



Специализированные системы мониторинга

Сценарии использования в энергетике

❖ Вопросы и проблемы:

- Большое количество объектов мониторинга
- Различные приложения мониторинга для одних задач
 - сложность сбора полной информации
 - невозможность эффективного контроля SLA
- Различные требования к визуализации от пользователей
 - инструменты управления
 - различные формы отчетности

❖ Задачи развития ИТ:

- Повышение качества ИТ-сервисов для пользователей
- Повышение эффективности эксплуатации ИТ
- Повышение эффективности инвестиций в ИТ



Создание унифицированной системы мониторинга
Формирование пула типовых решений по мониторингу
Разработка универсальных регламентов мониторинга

Проблематика систем мониторинга

ИСТОЧНИКИ ДАННЫХ

- Мультивендорная инфраструктура
- Разнородные системы управления
- Разнородные протоколы взаимодействия

ОШИБКИ

- Возможна неверная интерпретация событий
- Задержки внесения изменений (при изменении объектов мониторинга)

ПРОЦЕССЫ

- Неэффективное управление ресурсами
- Неэффективное планирование
- Потеря контроля за инцидентами



По объектам мониторинга

- Например:
 - Сеть, Технологическое оборудования, Информация

По целям

- Например:
 - Информационная безопасность, (Качество) Оптимизация производительности, обеспечение надежности

По пользователям

- Например:
 - Руководство, Эксплуатация, Разработчики

Финансы

- Оптимизация затрат на обслуживание ИТ инфраструктуры
- Снижение убытков от недоступности сервисов



Качество (надежность, производительность)

- Снижение времени простоя сервисов и времени реагирования на выявленные сбои и нарушения
- Контроль за состоянием и качеством предоставляемых сервисов, критичных для бизнеса



Контроль

- Централизованное управление инфраструктурой и системами, включая проактивный мониторинг, для предупреждения возможных проблем и минимизации рисков



Безопасность

- Защита от угроз информационной безопасности и предотвращение утечек



Сценарии использования систем мониторинга

- Влияние производительности сервиса на бизнес показатели
- Формирование и мониторинг SLA
- Аналитические данные для маркетинга
- Оценка инвестиций в ИТ



- Анализ производительности до уровня кода через все слои приложения
- Быстрая диагностика и локализация проблем
- Быстрый поиск ошибок при тестировании
- Возможность динамически вносить изменения

- Видимость сервиса на всех уровнях в режиме 24x7
- Быстрая диагностика и локализация проблем
- Анализ узких мест в ИТ-инфраструктуре
- Анализ и контроль КПЭ по внешним сервисам и подрядчикам

Подход к мониторингу «сверху-вниз»

