NON-INTRUSIVE REMOTE MONITORING OF SERVICES IN A DATA CENTRE

Hemanta Kumar Kalita, Manoj K. Nambiar, and Amol Khanapurkar

Tata Consultancy Services Ltd
TCS Innovation Lab–Performance Engineering, Mumbai
Akruti Business Port, Gateway Park
MIDC, Road No 13, Andheri(E)–400093
{h.kalita, m.nambiar, amol.khanapurkar}@tcs.com

ABSTRACT

Non-intrusive remote monitoring of data centre services should be such that it does not require (or minimal) modification of legacy code and standard practices. Also, allowing third party agent to sit on every server in a data centre is a risk from security perspective. Hence, use of standard such as SNMPv3 is advocated in this kind of environment. There are many tools (open source or commercial) available which uses SNMP; but we observe that most of the tools do not have an essential feature for auto-discovery of network. In this paper we present an algorithm for remote monitoring of services in a data centre. The algorithm has two stages: 1) auto discovery of network topology and 2) data collection from remote machine. Further, we compare SNMP with WBEM and identify some other options for remote monitoring of services and their advantages and disadvantages.

KEYWORDS

DES, AES, ARP, SNMP, MIB, DNS, ICMP, WBEM

1. INTRODUCTION

A Data Centre is a facility for housing computer systems such as web servers and associated components, for example, dedicated Internet connection, security, support and regulated power. Since a data centre houses many servers involving business critical operations hence, 24x 7 service availability is a high priority requirement in this scenario. In order to keep the services available 24x 7 the support team in a data centre need to monitor health of each and every server periodically. Manual and local observation is a time taking painful job, where a support team member needs to go to each and every server physically and look at the status. This is where the need of remote monitoring of services arises. In the case of remote monitoring of services, a user can monitor service availability of each and every server in a data centre from a single machine and locate the erring server for necessary action. However, remote monitoring and controlling of data centre services has some challenges. One of the biggest challenges is security. Is it possible to remotely monitor and control data centre services in a non-intrusive way? In this paper we investigate this problem.

Remainder of the paper is divided into four sections. We identify and categorize some of the available open source and commercial tools for remote monitoring of services in Section 2. In

D.C. Wyld, et al. (Eds): CCSEA 2011, CS & IT 02, pp. 10–16, 2011.
 DOI : 10.5121/csit.2011.1202

Section 3 we propose an algorithm to monitor data centre services remotely. In Section 4 we give analysis and finally in Section 5 we conclude the paper.

2. BACKGROUND

SNMP based solution is non-intrusive provided inclusion of the framework minimize modifications to any existing legacy code or standard practices. Furthermore, a local user should not be able to perceive that local resources are being stolen for foreign computations [1].

Simple Network Management Protocol, or SNMP, is the standard operations and maintenance protocol for the Internet. SNMP is used to administer and manage networked devices. It can be used to manage large networks that span firewalls and embedded devices. The SNMP protocol came into existence in the late 1980s due to the requirement of having to manage ever growing networks, and the need to verify certain conditions being experienced on those networks. Most of the protocols seen in the TCP/IP suite follow the client/server model. SNMP protocol is no different except for a minor syntax distinction; it follows the client/manager model [14].

Currently there are three versions of SNMP. They are–SNMPv1, SNMPv2 and SNMPv3. SNMPv3 is the IETF recommended standard. SNMPv3 provides a security and administrative framework to the protocol which allows for the addition of new security mechanisms. For example, triple-DES and AES can be used for SNMPv3 privacy [2]. In Table 1 we highlight some of the SNMP characteristics. Net-SNMP [15] is a suite of applications used to implement SNMPv1, SNMP v2c and SNMP v3 using both IPv4 and IPv6. The suite includes command line applications to retrieve information from SNMP enabled device, either using single requests (snmpget, snmpgetnext) or multiple requests (snmpwalk, snmptable, snmpdelta). The application suite also includes a graphical MIB browser, a daemon application for receiving SNMP notifications (snmptrapd), etc. For using NET-SNMP one needs to configure *snmpd.con*f and specify the community in the server where snmpd is running so that one can read all the MIBs from a remote client.

