МОДУЛЬНАЯ СИСТЕМА ТРАБЛШУТИНГА СЕТИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Станевич М.А.
Макейчик Е.Г. – м.т.н.,старший преподаватель

На сегодняшний день практически все крупные компании сталкиваются с необходимостью контролировать инфраструктуру, обеспечивающую экономическую эффективность бизнеса.

Операторам отдела сервисного и операционного контроля необходима система для быстрого выявления и локализации аварий на сети, способная взаимодействовать с разными топологиями и типами сетей.

Решением стало начало постепенного наращивания функциональности утилит, добавления возможности корреляции, выявления и обогащения информации, анализа статистических данных: вплоть до выявления неизвестных проблем, возможности автономного траблшутинга и выяснения степени влияния ИТ-метрик на бизнес-метрики.

OSS (Operation Support System) – модульная система мониторинга, основанная на концепции управления системами связи (Telecommunication Management Networks – TMN).

По специализации системы управления и мониторинга можно разделить на три вида:

– низкоуровневые;

– зонтичные;

– унитарные.

Низкоуровневые системы предназначены обычно для управления оборудованием конкретного производителя или оборудованием определенного класса, например: оборудованием первичных сетей, телефонными станциями, оборудованием вторичных сетей и пр. Специализированные системы управления для своего оборудования производят такие компании как Ciena, Cisco, Keymile и другие.

Зонтичные системы Manager Of Managers, Orchestrators собирают данные от низкоуровневых систем, которые, в свою очередь, выполняют задачи управления и мониторинга отдельных частей инфраструктуры. По сути низкоуровневые системы становятся информационными агентами для зонтичной системы. Зонтичная система производит анализ всей поступающей информации с целью корреляции событий, траблшутинга, аварий, поиска первопричин сбоев, прогнозирования наступления нештатных ситуаций и т.д. Сетевые и системные администраторы в этом случае получают единую точку контроля состояния инфраструктуры и бизнес приложений, единую точку генерации отчетности. Ограничением для зонтичных систем зачастую становится невозможность управления элементами ИТ инфраструктуры, поскольку далеко не все низкоуровневые системы способны принимать к исполнению команды от вышестоящего программного обеспечения.[2]

Траблшутинг (англ. troubleshooting – устранение неполадок, работа над траблом) – форма решения проблем, часто применяемая к ремонту не работающих устройств или процессов. Представляет собой систематический, опосредованный определённой логикой поиск источника проблемы с целью её решения. Траблшутинг как поиск и устранение неисправностей необходим для поддержания и развития сложных систем (встречающихся, например, в таких областях, как связь, инженерия, системное администрирование, электроника, ремонт автомобилей, диагностическая медицина и организация бизнес процессов), где проблема может иметь множество различных причин.

В основные возможности зонтичного решения мониторинга сети входят:

1 Мониторинг опциональной сигнализации оборудования.[1]

2 Инвентаризацию сетевого и серверного оборудования.

3 Определение или расчет KPI (Key Performance Indicators): формулы для определения и анализа «эффективности» того или иного параметра сети.

4 Конфигурирование оборудования

5 Выдача рекомендаций по устранению неисправностей

Основной недостаток Зонтичных систем – стоимость такого решения. Высокая цена обусловлена несколькими недостатками:

1 Кастомизация решения. Как правило продукт из коробки не может быть интегрирован в большую инфраструктуру компании без дополнительной настройки. Некоторые сегменты сети не имеют базы данных с информацией о составе и количестве элементов в нем. В таких случаях ввод данных в систему мониторинга производится вручную. А при изменении структуры сети или адреса сетевого элемента, изменение информации так же будет производиться вручную

2 Статичность интеграции. Все системы, которые интегрируются в OSS, как правило со временем модернизируются, меняются вендоры, соответственно, и ПО. Поэтому будет изменяться тип коммуникации серверов с системой мониторинга, тип базы данных, для его считывания.

Список использованных источников:

1. АДВ [Электронный ресурс]. – Режим доступа : http://www.advc.ru/solutions/sistemi_upravlenija_i_monitoringa.html

2. NetCracker Technology® [Электронный ресурс] : Datasheet / NetCracker Technology. – Режим доступа : NetCracker Velcom CRIM project SOW.pdf.