Отслеживание всей цепочки доставки сервиса от пользователя к инфраструктуре



Типы решений мониторинга

Комплексные решения («линейки») мониторинга

- Решения HP, BMC, EMC
- Комплексный набор «специализированных» решений



Универсальные платформы («конструкторы») для реализации мониторинга

- Zabbix, Инити

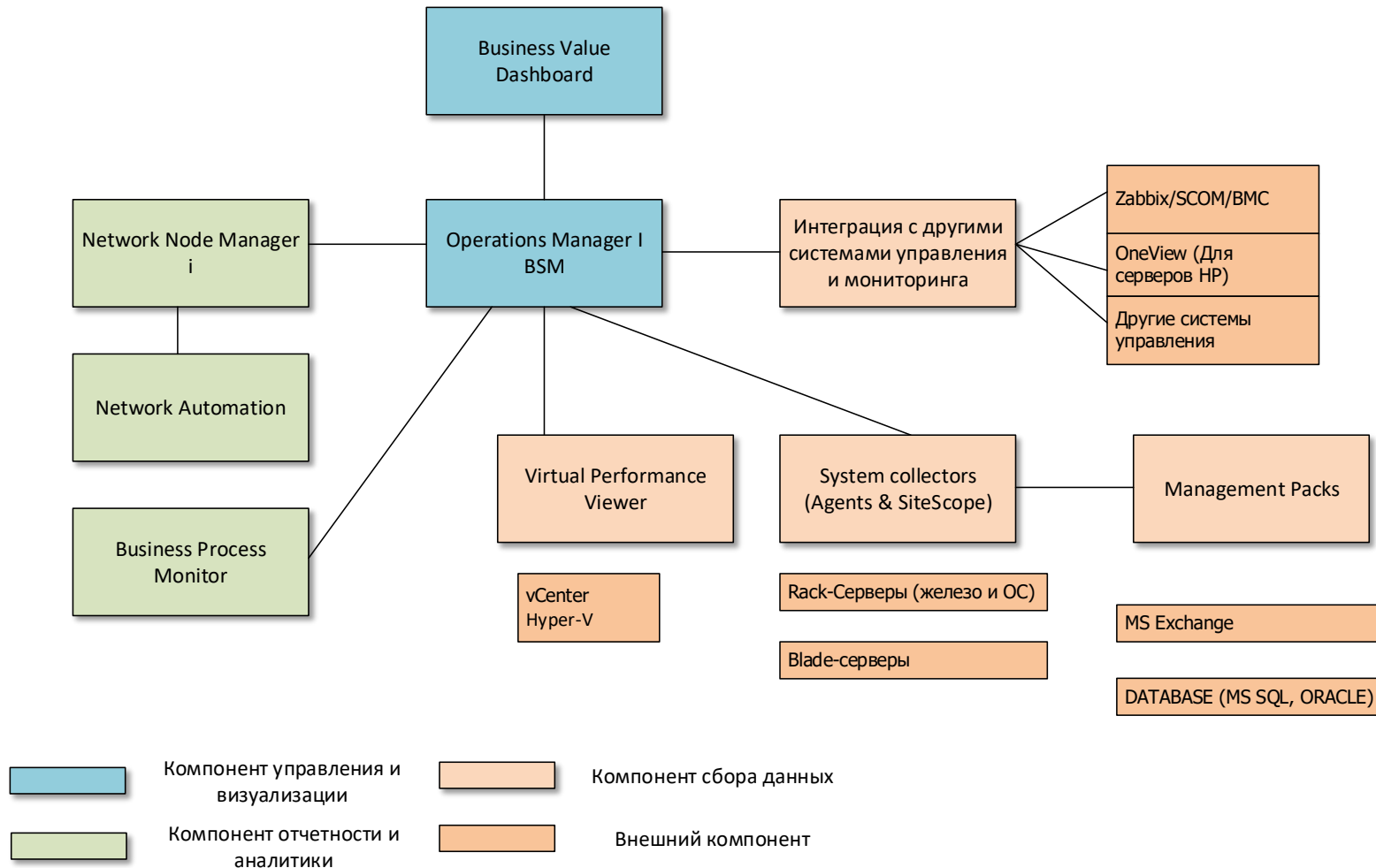


Специализированные решения

- Dynatrace, HP ArcSight
- Журналы событий Windows, Центр администрирования MS SharePoint, SAP Event monitor VMware

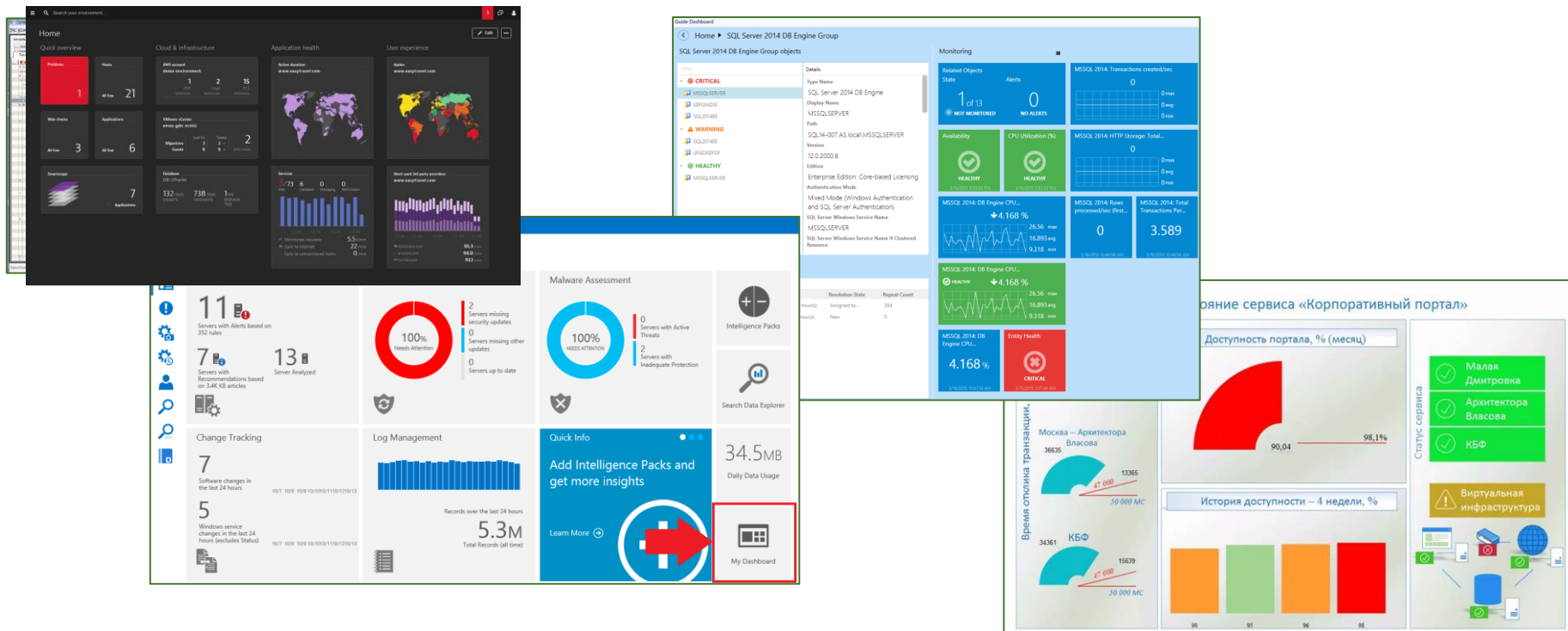


Компоненты комплексной системы мониторинга (пример)



Зонтичная система мониторинга

- Объекты мониторинга – ИТ-сервисы\Бизнес-приложения
- Назначение – Надежность + Качество
- Пользователи – Руководство, Эксплуатация

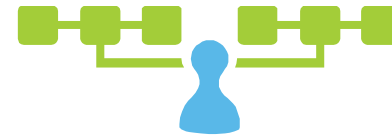


Ресурсы, необходимые для создания зонтичной системы мониторинга

Персонал (штатная
структура \аутстаффинг)



Процессы
(утверждённые процедуры и
регламенты)



Готовность источников данных
(внешние системы,
настроенные интерфейсы)



Шаг 1. Анализ задачи

- Объект мониторинга?
- Пользователи системы? Показатели и реакция?
- Последствия отказа? (финансовые потери)
- Контрольный срок
- Уже используемые платформы мониторинга?


