Nagios был разработан для Linux, но теперь способен отслеживать операционные системы на базе UNIX. Он состоит из трех компонентов: демона, веб-интерфейса и плагинов. Nagios имеет четыре основных типа объектов, которые перечислены ниже.

* Команды: они используются для взаимодействия с плагинами и для управления обработчиками событий, уведомлениями и проверками.
* Контактные и контактные группы: они определяют лиц, с которыми необходимо связаться в случае события.
* Группы хостов и хостов: они используются для указания служб и хостов в определенной сети.
* Уведомления. Они определяют, какой контент должен быть отправлен контактам и контактным группам, когда обнаружены.

Определения проверки хоста и службы определяют, какие плагины вызывать для получения статуса хоста или службы. Определения в плагинах проверяются на этом конкретном хосте / службе. Если видно, что значения выходят за порог, Nagios уведомляет контакты / контактные группы. Nagios возвращает любой из следующих четырех кодов статуса для любого события:

1. OK
2. Предупреждение
3. Критический
4. Неизвестно

Nagios можно настроить для проведения пассивных или активных проверок. В активных проверках хост, который так часто запускает устройства или службы Nagios для получения информации о статусе, тогда как пассивные проверки инициируются и выполняются внешними приложениями / процессами. Затем результаты отправляются на хост мониторинга (где работает Nagios) для обработки. Основное различие между активными и пассивными проверками заключается в том, что активные проверки инициируются и выполняются Nagios, в то время как пассивные проверки выполняются внешними приложениями. Пассивные проверки могут использоваться для мониторинга асинхронных служб и мониторинга служб, расположенных за брандмауэром. Активные проверки могут использоваться для проверки по требованию и регулярных проверок интервалов. Результаты могут контролироваться через веб-интерфейс, основанный на CGI.

Используя Nagios, возможно:

* Планирование обновления инфраструктуры до того, как устаревшие системы вызывают сбои
* Отвечать на вопросы при первом признаке проблемы
* Автоматическое исправление проблем при обнаружении
* Согласовать ответы технической команды
* Обеспечьте соблюдение SLA вашей организации
* Обеспечить минимальные последствия для ИТ-инфраструктур на нижней строке вашей организации
* Мониторинг всей инфраструктуры и бизнес-процессов