Table 1 SNMP Characteristics

Easy setup
SNMP traffic can't be filtered
SNMP filters BW usage by port
Monitor network parameter other than bandwidth usage

Version 3 of the SNMP protocol introduced a User-based Security Model (USM) which comes with its own user and key-management infrastructure. However, many operators are reluctant to introduce a new user and key management infrastructure just to secure SNMP. [5] describes how the Secure Shell (SSH) protocol can be used to secure SNMP.

We divide the existing tools known so far into two categories: open source and commercial. In open source there are tools like Nagios[6], Open-Audit[12], Net-SNMP[15], Cacti[3], ZenOss[17], OpenNMS[13], Net-Disco[8], NeDi[7] and NMAP[11]. Tools such as NetworkView[10], NetFlow[9], and DopplerVUE[4] are commercial network monitoring tools.

3. DESIGNING ALGORITHM

Designing algorithm for remote monitoring services involves discovering active services in the remote servers inside a data centre. Further it may collect information such as open ports and usage of resources in the remote computer. We categorize the requirements of designing an

algorithm for remote monitoring services as: auto-discovery of network topology and data collection from remote machine.

3.1 Auto-discovery of Network Topology

The proposed algorithm should automatically discover the network. We observe that most of the tools discussed in the previous section do not have this feature. NetDisco does this if remote machine supports protocol such as Cisco Discovery Protocol, Link Layer Discovery Protocol, Foundry Discovery Protocol or SynOptics Network Management Protocol. The challenges to this requirement are

- Protocols such as Cisco Discovery Protocol, Link Layer Discovery Protocol, Foundry Discovery Protocol or SynOptics Network Management Protocol are not common.
- We need an algorithm which requires minimal configuration or enabler in the remote machine. Also, it should be non-intrusive in nature.

The input or requirements to the algorithm designed for auto discovery of network topology are

- Remote machines are enabled with SNMP
- IP address of at least one gateway router in the enterprise
- Boundary information, i.e., one or multiple range of IP address(es)
- One or multiple community string(s)
- SNMP port number and database credentials

And, subsequently output from the algorithm is a topology map of the network.

To discover devices the device discovery algorithm uses a routing table, an ARP cache table, and ICMP utilities. For each discovered device, it verifies SNMP support and then discovers the device type, such as router, L2, L3, L4 or L7 switches, printers, or network terminal nodes. Depending on the type of device, the relevant MIB information is retrieved from SNMP agents.

Discovering network topology around L3 device. A routing table of the device is maintained by the *ipRouteTable* object. The *ipRouteTable* object contains an entry for each route presently known to this entity in *ipRouteEntry*. We utilize only *ipRouteNextHop* and *ipRouteType* entries for these tables. *ipRouteNextHop* is the IP address of the next hop in the route. *ipRouteType* can be one of four types: direct, indirect, invalid, or other. The ‘type direct’ refers to the same device, having multiple IP addresses. The entries of types direct, invalid or other are discarded. The records are filtered and taken only those entries that are of type indirect.

Discovering topology of the network around L2 device. To discover end hosts and L2 devices, we rely on *ipNetToMediaTable*, an IP address translation table. For resolving IP address to MAC address mapping, ARP protocol is used. To make this resolution work faster, the router maintains an ARP cache that contains the MAC to IP mapping of the active devices in the network. As soon as we discover a node, we use all unique *ipNetToMediaNetAddress* entries to discover another set of new nodes. One device can help in discovering more devices, and the algorithm comprises a recursive process.

In Algorithm 1 algorithm for auto-discovery of network topology is described.

3.2 Data collection from remote machine

Once the network is discovered the next step is rather simple. One needs to get the information such as reach-ability, services running, open port, resource utilization etc from each remote machine to the host machine. For this requirement available options are using Ping, Traceroute, DNS, ARP, SNMP etc. The challenges to this requirement are

- Configuring remote machine. For example, enabling SNMP.
- Continuous monitoring needs handling of huge volume of data.
- Presentation/Visualization of data. Evaluated tools does give lots of information; but not necessarily useful. Extracting/Mining meaningful information from the set of available data is an important task.