Рекомендации по выбору

 **Сценарий 1.** *Сжатые сроки. Существенные последствия отказа*

- Использование узкоспециализированных решений (в составе используемой комплексной системы или отдельных)

 **Сценарий 2.** *Разумные сроки. Пользователи = эксплуатация*

- Реализация решения (доп. настроек) на используемой универсальной платформе мониторинга

 **Сценарий 3.** *Цель – ситуационный центр. Сроки и бюджеты позволяют*

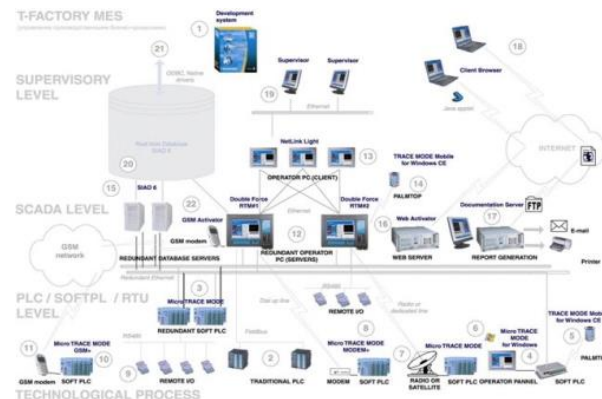
- Выбор комплексного решения для мониторинга под основные категории объектов мониторинга

Ситуационный центр

Единый ситуационный центр

Сбор всех событий, необходимых для принятия решений:

- Сообщения оборудования IP сетей, транспортных сетей, сетей передачи данных, оборудования сетей спутниковой связи
- Сообщения тех. процессов: Контроллеры, АСУТП, SCADA
- Сообщения оборудования электрообеспечения, кондиционирования, датчиков
- Сообщения БД, приложений, систем хранения данных
- Сообщения подсистем информационной безопасности – межсетевые экраны, антивирусы, DLP и пр.





Системы мониторинга. Примеры

Инити. Zabbix. Dynatrace.

Единая платформа для сбора и нормализации данных с большого количества разнородных источников безагентными методами

- Access Control, Authentication
- DLP системы
- IDS/IPS системы
- Антивирусные приложения
- Журналы событий серверов и рабочих станций
- Межсетевые экраны
- Активное сетевое оборудование
- Сканеры уязвимостей
- Системы инвентаризации и asset-management
- Системы web фильтрации
- Технологическое оборудование и системы управления



- **Пассивный сбор** «сырых» событий – SNMP trap, Syslog и пр..

Типы алармов

Тип	Шаблон з...	Шаблон id	Системный	Типы соб...	Очищающ...	Переменн...
atAu	По возрастанию		<input checked="" type="checkbox"/>	data": "etA...	[]	[]
atComponen	По убыванию		<input checked="" type="checkbox"/>	data": "etC...	[{"data": "etC...	[]
atComponen	Колонки		<input checked="" type="checkbox"/>	data": "etC...	[{"data": "etC...	[]
atCustomAlarm	%title%	%alr	<input checked="" type="checkbox"/>		[]	[]
atEgpNeighbo...	etEgpNeighb...	%m	<input checked="" type="checkbox"/>	data": "etE...	[]	[]
			<input checked="" type="checkbox"/>			
			<input checked="" type="checkbox"/>			

Тип
 Шаблон заголовка
 Шаблон id
 Системный
 Типы событий
 Очищающие события
 Переменные

