A Network Isolation Analysis in Xen

PRESENTA

M.C. Violeta Medina Rios
Dr. Juan Manuel García García

División de Estudios de Posgrado
Facultad de Ingeniería Eléctrica
Universidad Michoacana de San Nicolás de Hidalgo

Junio, 2009

ACIS

Introducción

- **Aislamiento,** característica importante de un Monitor de Máquina Virtual *(MMV)*.

- **Sistema bien aislado**, la degradación de rendimiento de una máquina virtual *(MV)* no afecta a otras MVs que comparten el mismo equipo.
  - Aislamiento de falla
  - Aislamiento de rendimiento

- En este artículo, se presenta un análisis de aislamiento de red usando como MMV, Xen en tres diferentes pruebas.

ACIS

Introducción

Virtualización, técnica de división de recursos de un servidor en múltiples e independientes ambientes de ejecución. Líneas principales:

- **Virtualización completa**
- **Paravirtualización**
- **Virtualización a nivel sistema operativo**
- **Virtualización Nativa**

ACIS

Introducción

- Ataques de Denegación de Servicios *(DoS),* irrumpen o bloquean completamente el servicio para los usuarios legítimos, redes, sistemas y otros recursos.

- Existen varias formas de ataques de DoS: SYN flood, ICMP flood, UDP flood, etc.

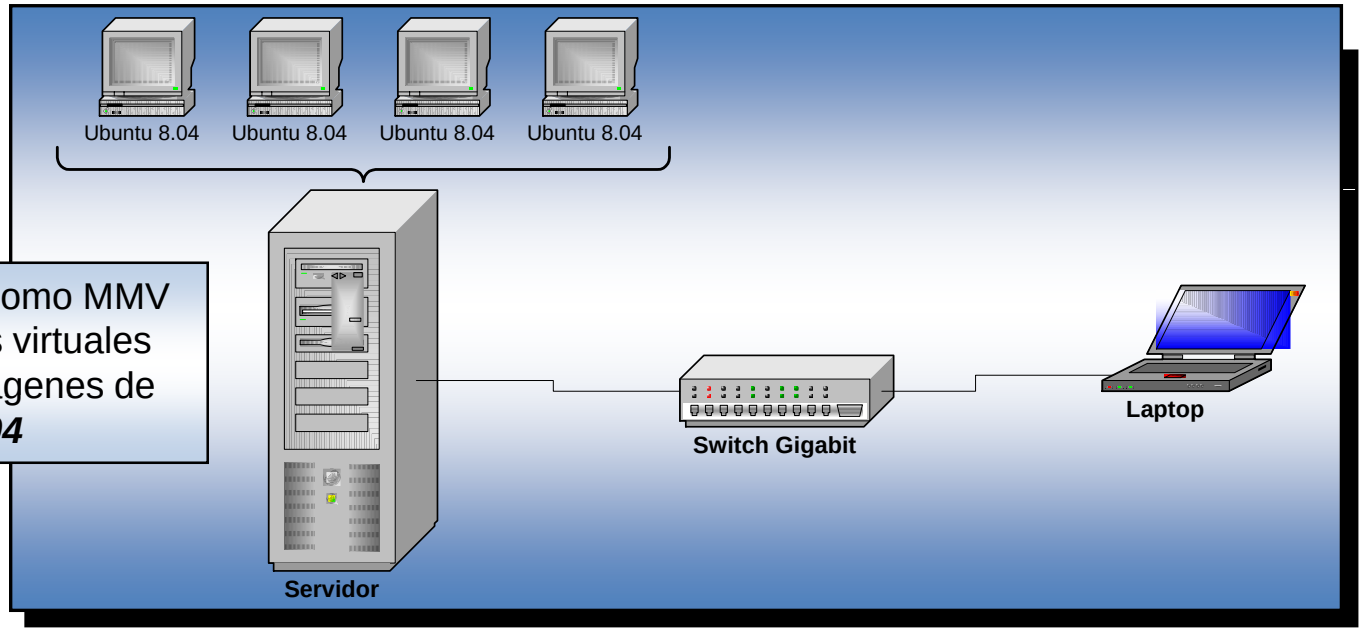
- En este trabajo se simularon ataques de denegación de servicios.

Trabajos Relacionados

- Comparación de rendimiento de Xen contra Linux Nativo y contra otros VMM, tales como VMWare [15].
- Análisis de algunos VMM en un ambiente clusterizado contra Linux nativo [2].
- Análisis de aislamiento de rendimiento. Pruebas intensivas sobre CPU, memoria, disco, envío/recepción de paquetes UDP, bombas fork en diferentes ambientes virtualizados [16].
- Comparación de aislamiento de rendimiento entre Xen y KVM [17].

Escenario de Pruebas

- ***Xen*** 3.0.3 como MMV
- 4 Máquinas virtuales usando imágenes de ***Ubuntu 8.04***



Servidor
2 procesadores Quad-core 2.0 GHz
3 GB memoria RAM
72 GB Disco duro
Debian 4.0 SO base

Laptop
1 procesador Pentium M 2.0 GHz
2 GB memoria RAM
80 GB Disco duro
Debian 4.0 SO base

ACIS

Experimentos

- Se aplicaron tres diferentes pruebas de estrés en una máquina virtual.

- Para calcular el porcentaje de degradación en el ancho de banda durante las pruebas, se calculó el rendimiento sin carga.

