

## Мониторинг ИТ-инфраструктуры банка с помощью решений SolarWinds

**Заказчик:** российский банк (ТОП-100), входящий в международный финансовый холдинг.

**Назначение проекта:** автоматизация процессов мониторинга и регистрации данных о состоянии параметров информационно-телекоммуникационной инфраструктуры, включая формирование уведомлений о ключевых событиях.

### Цели выполнения проекта:

- сокращение времени реакции на события<sup>1</sup>, возникающие в ИТ-инфраструктуре
- своевременное выявление и предотвращение возможных инцидентов<sup>2</sup> и/или проблем<sup>3</sup> в ИТ-инфраструктуре
- повышение наглядности (визуализация) информации о состоянии параметров ИТ-инфраструктуры
- обеспечение возможности ретроспективного анализа состояния параметров ИТ-инфраструктуры

### Средства и системы, подлежащие мониторингу:

- активное сетевое оборудование (коммутаторы, маршрутизаторы, межсетевые экраны Cisco и D-Link, Citrix Access Gateway) – 50 шт.
- системы хранения данных (EMC CLARiON CX3, VNX) – 3 шт.
- серверы, в том числе виртуальные – 120 шт.
- средства виртуализации Wmware – 3 ESXi-кластера
- система телефонии производства Cisco Systems, Inc. – две сети
- периферийные сетевые устройства – 20 шт.

### Приложения (сервисы), подлежащие мониторингу:

- Active Directory 2003/2008 Services and Counters
- Microsoft DNS-сервер, DHCP-сервер, Web-сервер (IIS)
- другие штатные роли и сервисы ОС Microsoft
- Microsoft SQL server 2005/2008
- Lotus Domino Server
- IBM WebSphere
- специализированные прикладные сервисы, обеспечивающих операционную деятельность банка



Application Summary

Application Name	Status
Active Directory 2008 R2 - 2012 Services and Counters	All applications up
Citrix XenApp 6.0 Core counters	All applications up
Citrix XenApp 6.0 ICA Session	All applications up
Citrix XenApp 6.0 Presentation Server	All applications up
Credit Registry	All applications up
Errors in Application Event Log	All applications up
IBM WebSphere (JMX)	All applications up
Informatica	All applications up
Internet Information Service (IIS) Services and Counters	All applications up
Lotus Domino Server Processes and Network Ports (Windows)	All applications up
Microsoft Windows Server 2003 Failover Cluster	All applications up
Microsoft Windows Server 2008 Failover Cluster	All applications up
None	All applications up
SQL Server 2005-2008 Performance (SQL)	All applications up
SQL Server 2005-2008 Performance (WMI)	All applications up
Symantec NetBackup Server	1 application(s) down
Volume Shadow Copy Service Windows Server 2003-2012	All applications up
Windows DNS Server	All applications up
Windows Print Services	All applications up
Windows Remote Desktop Services (Session Host Role)	All applications up
Windows Server 2003-2012 Services and Counters	All applications up
XML Blaster	All applications up

<sup>1</sup> Под событием понимается изменение состояния, которое имеет значение для управления, работоспособности и/или безопасности ИТ-инфраструктуры или ее компонента(ов)

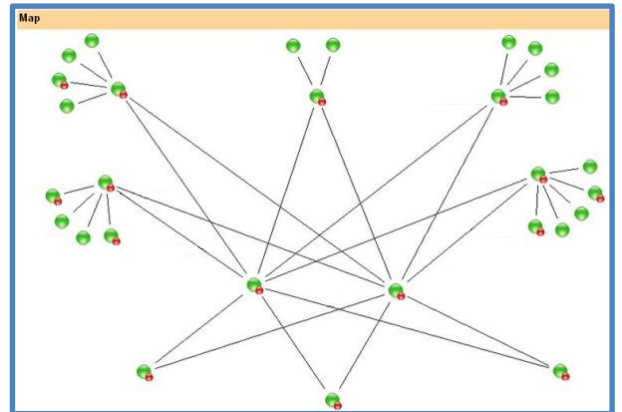
<sup>2</sup> Под инцидентом понимается незапланированное прерывание работы ИТ-инфраструктуры или снижение показателей ее работы или ее компонента(ов)

<sup>3</sup> Под проблемой понимается причина одного или нескольких инцидентов

Стандартами заказчика в качестве средств мониторинга предусмотрено использование решений компании SolarWinds. Реализация проекта поручена «НТЦ Вулкан».

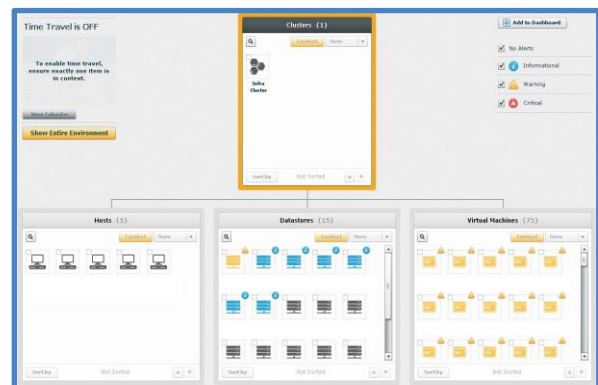
При создании системы использованы следующие продукты SolarWinds:

- Network Performance Monitor
- IP Address Manager
- User Device Tracker
- Server & Application Monitor
- Storage Manager
- Virtualisation Manager
- VoIP & Network Quality Manager



В рамках проекта проведены следующие работы:

- подключение к системе всех объектов мониторинга по протоколу SNMP и с использованием технологии WMI
- формирование карт и схем сети
- разграничение прав доступа к функциям и информации в системе мониторинга
- формирование целевых рабочих областей (Dashboard) для различных подразделений (отдел поддержки оборудования, отдел поддержки приложений, отдел информационной безопасности)
- настройка уведомлений операторов
- настройка формирования отчетов по расписанию
- подготовка проектной и эксплуатационной документации<sup>4</sup>



В результате внедрения системы мониторинга заказчик получил:

- ускорение времени реакции на события в ИТ-инфраструктуре, в том числе идентификация и разрешение ряда инцидентов до начала их влияния на работу пользователей
- заблаговременное выявление возможных проблем в ИТ-инфраструктуре, в том числе выявление некорректных конфигураций на активном сетевом и серверном оборудовании
- отображение основных параметров состояния ИТ-инфраструктуры на единой консоли, а также формирование целевых консолей для ключевых специалистов ИТ-департамента
- оперативное информирование ключевых специалистов ИТ-департамента о состоянии критичных ИТ-систем и сервисов

<sup>4</sup> Разработка документации на систему выполнена в соответствии с требованиями ГОСТ «Информационная технология. Комплекс стандартов на автоматизированные системы» и комплекса СТО БР ИББС.