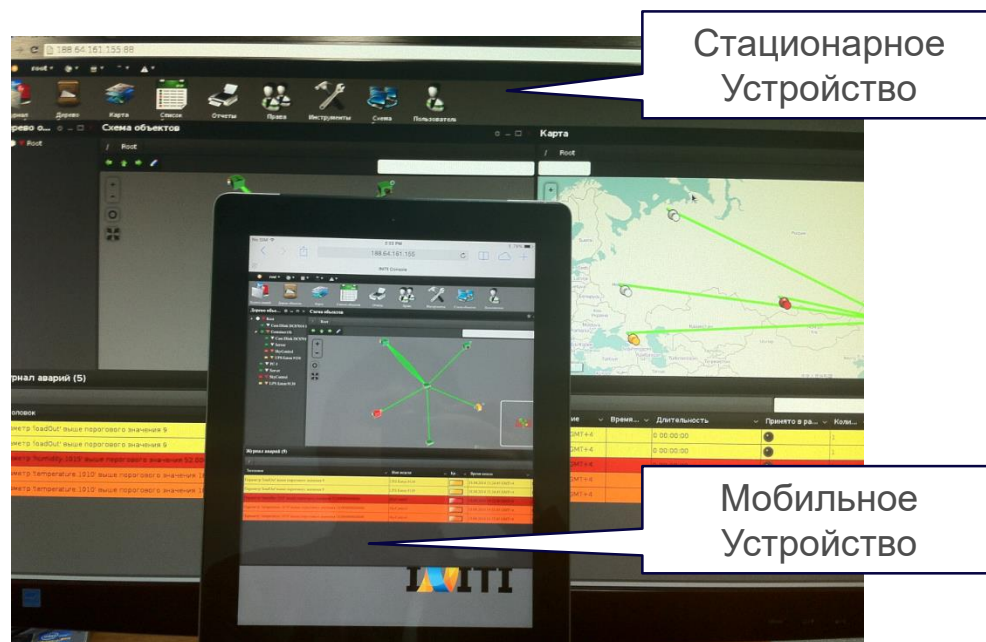
Моделирование топологии

Визуальное отображение видов связанности.

Заголовок	Имя моде...	Критично...	14.11.2014 12...	14.11.2014 12...		atModeThresh...	1	m.mm.g.10.0.0.2	server
Параметр 'totalCpuUsage' выше порогового зн...	OracleSrv2								
Параметр 'totalCpuUsage' выше порогового зн...	OracleSrv1								
Параметр 'totalCpuUsage' выше порогового зн...	OracleSrv3								
Параметр 'totalCpuUsage' выше порогового зн...	OracleSrv4								
Параметр 'humidity' выше порогового значе...	Инженерное								

Уровень представления

- Полнофункциональный веб-интерфейс предоставляет полный набор инструментов для анализа событий и построения отчётов;
- GUI с возможностью редактирования режимов отображения "на лету"
- Поддержка мобильных устройств;
- Возможность оптимизировать интерфейс для каждого пользователя



Основные характеристики:

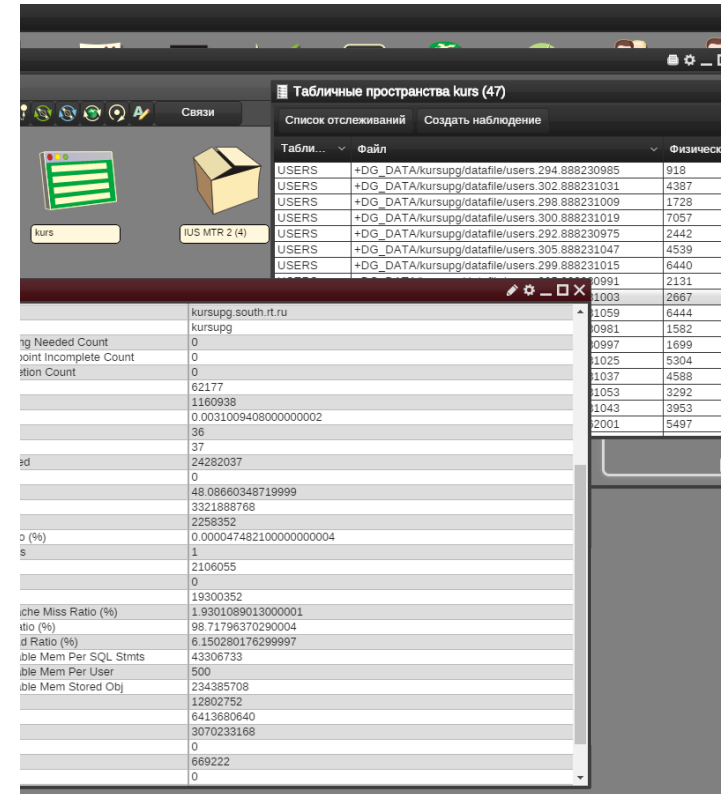
- Инвентарные отчёты
- Общее распределение
- Состояние схемы
- Прогнозирование роста
- Отчёты по утилизации в реальном времени

Преимущества:

- Оценка производительности баз данных/схем
- Понимание трендов утилизации ресурсов
- Устранение проблем производительности в реальном времени
- Прогнозирование роста на основе исторических значений

Контролируемые метрики:

- Макро статистика (подключения пользователей, размер базы данных, время безотказной работы и т.д.)
- Статистика пользователей (коммиты, откаты)
- Производительность (Сканирование таблиц, полное сканирование индексов и т.д.)
- Статистика системного журнала
- Статистика файлов базы данных



Таблицные пространства kurs (47)

Список отслеживаний Создать наблюдение

Табл...	Файл	Физическ
USERS	+DG_DATA/kursupg/datafile/users.294.888230985	918
USERS	+DG_DATA/kursupg/datafile/users.302.888231031	4387
USERS	+DG_DATA/kursupg/datafile/users.298.888231009	1728
USERS	+DG_DATA/kursupg/datafile/users.300.888231019	7057
USERS	+DG_DATA/kursupg/datafile/users.292.888230975	2442
USERS	+DG_DATA/kursupg/datafile/users.305.888231047	4539
USERS	+DG_DATA/kursupg/datafile/users.299.888231015	6440
		10991
		2131
		1003
		2667
		1059
		6444
		0981
		1582
		1097
		1699
		1025
		5304
		1037
		4588
		1053
		3292
		1043
		3953
		2001
		5497

ig Needed Count	0
joint Incomplete Count	0
tion Count	0
	62177
	1160938
	0.0031009408000000002
	36
	37
id	24282037
	0
	48.08660348719999
	3321888768
	2258352
o (%)	0.00004748210000000004
s	11
	2106055
	0
	19300352
iche Miss Ratio (%)	1.9301089013000001
tio (%)	98.71796370290004
d Ratio (%)	6.150280176299997
ble Mem Per SQL Stmt	43306733
ble Mem Per User	500
ble Mem Stored Obj	234385708
	12802752
	6413680640
	3070233168
	0
	669222
	0

Мониторинг приложений

Обнаружение: Сбор данных напрямую или от элемент-менеджеров (систем управления) компонент технологического сегмента:

- Контрольно-измерительные приборы
- Контроллеры (ПЛК)
 - Универсальные программируемые контроллеры
 - PC-совместимые контроллеры
 - Программируемые реле
- Рабочие станции пользователя (АРМ)

Используется:

- SNMP, CLI (Telnet, SSH), NetBus, ModBus, RS XXX

Осуществляется кросс-доменная корреляция с прочими технологическими доменами

Сбор и мониторинг событий ИБ

Функционал:

- Выявление сетевых атак во внутреннем и внешнем периметре
- Выявление вирусных эпидемий и отдельных заражений
- Выявление попыток несанкционированного доступа
- Выявления уязвимостей
- Выявления ошибок в конфигурациях СРЗИ и информационных системах
- Выявления целевых атак (АРТ)

Источники:

- Access Control, Authentication
- DLP системы
- Антивирусные приложения
- Журналы событий серверов и рабочих станций
- Межсетевые экраны
- Активное сетевое оборудование
- Сканеры уязвимостей
- Системы инвентаризации и asset-management
- Системы web фильтрации
- Технологическое оборудование и системы управления

Мониторинг на Zabbix

Сбор данных:

