

Основы администрирования сетевых устройств

Лекция 4 — Удаленное
администрирование. Протоколы и
мониторинг.

- В современном мире телекоммуникаций для обеспечения бесперебойной работы сетевых устройств недостаточно хорошо выполнить только первоначальную настройку;
- Существует множество дополнительных требований и методов их исполнения для сетевых устройств находящихся в эксплуатации.

- Часто требуется организовать **удаленный доступ** – способ получения доступа к устройству (веб-конфигуратор и/или консоль) без непосредственного физического доступа;
- Удаленный доступ может применяться для работы с большим количеством устройств распределенных территориально. Также применяется в аварийных ситуациях для оперативного подключения или оказания помощи неквалифицированным клиентам.

- Понятие «удаленного доступа» часто имеет несколько значений. По факту это разрешение правил управляемого устройства для обмена пакетами целевого протокола. Например для удаленного консольного доступа потребуется разрешить на устройстве протоколы **TELNET** (23 порт, незащищенный протокол) и/или **SSH**(22 порт, использует шифрование). Для доступа к веб-интерфейсу соответственно **HTTP(S)** (80(443) порты). Часто стандартное значение портов можно изменить;
- Также нужно помнить, что протокол и порты с которыми ведется обмен должны быть свободно пропущены на всем участке от ПК до устройства.

- Для обеспечения **надежности** сети, важно, чтобы устройства работали бесперебойно на максимальном временном промежутке. Данная теория также рассматривает очень важные вопросы резервирования устройств, повышающее значение коэффициента готовности;
- Однако, в данном курсе мы рассматриваем как своевременно обнаружить неисправность и вовремя ее устранить.

- Для обнаружения **неисправностей** (некорректная работа оборудования, не заявленные функции, и т.д.) применяются автоматизированные методы считывания текущих параметров системы – мониторинг, т.е. непрерывный процесс отслеживания состояния устройства, узлов или сети в целом;
- Применяемые вендором средства мониторинга часто позволяют отслеживать только параметры одного устройства (исключение крупные вендоры со своими системами мониторинга).

- На сетях связи имеющих в наличии большое количество оборудования разных производителей применяются системы мониторинга, такие как: Zabbix, Nagios, Cacti и др. Они разделяются на платные коммерческие продукты и бесплатные для скачивания. Однако часто даже бесплатные СМ требует больших вложений человеко-часов и мощные сервера для развертывания (в зависимости от размеров сети);
- Проверка доступности устройства происходит с заданным периодом, для этого могут быть использованы простейшие утилиты (пр. Ping) так и специализированные протоколы мониторинга и управления.

- Наиболее распространенным является протокол **SNMP** (англ. Simple Network Management Protocol);
- Данный протокол позволяет осуществлять мониторинг состояния и наличие аварий на устройстве, а также управлять некоторыми устройствами. Т.к. **SNMP** анализирует данные только на устройстве, то для сетевых устройств, где требуется анализ взаимодействия (трафика) между устройствами часто используется **RMON** (англ. Remote Monitoring) как расширение SNMP.

- При работе с протоколом SNMP используются понятия **Агент** (устанавливается на управляемые устройства, отслеживает состояние) и **Менеджер** (чаще устанавливается на системы мониторинга и управления, взаимодействует с агентами и другими менеджерами);
- Существует SNMP версий v1, v2, v3. Для первых двух версий для идентификации хостов применяются следующие поля: Contact, Location, Read community, Write community, Trap community

- Поля `community` у Агента и Менеджера должны совпадать, например по умолчанию для чтения указывается – **public**, для записи – **private**, а для сообщений **trap** – либо **trap** либо **private**.
- Сообщения **Trap** особый асинхронный тип сообщений часто передаваемых от Агента к Менеджеру при непосредственном возникновении событий на устройстве (аварий) а не только в момент опроса устройства со стороны Менеджера. Также SNMP обмен можно часто идентифицировать на портах 161 и 162.

Удаленное администрирование. Протоколы и мониторинг

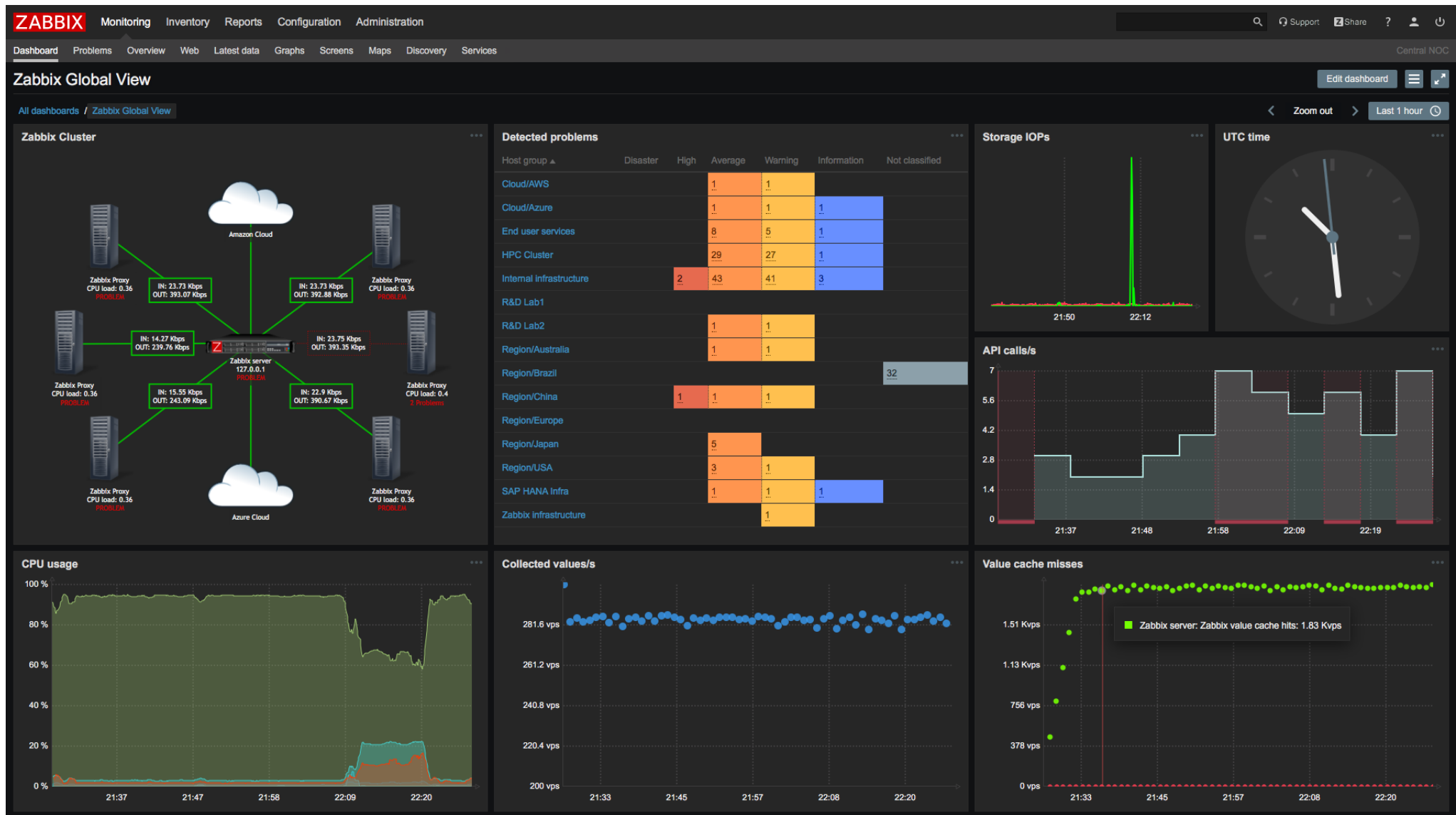


Рис. 1 Внешний вид панели управления и мониторинга Zabbix (zabbix.com)

- Для работы протокола **SNMP** необходима его поддержка на устройстве, т.е. наличие базы MIB позволяющей сопоставлять название в читаемом виде с т.н. OID – идентификатором объекта, который записывается в формате 1.3.6.1.2.1.1.5
- Часто производители оборудования предлагают собственные системы мониторинга и управления с уже предустановленными базами MIB.

- Список литературы:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов 4-е изд. — СПб.: Питер, 2010. — 944 с.: ил
2. Гольдштейн Б.С. Протоколы сети доступа. Том 2. 3..е изд. — СПб.: БХВ – Санкт..Петербург, 2005.
3. Xgu.ru [Электронный ресурс] Протокол SNMP URL: <http://xgu.ru/wiki/SNMP> (дата обращения 1.09.19)

- **Материалы для самостоятельной подготовки:**

Тема	Источник
Удаленный доступ, протоколы	[1, с. 760-767]
Краткое описание протокола SNMP	[3]

Спасибо за внимание!

Лекция 4 — «Удаленное администрирование.
Протоколы и мониторинг»
Версия документа 1.0
Стенин А.В.
av.stenin@yandex.ru