The advantages of SNMP are SNMP is simple, easy to implement, secure and non-intrusive. However, drawback is SNMP is required to be installed in all network elements.

```
01 Visited device set ← Set of routers already visited,
   initially empty;
   // Next hop discovery (Router IP address)
02 repeat
03   if router is not in visited device set then
04        Get all unique next hops of router through
          ipRouteNextHop, where ipRouteType is indirect;
05   if there is no ipRouteNextHop then
06        return;
07 until ipRouterNextHop is NULL;
   // ARP cache discovery (IP address)
08 repeat
09   if IP address is not in the visited device set
     then
10        Get all the unique ipNetToMediaNetAddress;
11   if there is no ipNetToMediaNetAddress then
12        return
13 until ipNetToMediaNetAddress is NULL;
```

Algorithm 1 Auto discovery of Network Topology

4. ANALYSIS

In the previous section we propose an algorithm for remote monitoring of services in a data centre based on SNMP protocol. The algorithm has two stages: auto discovery of network topologies and data collection from remote machine for remote monitoring of services. In this section we compare SNMP based approach with WBEM. Also, there are some other options available for auto discovery of network topologies and remote monitoring of services. For example, TCP/UDP Scan, Zone Transfer from a DNS Server, Active probing using PING Scan, ARP Scan, Traceroute, Passive Monitoring etc. We analyze these options too.

4.1 WBEM vs SNMP

As observed each approach has advantages and disadvantages. Web-Based Enterprise Management (WBEM) provides the ability for the industry to deliver a well-integrated set of standard-based management tools, facilitating the exchange of data across otherwise disparate technologies and platforms. The DMTF has developed a core set of standards that make up

Table 2 SNMP vs WBEM

SNMP	WBEM
Simple Network Management Protocol	Web-based Enterprise Management. The current version of WBEM in Windows is called WMI (Windows Management Instrumentation)
Old	Relatively Newer than SNMP
SNMP can't use WBEM	Compatible to SNMP
SNMP Client/Server (snmpd, MIBs)	WBEM Client/Server (CIMOM,WBEM provider)
Backed by IETF (Internet Engineering Task Force)	Backed by DMTF (Distributed Management Task Force)
A variety of Security options can be set in SNMPv3	No extra security; whatever HTTP has for security can be applied
SNMP over TCP-IP/UDP-IP	WBEM includes CIM as the data definition, XML as the transport/ encoding method and HTTP as the access mechanism
Simple	Not simple
SNMPv1 and v2c sends messages over unencrypted UDP datagram on ports 161 and 162. SNMPv3 has security features: MD5,SHA for authentication, DES for encryption	WBEM in itself does not offer any specific security features. WBEM sends messages over HTTP encrypted using SSL on TCP port 5989
SNMP proponents disagree that management object files - a basic building block for CIM - are more object-oriented than Management Information Bases in SNMP	CIM's object-oriented approach makes it easier to track the relationships and interdependencies between managed objects
SNMP is firmly entrenched in terms of network devices	WBEM can't beat SNMP in managing network devices
SNMP is not dependent on vendor's support	CIM's future is highly dependent on how many vendors actually implement it, how quickly, and at what level of support. Also important is whether vendors implement products as a giver of information or as a taker only

WBEM, which includes the Common Information Model (CIM), CIM-XML, CIM Query Language, WBEM Discovery using Service Location Protocol (SLP) and WBEM Universal

Resource Identifier (URI) mapping [16]. Key features of WBEM technology include: remote management of applications, management of several instances of an application as a single unit, standard interface for remote application management across different applications, decoupling of application management from the client, "publishing" of key information about an application to other applications. In Table 2 we compare SNMP based approach with WBEM.

4.2 Other Methodology

In this section we highlight some options (other than SNMP) for auto discovery and monitoring of network and discuss their advantages and disadvantages.

TCP/UDP Scan. This approach searches for open ports, identify public service being executed on a remote host. If a response is received from a remote device then we can safely identify them as active. Since the results can be affected by firewalls and countermeasures from host, each address is supposed to be scanned by probing all the ports mentioned below: 21 (FTP), 22 (SSH), 23 (TELNET), 80 (WWW), 135 (DCOM Service Control Manager), 161 (SNMP), and 445 (Microsoft Directory Services). *Advantag*e of this technique is it is efficient for discovering remote server. *Drawbac*k is slow as it needs to hit on the ports one after the other if the response is not positive and hence has high overhead.