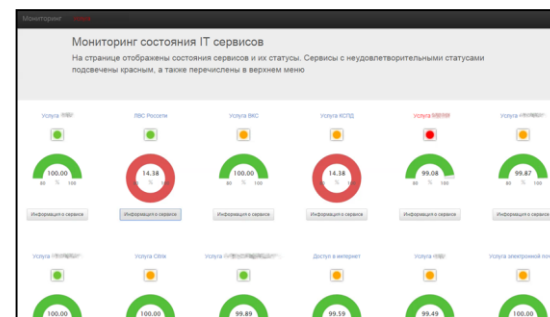
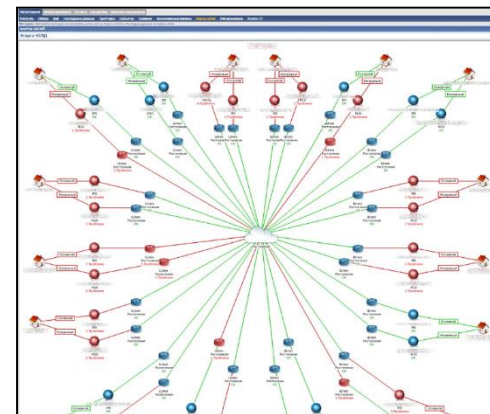
- проверки доступности и производительности
- поддержка мониторинга по SNMP, IPMI, JMX
- пользовательские проверки
- сбор желаемых данных за выборочные интервалы

Широкие возможности визуализации:

- Графики в режиме реального времени
- Карты сети
- Пользовательские экраны и слайд шоу
- Отчеты

Гибкая настройка:

- Определение порогов
- Автоматические реакции на события, в том числе удаленные команды
- Шаблонизация



Dynatrace. Производительность приложений



Мониторинг SAP

SAP

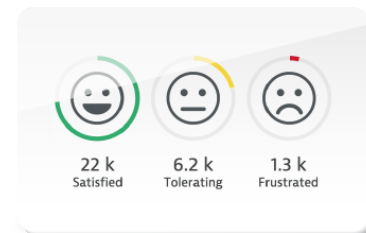
- Мониторинг всех SAP транзакций и пользователей, 24/7
- Автоматическое определение SAP процессов и уникальных имен пользователей
- Глубокая видимость для протокола SAP GUI (DIAG) и шифрованного трафика (SNC)
- Безагентный мониторинг – отсутствие дополнительной нагрузки на сервис
- Отчетность и оповещения в режиме реального времени



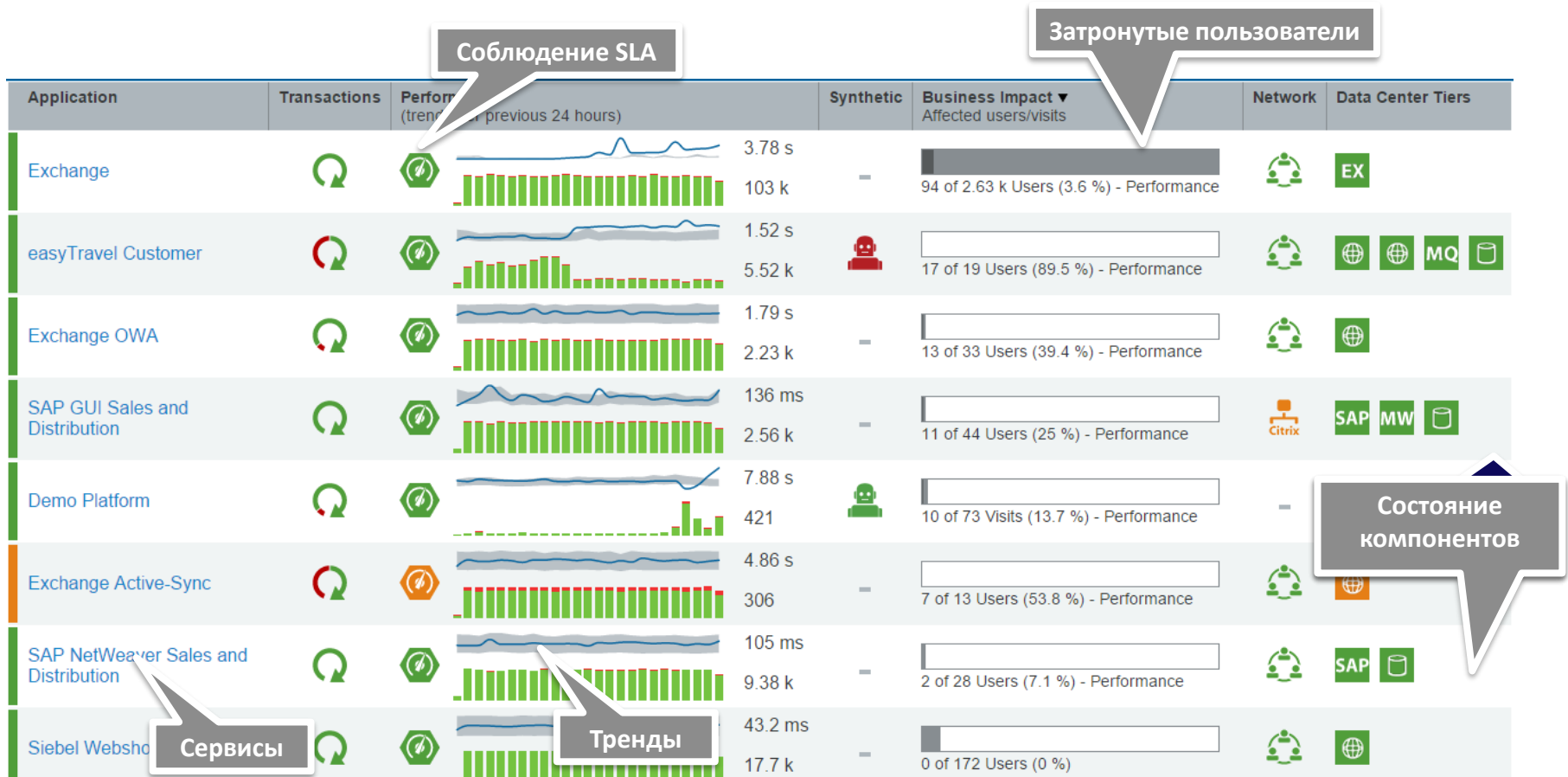
SAP® Certified
Integration with SAP NetWeaver®

Информация для Бизнес пользователей

- Информация о текущей работе сервисов
- Фиксация и контроль SLA
- Детализация функционирования системы с точки зрения пользователей
- Детализация по разным SAP транзакциям:
 - Логин в системе
 - Создание отчета
 - Бухгалтерская выписка
 - Управление персоналом



Пример контрольной панели для Бизнес пользователя



Универсальная платформа vs. Специализированные решения

Универсальная платформа

- + *Унификация поддержки и развития*
- + *Гибкость*
- *Дольше: первичное внедрение, развитие*
- *Дешевле лицензии (?)*

Специализированные решения

- + *Быстрее*
- + *Продвинутые алгоритмы анализа*
- *Дороже (зависит от специализации)*
- *Ограничения кастомизации (интерфейса, логики)*



- 🌿 Нельзя объять необъятное
- 🌿 Унификация интерфейсов вместо унификации решений
- 🌿 Стоимость внедрения системы мониторинга не должна превышать реального эффекта от её использования
 - Снижение простоя сервисов
 - Оптимизация ресурсов
 - Снижение рисков утечки данных
- 🌿 Выбор платформы мониторинга с учетом реальной задачи, а не только стратегических целей



ООО «Унитех»

117312, Москва, ул. Вавилова, д.47А

Тел.: (495) 662-92-91

info@unitechnologies.ru

www.unitechnologies.ru



**УНИВЕРСАЛЬНЫЕ
ТЕХНОЛОГИИ®**