A Free Antivirus information newsletter from the developers of SmartCOP Internet Security

Vol. 8 Issue 1.

January, 2012

SmartCOP Times

Dear Reader,

We wish our readers and associates a Very Happy and Prosperous New Year 2012. May this Year 2012 bring peace and happiness to all, around the world. When it comes to the new year resolution for our team, it will remains the same, as it was for every year, that we will put our best efforts to give virus free network by providing effective software and prompt support.

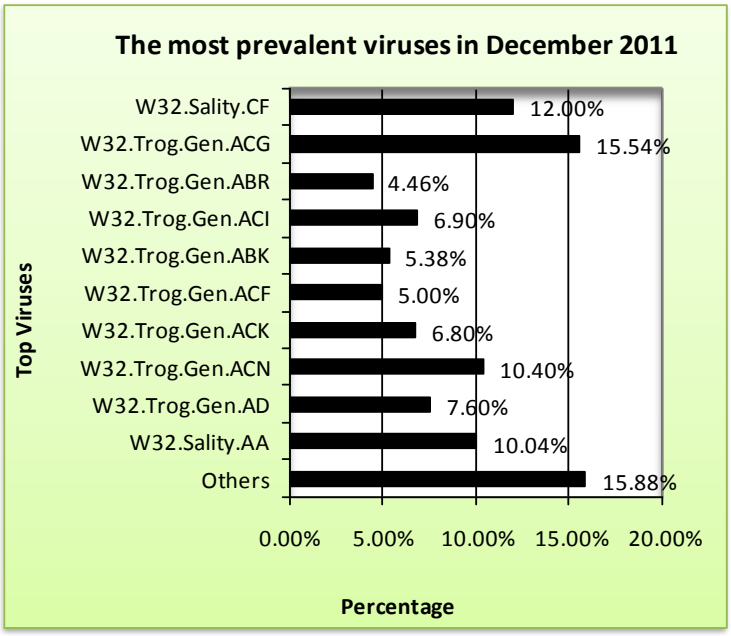
This Year 2011 has been very successful for our company. We have developed our dealer network all over India and especially in Gujarat, Rajasthan, and Haryana. Now SmartCOP Internet Security is spreading all over India and has a strong channel network of dealers and distributors across the country. We have also stepped in international market. SmartCOP is now globally present.

We are very actively bringing out various schemes and offers for our dealers and distributors. These schemes will give direct benefits to the dealers and distributors. For more detail of the various schemes and offers, we request you to kindly contact us at our office nos. We will love to forward the schemes.

Further we would like to extend our users about the new feathers in our cap this year. SmartCOP Internet Security Suite is now international certified product. Our product has been awarded the Check Mark Certification. This is elite organization which tests the internet security product and if satisfied with the performance of the software, then awards the certification.

Now user can also get the detail of SmartCOP on the current on going social networking sites like Face Book, Twitter, Google +. