Создание централизованной системы сбора и обработки событийной информации ИТ-инфраструктуры ЗАО «Энергопром Менеджмент»

Предпосылки и задачи проекта

Компания «ЭНЕРГОПРОМ МЕНЕДЖМЕНТ» - одна из наиболее эффективных компаний несырьевого сектора российской экономики. Под управлением компании находятся три электродных завода: Новочеркасский, Новосибирский и Челябинский, производящие высокотехнологичную электродную и катодную продукцию, основными потребителями которой являются производители стали, алюминия, кремния и ферросплавов. Все предприятия компании оснащены современным высокопроизводительным оборудованием. Ряд производимых на заводах видов продукции и применяемых технологий не имеют аналогов в мире. С целью повышения конкурентоспособности на заводах компании осуществляется комплексная модернизация и реконструкция мощностей, ведется строительство новых мощностей по выпуску перспективных видов продукции, способных удовлетворять потребности металлургических предприятий, использующих новейшие способы производства металлов, а также растущий мировой спрос на углеграфитовую продукцию. ЗАО «Энергопром Менеджмент» имеет территориально-распределенную ИТ-инфраструктуру, которая обслуживается ИТ-специалистами центрального и локальных офисов. При этом контроль работоспособности элементов инфраструктуры и своевременное устранение неисправностей затруднены, что снижает устойчивость работы критичных для бизнеса приложений. Анализ текущей ситуации и требование повышения доступности критичных бизнес-приложений привели к принятию решения о необходимости создания централизованной системы сбора и обработки событийной информации ИТ-инфраструктуры (Системы).

Описание решения

Для построения Системы необходимо было решить задачи:

- мониторинга информационных ресурсов компании;
- мониторинга сетевого оборудования;
- консолидации событийной информации в единой точке;
- создания интерфейса для работы с событиями о состоянии информационных ресурсов и сетевого оборудования;
- автоматического оповещение персонала о критичных событиях в ИТ-инфраструктуре;

Централизованная система сбора и обработки событий ИТ-инфраструктуры была построена по модульному принципу. Центральным элементом архитектуры является сервер обработки событийной информации (IBM Tivoli Enterprise Console Event Server). Источниками событийной информации для этого звена являются адаптеры (IBM Tivoli Enterprise Console Event Adapters), предназначенные для сбора событийной информации и сервер сетевого мониторинга (IBM Tivoli NetView Server).

Единая точка представления информации, в которой консолидируются события о состоянии компонентов ИТ-инфраструктуры, была создана на базе программного продукта IBM Tivoli Enterprise Console. Для мониторинга информационных ресурсов были использованы адаптеры IBM Tivoli Enterprise Console, позволяющие собирать информацию из журнальных файлов операционных систем. В связи с тем, что на серверных операционных системах проводится подробный аудит системных событий, событий безопасности и событий приложений, были разработаны алгоритмы фильтрации событийной информации, позволяющие снизить информационную нагрузку на операторов системы. В дальнейшем разработанные алгоритмы были применены ко всем серверным операционным системам ИТ-инфраструктуры.

Для мониторинга доступности сетевого оборудования был использован программный продукт IBM Tivoli NetView, позволяющий строить карту сетевой топологии второго уровня модели OSI и оперативно отслеживать важные характеристики производительности сетевого оборудования. В рамках проекта была создана логическая карта сетевой топологии, отображающая различные типы ресурсов сетевой инфраструктуры и их статус. Работа со всем сетевым оборудованием и серверами ведется по протоколу SNMP, что позволяет в режиме реального времени снимать важные характеристики функционирования и использовать инструменты диагностики неполадок. Доступ ИТ-специалистов к системе сетевого мониторинга осуществляется через web-интерфейс. При этом представление информации для каждого конкретного пользователя зависит от его зоны ответственности.

Настройка доступа к системе сетевого мониторинга через web-интерфейс, совместно с дифференциацией пользователей по правам и зонам ответственности позволила предоставить интерфейс подсистемы сетевого мониторинга ответственному персоналу подразделений компании. Интеграция с почтовой системой и SMS-шлюзом позволила расширить функциональность Системы. Сотрудники ИТ-отдела ЗАО «Энергопром Менеджмент» получают оповещения о критичных проблемах в ИТ-инфраструктуре по электронной почте и в виде SMS-сообщения, что позволяет оперативно реагировать на сбои и отклонения в работе ИТ-инфраструктуры.

Результаты

В настоящее время информация о проблемах функционирования всех информационных ресурсов компании представлена в единой точке, сотрудники своевременно получают оповещения о неполадках в работе компонентов ИТ-инфраструктуры. Консолидация и корреляция информации позволяет отсеивать симптоматические сообщения о проблемах и выявлять корневую причину неполадок. Созданная карта сетевой топологии позволяет диагностировать проблемы на уровне сетевой инфраструктуры.

За счет использования инструментов централизованной системы сбора и обработки событийной информации

- повышена доступность критичных бизнес-приложений;
- сокращена длительность обнаружения и устранения неисправностей;
- сбор исторической информации о событиях позволил обоснованно принимать решения о внесении изменений в ИТ-инфраструктуру;
- повышено качество поддержки ИТ-персонала удаленных подразделений из центра;
- автоматического оповещение персонала о критичных событиях в ИТ-инфраструктуре;

По материалам сайта: http://www.tivoli.computel.ru/projects/projects/content/energoprom_case