системы мониторинга всегда имели представление о состоянии сервиса в режиме реального времени, а также, чтобы видеть иерархию серверов, необходимо создать ресурсно-сервисную модель. В

общем случае это логическая схема системы, в которой видно их влияния друг на друга.

Для этого воспользуемся BMC CMDB Atrium. Это программное обеспечение как раз для того, чтобы создавать ресурсно-сервисные модели для системы BMC ProactiveNet, с последующей их выгрузкой на Publishing сервер. На рисунке 25 показаны элементы ресурсно-сервисной модели.

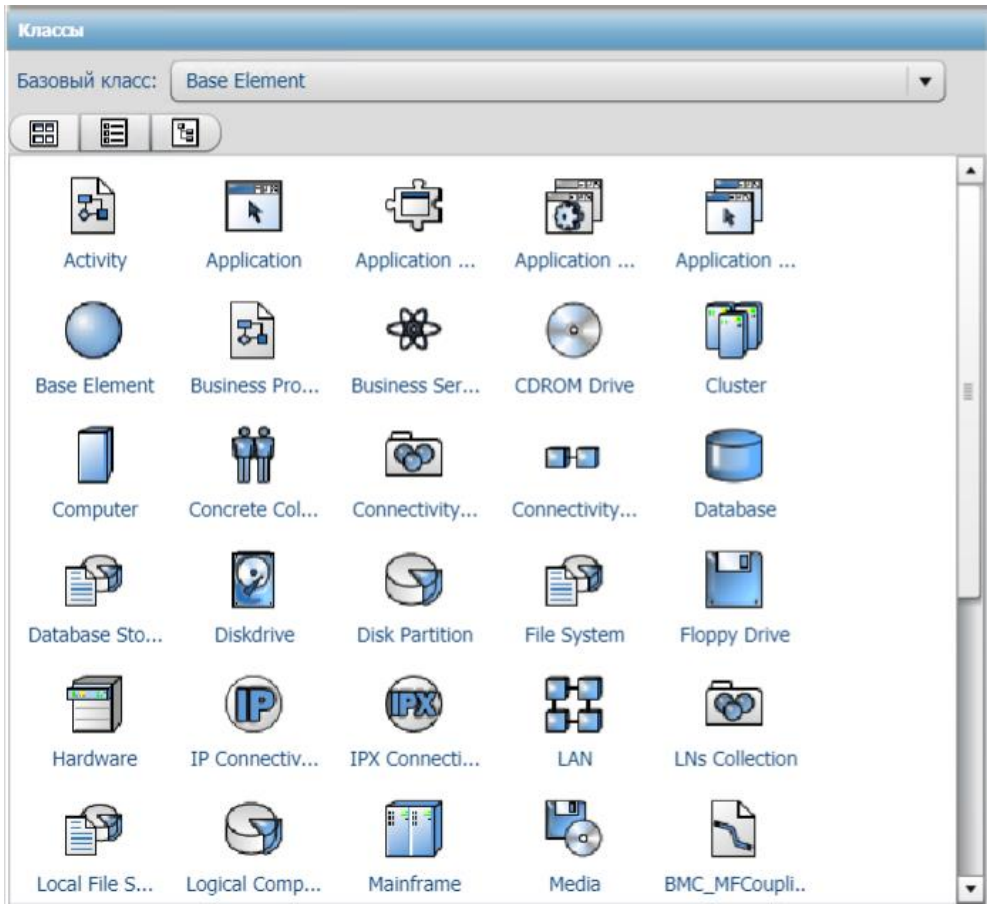


Рисунок 25 – Логические элементы BMC CMDB Atrium

Откроем BMC CMDB Atrium. В нем представлено пространство для создания ресурсно-сервисной модели – «Impact Model Designer». Это пространство предлагает нам создание из логических элементов, каждый из которых отвечает за свою роль. Рассмотрим некоторые из них, которые будут задействованы в данной работе:

1) Business service – это элемент, создание которого добавит эту ресурсно-сервисную модель в консоль оператора, является высшим в иерархии;

2) Computer – физический сервер, на нем будут указано состояние сервера согласно системному мониторингу;

3) Logical Component – логический компонент, который не привязан ни к какому из серверов. Может служить перенаправляющим звеном – с помощью переназначения событий, вместо того, чтобы создаваться на сервере, они будут указываться как события на логической единице. Это очень полезно при создании сложных схем, либо переназначения более критичного события на логический элемент, который выше по иерархии, чтобы он имел большее влияние на сервис.

Следующим шагом будет создание из данных элементов ресурсно-сервисной модели. Для этого необходимо создать столько же элементов «Computer», сколько серверов в системе. После этого их необходимо настроить, чтобы агент мониторинга мог присоединиться к логическому элементу по заданным параметрам. Такие параметры называются «Alias» – когда агент успешно устанавливается на сервер, он создается Alias, название которого он берет из файла «/etc/hosts/». Таким образом, связать сервер и логический компонент легче всего по hostname сервера, хотя это и не единственный способ. К примеру, можно указать Alias при инсталляции агента мониторинга, и точно такой же на логическом компоненте. На рисунке 26 показана настройка параметров логического компонента ресурсно-сервисной модели.

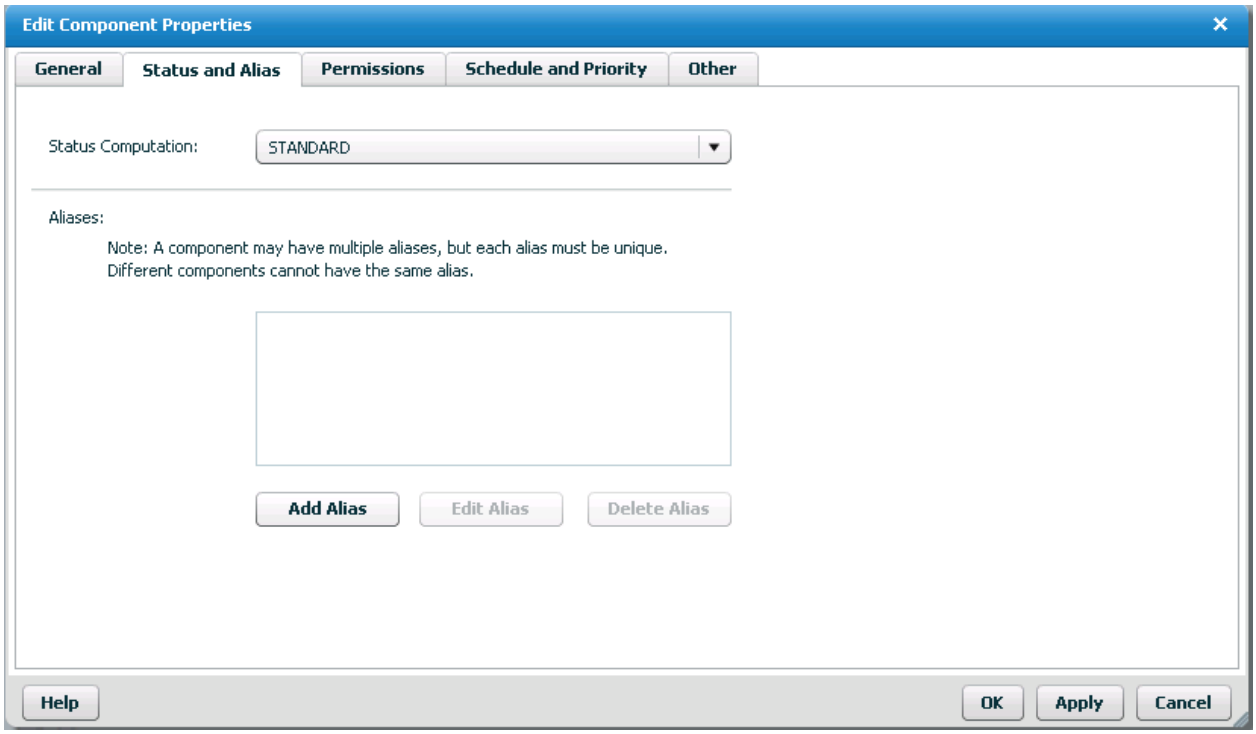


Рисунок 26 – Настройка параметров логического компонента

После настройки всех элементов, их необходимо соединить с логическим компонентом «Business Service». Таким образом, они преобразуются в ресурсно-сервисную модель, которая при выполнении публикации выгрузится в ProactiveNet сервер и будет доступна для просмотра в консоли оператора. Выполненные ресурсно-сервисные модели представлены в приложении В и приложении Г.

3.5 Мониторинг ошибок в работе оборудования с помощью SMNP-ловушек

Для бесперебойной работы оборудования, в частности, коммутатора и источника бесперебойного питания, необходимо своевременно получить от них оповещения об ошибках в их работе. Для этого воспользуемся SMNP-ловушками, которые будут отправляться на ProactiveNet сервер. После получения SNMP-ловушки генерируется аварийное событие, в котором содержится информация об

ошибке. Это событие поступает в коллектор событий и пересылается на группы рассылки ответственных лиц.

3.6 Расчет экономической эффективности

Для того, чтобы рассчитать экономическую эффективность от данного проектного решения, воспользуемся формулой 3:

$$M = \frac{P}{E \cdot A \cdot h}, \quad (3)$$

где M – количество месяцев до полной окупаемости проектного решения,

P – полная стоимость, затраченная на оборудование,

E – количество сотрудников, которых затронет данное проектное решение,

A – расчетная почасовая ставка сотрудника,

h – количество часов в месяц, которое сэкономит данное проектное решение для каждого сотрудника.

На данный момент в отделе технической поддержки внутренних пользователей работает 15 человек. Расчетная ставка равна 130 рублей в час. Чтобы получить количество часов в месяц, которое сэкономит данное проектное решение для каждого сотрудника, необходимо перевести расчетное увеличение доступности сервисов, ожидаемое от проектного решения, в часы. Расчетное увеличение доступности сервисов – 15%. Расчет будем вести от рабочего времени в часах за месяц. За апрель 2020 года было отработано 176 часов. Значит, количество сэкономленных часов будет составлять:

$$176 \cdot 0{,}15 = 26{,}4$$

Постановка на мониторинг сервисов Базы Знаний и САСП расчетно увеличит время их безотказной работы на 26,4 часов рабочего времени в месяц. Подставляя эти значения в формулу 3, получим:

$$\frac{420522}{15 \cdot 130 \cdot 26{,}4} = 8{,}2$$

Из данной формулы мы можем сделать вывод, что данное проектное решение полностью окупится через 8,2 месяцев.

В данной главе была выполнена замена коммутатора и источника бесперебойного питания, установка серверов для системы мониторинга BMC ProactiveNet 9.6, постановка на мониторинг систем САСП и База Знаний, а также расчет экономической эффективности введения проектного решения. В результате было выявлено, что полная окупаемость составляет 8,2 месяцев.

ЗАКЛЮЧЕНИЕ

Результатом выполнения дипломной работы является проектирование и постановка на мониторинг корпоративной сети Департамента ситуационного реагирования и аналитики ПАО «Ростелеком». Потребность в замене оборудования и постановке серверов сервисов Базы Знаний и САСП была обусловлена следующими причинами:

1) необходимость в замене устаревшего оборудования;
2) потребность в увеличении пропускной способности коммутатора;
3) потребность в контроле состояния оборудования;
4) потребность в увеличении емкости источника бесперебойного питания;
5) потребность в увеличении времени бесперебойной работы сервисов, критичных для работы отдела технической поддержки.

Были изучены основные виды мониторинга, системы мониторинга, технология SNMP-ловушек. Также был получен опыт в проектировании корпоративной сети, системы мониторинга, постановки важных для бизнеса систем на мониторинг. Был осуществлен анализ оборудования, программного обеспечения для постановки на контроль серверов IT-систем и IT-сервисов.

В результате расчета экономической эффективности данного проектного решения было выяснено, что оно полностью окупится спустя 8,2 месяцев.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 BMC ProactiveNet 9.6 документация [Электронный ресурс]. – Режим доступа: https://docs.bmc.com/docs/display/public/proactivenet96/Home?key=proactivenet96. – Загл. с экрана.

2 SCOM [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/System_Center_Operations_Manager. – Загл. с экрана.

3 Потемкин С. А. Формирование системы финансового мониторинга в кредитных организациях. Учебное пособие / Потемкин С. А. – М.: Кнорус. 2010.

4 Гаранин М.В. Системы и сети передачи информации / М.В. Гаранин и др. – М.: Радио и связь, 2001.

5 Построение СКС [Электронный ресурс]. – Режим доступа: http://www.xnets.ru/plugins/content/content.php?content.96.2. – Загл. с экрана.

6 Электронный каталог HP Proliant [Электронный ресурс]. – Режим доступа: https://www.proliant.ru/catalog/. – Загл. с экрана.

7 Прокимнов Н. Н. Моделирование мониторинговых процессов. Прикладная информатика / Прокимнов Н. Н. – М. : Издательство «Синергия», 2010.

8 Бариленко В.И. Информационно-аналитические методы оценки и мониторинга эффективности инновационных проектов / Под ред. проф. В.И. Бариленко ; В.И. Бариленко, В.В. Бердников, О.Ю. Гавель, Ч.В. Керимова. – М. : Издательство «Русайнс», 2015.

ПРИЛОЖЕНИЕ А

(обязательное)

Технические требования для серверов мониторинга

Таблица А.1 – Технические требования для серверов мониторинга

Элементы системы мониторинга	Процессор			Оперативная память			Жесткий диск		
	min	med	max	min	med	max	min	med	max
ProactiveNet Server	4	4	8(16)	8	32	48	100	200	400
Remedy SSO	2	2	2	2	2	2	10	10	10
TS Presentation Server	4	4	8(16)	8	32	48	100	200	400
TS Infrastructure Management Server with SAP SQL Anywhere EBF	4	4	8	16	32	48	200	300	600
TS Infrastructure Management Server with Oracle	4	4	8	16	24	40	30	50	100
TS Integration Service Server (Proxy) на 500 и 900 агентов	2	4	8	2	8	40	30		
Oracle DB for TSIM Server	4	4	8	16	32	32	170	250	500
Atrium ARS + CMDB	4	4	8(16)	8	32	48	100	200	400

ПРИЛОЖЕНИЕ Б

(обязательное)

Спецификация оборудования

Таблица Б.1 – Спецификация оборудования

Наименование	Тип, марка	Завод изготовитель	Ед. измер-я	Кол-во	Цена за шт	Сумма
1	2	3	4	5	6	7
1. Коммутатор FS S3900-24T4S	Коммутатор	FS	шт.	1	26 785	26 785
2. ИБП APC Smart-UPS SMT1500RMI2U, 1500BA	Источник бесперебойного питания	APC	шт.	1	69 399	69 399
3. Сервер HPE ProLiant dl20 Gen10 (1U), процессор Intel Xeon E-2124 (3.3GHz/4-core/71W), оперативная память 8GB (1x8GB) Single Rank x8 DDR4-2666,жесткий диск 1TB 3,5" (LFF) SATA 7.2K 6G Non-HP	Сервер	HP	шт.	3	77 975	233 925
4. Сервер HPE ProLiant dl20 Gen10 (1U), процессор Intel Xeon E-2124 (3.3GHz/4-core/71W), оперативная память 2x8GB (1x8GB) Single Rank x8 DDR4-2666,жесткий диск 1TB 3,5" (LFF) SATA 7.2K 6G Non-HP	Сервер	HP	шт.	1	90 413	90 413
Итого						420 522

ПРИЛОЖЕНИЕ В

(обязательное)

Ресурсно-сервисная модель сервиса САСП

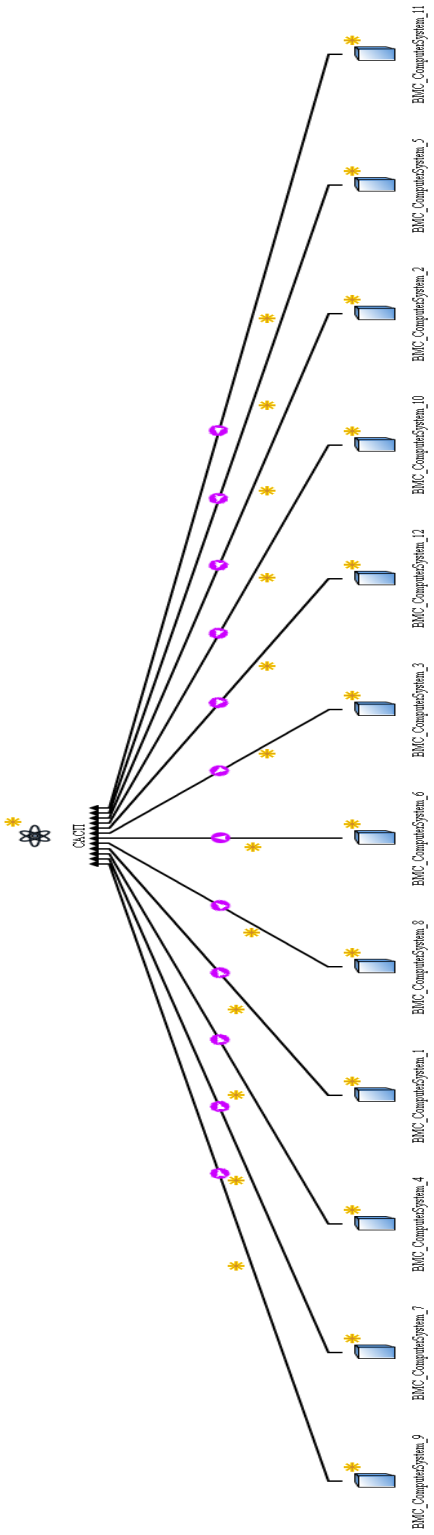


Рисунок В.1 – Ресурсно-сервисная модель сервиса САСП

ПРИЛОЖЕНИЕ Г

(обязательное)

Ресурсно-сервисная модель сервиса База Знаний

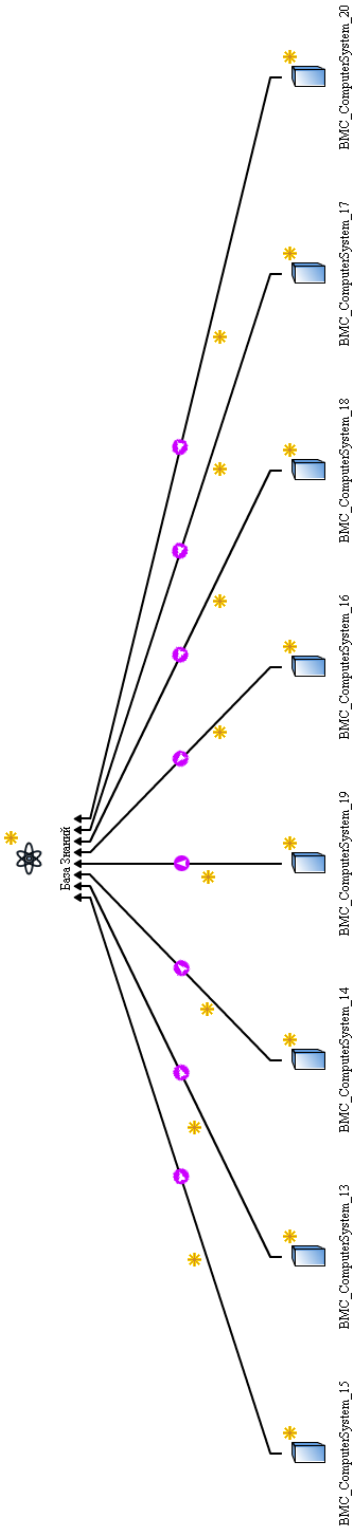


Рисунок Г.1 – Ресурсно-сервисная модель сервиса База Знаний