Throughput promedio sin carga en las máquinas virtuales

	MV1	MV2	MV3	MV4
Throughput (10^6 bits/seg)	247.04	219.39	237.42	233.15

ACIS

Experimentos. Ataque SYN Flood/Web

Throughput (10^6 bits/seg) promedio en máquinas virtuales durante ataques de denegación de servicios

	MV Estresada	VM1	VM2	VM3	Resultados
SYN Flood	99.82	279.38	278.19	277.42	**MV Estrasada** Rendimiento: 40.41% Degradación: 59.59% **MVs no estresadas** No sufren degradación
Ataque al servidor web	234.09	231.50	236.14	234.83	**MV estresada** Denegación de servicio desde la conexión de 4,000 clientes. **MVs no estresadas** Ligera degradación de hasta 0.6%

ACIS

Experimentos. Cargas/descargas masivas

Throughput promedio del sistema durante un ataque de cargas masivas

Clientes	% Throughput	%Degradación
100	18.72	81.28
250	29.52	70.48
500	59.20	40.80
750	65.89	24.11
1,000	89.91	10.09

Degradación de throughput del sistema de hasta un 81.28% con 100 clientes.

Throughput promedio del sistema durante un ataque de descargas masivas

Clientes	% Throughput	%Degradación
100	5.35	94.65
250	3.57	96.43
500	0.39	99.61
750	0.54	99.46
1,000	0.75	99.25

Degradación de throughput del sistema de hasta un 99.43% con 500 clientes.

ACIS

Conclusiones

- Xen presentó un aislamiento excelente durante ataques de tipo SYN flood y a un web server.
- El sistema puede ser degradado casi un 100% durante cargas/descargas masivas de información.
- Se obtuvieron resultados opuestos a lo reportado en anteriores trabajos relacionados.

ACIS

Trabajos Futuros

- Desarrollo de un mecanismo que permita limitar el ancho de banda usado para cada SO huésped como parte del hipervisor Xen.

ACIS

Referencias

[1] P. Changarti, *Xen Virtualization: A Practical Handbook*, 1st ed. Birmingham, B27 6PA, UK.: Packt Publishing Ltd., 2007.

[2] V. Chaudhary, M. Cha, J. Walters, S. Guercio, and S. Gallo, "A comparison of virtualization technologies for hpc," *Advanced Information Networking and Applications, 2008. AINA 2008. 22nd International Conference on*, pp. 861–868, March 2008.

[3] D. Chisnall, *The definitive guide to the xen hypervisor*. Upper Saddle River, NJ, USA: Prentice Hall Press, 2007.

[4] J. Smith and R. Nair, "The architecture of virtual machines," *Computer*, vol. 38, no. 5, pp. 32–38, May 2005.

[5] D. Hu and Y. Y. Wang, "Teaching computer security using xen in a virtual environment," *Information Security and Assurance, 2008. ISA 2008. International Conference on*, pp. 389–392, April 2008.

[6] J. William I. Bullers, S. Burd, and A. F. Seazzu, "Virtual machines - an idea whose time has returned: application to network, security, and database courses," *SIGCSE Bull.*, vol. 38, no. 1, pp. 102–106, 2006.

[7] M. Rosenblum and T. Garfinkel, "Virtual machine monitors: current technology and future trends," *Computer*, vol. 38, no. 5, pp. 39–47, May 2005.

[8] D. Rule and R. Dittner, *The Best Damn Server Virtualization Book Period*, 1st ed. Burlington, MA, USA: Syngress Publishing Inc., 2007.

[9] S. E. Madnick and J. J. Donovan, "Application and analysis of the virtual machine approach to information system security and isolation," in *Proceedings of the workshop on virtual computer systems*. New York, NY, USA: ACM, 1973, pp. 210–224.

[10] D. Gupta, L. Cherkasova, R. Gardner, and A. Vahdat, "Enforcing performance isolation across virtual machines in xen," in *Proceedings of the 7th ACM/IFIP/USENIX Middleware Conference*, November 2006.

[11] C. Schuba, I. Krsul, M. Kuhn, E. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a denial of service attack on tcp," *Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on*, pp. 208–223, May 1997.

[12] A. Piskozub, "Denial of service and distributed denial of service attacks," *Modern Problems of Radio Engineering, Telecommunications and Computer Science, 2002. Proceedings of the International Conference*, pp. 303–304, 2002.

[13] J. Mirkovic and P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms," *SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–53, 2004.

[14] S. Kamal and B. Issac, "Analysis of network communication attacks", *Research and Development, 2007. SCOReD 2007. 5th Student Conference on*, pp. 1–6, Dec. 2007.

[15] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, "Xen and the art of virtualization," in *SOSP '03: Proceedings of the nineteenth ACM symposium on Operating systems principles*. New York, NY, USA: ACM, 2003, pp. 164–177.

[16] J. N. Matthews, W. Hu, M. Hapuarachchi, T. Deshane, D. Dimatos, G. Hamilton, and M. McCabe, "Quantifying the performance isolation properties of virtualization systems," in *ecs'07: Experimental computer science on Experimental computer science*. Berkeley, CA, USA: USENIX Association, 2007, pp. 5–5.

[17] T. Deshane, Z. Shepherd, J. N. Matthews, M. Ben-Yehuda, A. Shad, and B. Rao, "Quantitative comparison of xen and kvm," in *Xen Summit*, 2008.

[18] Jailtime, http://www.jailtime.org/, 2008.

[19] N. Homepage, http://www.netperf.org/, 2008.

ACIS