Zone Transfer from a DNS Server. Most DNS server responds to a zone transfer command by returning a list of every name in the domain. Thus, we can find all hosts and routers within a domain. *Advantag*e of this technique is it has low overhead, fast and accurate. However, *drawbac*k is the Network manager frequently disables DNS zone transfer due to security reasons.

Active probing using PING Scan. One needs to send ICMP echo request packets sequentially to every IP address on the network, relying on the response of each active device with an ICMP echo reply. *Advantag*e of PING scan is low overhead and fast. *Drawbac*k is ICMP echo reply can be blocked. Both firewalls and IDSs can be configured for detecting and hence blocking sequential PINGs.

ARP Scan. Send a chain of broadcast ARP packets to the local network segment and increment the destination IP address of each packet. *Advantage*: since every network equipment must answer when its IP address is mentioned on a broadcast ARP, this technique is failure-proof. Also, this technique is difficult to be blocked. *Drawback*: it only works for the current local sub net and is easily detected by sniffers and IDSs.

Traceroute. Traceroute discovers the route between a probe point and a destination host by sending packets with progressively increasing TTLs. On seeing a packet with zero TTL, routers along the path send ICMP TTL-expired replies to the sender, which makes this to discover the path. *Advantage*: Traceroute is usually accurate because all routers are required to send the TTL-expired ICMP message. *Drawback*: some network administrators are known to hide their routers from traceroute by manipulating these replies to collapse their internal topology. Also overheads are more than PING as two probes are sent to every router along the path and time to complete a traceroute is much longer than a Ping.

Passive Monitoring. Employ sniffers that capture all network traffic. *Advantage*: passive monitoring is useful to identify network elements that do not react to any of the previous techniques. *Drawback*: it depends on existence of network traffic. It also needs to know the local network address range for filtering out unnecessary sniffed packet.

5. CONCLUSIONS

In this paper we have discussed our approach to non-intrusive monitoring of data centre services using SNMP based solution. Our approach is divided into two stages: 1) auto discovery of network topology, to know the number of systems in the data centre that are in running state. 2) Once a remote system is known (or discovered), its various parameters including services are

collected. We also mention various open source and commercial tools present in this category and conclude that *auto-discover*y part is missing from most of these tools. Further we compare SNMP based approach with WBEM based approach and analyse some other options that can be utilized for remote monitoring of services. Implementation of our proposed approach is the next step.

REFERENCES

[1] Batheja, J., Parashar, M.: A framework for opportunistic cluster computing using javaspaces. In: HPCN. Electrical and Computer Engineering, Rutgers University (2001)

[2] Bibbs, E., Matt, B.: Comparison of snmp. Tech. rep., ICTN 4600-001 (2006)

[3] Cacti: The complete rrd based graphic solution (2011), "http://www.cacti.net/"

[4] dopplerVUE: Business class network management (2011), "http://www. kratosnetworks.com/products/dopplervue/"

[5] Marinov, V., Schnwlder, J.: Performance analysis of snmp over ssh. In: State, R., van der Meer, S., OSullivan, D., Pfeifer, T. (eds.) Large Scale Management of Distributed Systems, Lecture Notes in Computer Science, vol. 4269, pp. 25–36. Springer Berlin / Heidelberg (2006), "http://dx.doi.org/10.1007/11907466_3"

[6] Nagios: The industry standard in it infrastructure monitoring (2011), "http:// www.nagios.org/"

[7] NEDI: Network management suite (2011), "http://www.nedi.ch/about"

[8] NETDISCO: Network management tool (2011), "http://www.netdisco.org/"

[9] NetFlow: Cisco ios netflow (2011), "http://www.cisco.com/en/US/products/ ps6601/"

[10] NetworkView: Discovery and monitoring (2011), "http://www.networkview.com/ "

[11] NMAP: Network mapper (2011), "http://nmap.org/"

[12] OpenAudit: Open-audit (2011), "http://www.open-audit.org/"

[13] openNMS: Open source, enterprise grade network management application platform (2011), "http://www.opennms.org/"

[14] Parker, D.: Understanding the snmp protocol (2005), "http://www. windowsnetworking.com/"

[15] University, C.M.: Net snmp (1992), "http://www.net-snmp.org/"

[16] WBEM: Web-based enterprise management (2011), "http://www.dmtf.org/ standards/wbem"

[17] Zenoss: Unified network management (2011), "http://www.zenoss.com/product/ network"