Using Visualization Techniques for SNMP Traffic

Analyses

Ewerton Monteiro Salvador, Lisandro Zambenedetti Granville

Federal University of Rio Grande do Sul

Institute of Informatics

 Pengelolaan jaringan saat ini sedang menangani dengan sejumlah besar informasi. Misalnya, dengan skala besar dan jaringan berkecepatan tinggi, perangkat heterogen, dan sistem pemantauan dan notifikasi. Administrator jaringan sering didukung oleh informasi Teknik visualisasi dalam tugas menganalisis data set besar. Protokol Manajemen Jaringan Sederhana (SNMP) adalah standar de facto untuk pengelolaan jaringan TCP / IP. Meskipun demikian Penting, tidak ada visualisasi spesifik yang didefinisikan untuk SNMP. Secara umum Visualisasi jaringan yang ada saat ini tidak tersedia cocok untuk observasi SNMP. Teknik usulkan Telah dibuat prototip dalam perangkat lunak yang disebut Manajemen Lalu Lintas Analyzer, yang telah digunakan untuk menganalisa dan memvisualisasikan SNMP. Saat ini, admin jaringan dan operator mengandalkan sistem manajemen yang kompleks untuk mendukung proses manajemen. Sistem ini dapat menghitung sejumlah besar informasi tentang operasi jaringan, mengatur ulang dan menganalisisnya, dan menyajikan informasi tersebut ke operator jaringan, untuk membantu dia dalam mengelola keseluruhan jaringan. Karena itu, area pengelolaan jaringan semakin banyak dengan jumlah informasi yang besar .

 Informasi visualisasi, bertujuan untuk mendukung penemuan dan analisis data melalui

eksplorasi visual. Penggunaan teknik visualisasi memungkinkan orang untuk menggunakan sifat-sifat sistem visual manusia untuk mengeksplorasi dan memiliki wawasan tentang kumpulan data, mengenali pola, anomali, lebih cepat dan lebih efektif. Teknik visualisasi terdiri dari representasi visual dan, biasanya, mekanisme interaksi yang terkait dengan representasi visual didasarkan pada bentuk pemetaan atribut struktur data abstrak untuk atribut visual. Fitur penting dari Management Traffic Analyzer adalah integrasi, dalam satu aplikasi Web, dari berbagai macam

langkah-langkah yang didefinisikan dalam pendekatan NMRG. Kita perlu menggunakan berbagai perangkat lunak agar bias mengonversi dan melakukan analisis yang dia ingin lakukan, seperti menggunakan alat SNMPDUMP dan koleksi Skrip Perl Perangkat lunak SNMPDUMP dapat mengkonversi file PCAP mentah menjadi format XML atau CSV, serta menghapus atau menganonimkan data sensitif yang mungkin ada dalam jejak lalu lintas. Karena itu, Alat Pengelolaan Lalu Lintas Manajemen diimplementasikan di atas SNMPDUMP, meminta fungsinya kapanpun diperlukan. Akhirnya, teknik visualisasi ada telah diimplementasikan sebagai aplikasi Adobe Flash. Teknik visualisasi ini berdasarkan banyak grafik yang digunakan

sangat cocok untuk mewakili spesifik aspek jaringan komputer seperti topologinya. Untuk menghasilkan visualisasi topologi jaringan manajemen harus mengidentifikasi di antaranya

pesan di trafik lalu lintas SNMP, yang terminalnya bertindak sebagai manajer, agen. Kita bisa mengidentifikasi dengan membelah seluruh trafik lalu lintas ke berbagai SNMP. Pesan SNMP terdiri dari kumpulan pesan antara sumber dan alamat tujuan yang termasuk dalam Command Generator (CG) / Command Hubungan Responden (CR), atau Originator Pemberitahuan (TIDAK) / Hubungan Penerima Pemberitahuan (NR). Sebuah analisis yang mungkin untuk melacak lalu lintas SNMP adalah perhitungannya dari berapa kali objek SNMP berada terlihat dalam daftar varbind pesan. Jejak lalu lintas hanya dengan mengamati OID (pengenal) ini benda. Karena objek SNMP diatur dalam Manajemen Informasi Base (MIB), akan lebih mudah jika ada .Bisa juga memvisualisasikan hasil analisis ini pada pohon MIB, Karena itu, kami usulkan teknik visualisasi untuk mempresentasikan hasil analisis dengan cara yang potensi wawasan akan meningkat. Mekanisme interaksi memungkinkan pengguna bias melihat yang sedang divisualisasikan dalam histogram, serta untuk browsing melalui trafik yang tersedia di SNMP.

 Penggunaan teknik visualisasi memiliki potensi besar pada manajemen jaringan. Besarnya jumlah informasi yang dihasilkan oleh berbagai perangkat dan sistem itu menyusun jaringan modern menuntut lebih banyak usaha untuk membuat semua data manajemen lebih bersahabat bagi operator jaringan, dan vendor sistem manajemen dan penelitian. IRTF itu Pendekatan untuk pengukuran lalu lintas SNMP merupakan langkah penting dan menunjukkan kebutuhan akan perkembangan teknik visualisasi yang spesifik. Informasi baru tentang Penggunaan SNMP yang dikumpulkan di jaringan produksi dunia nyata lebih mudah diamati dengan kerja visualisasi analisis lalu lintas SNMP. Karya ini mengusulkan tiga teknik untuk pertama kalinya memvisualisasikan informasi spesifik yang terkait dengan pendekatan pengukuran lalu lintas SNMP IRTF. Visualisasi ini mampu Secara grafis menyandikan banyak informasi yang dihasilkan sebagai hasilnya dari jejak lalu lintas SNMP analisis.Kami juga menunjukkan bagaimana visualisasi yang diusulkan dalam makalah ini dapat membuat analisis Pengukuran lalu lintas semakin mudah dan efisien. Alat Traffic Analyzer Manajemen masih dalam pengembangan. Untuk pekerjaan di masa depan, kami berencana untuk meningkatkan himpunan Teknik visualisasi tersedia di alat, agar meningkatkan potensi wawasan dari jejak lalu lintas SNMP. Kita juga berniat menambahkan alat Pengelola Lalu Lintas Manajemen dukungan untuk mengukur jenis lalu lintas manajemen lainnya (misalnya, Lalu lintas layanan Web, lalu lintas ICMP, dll), agar bisa meningkat pengetahuan tentang pola penggunaan manajemen jaringan lalu lintas yang bisa ditemukan dalam produksi saat ini dan masa depan jaringan.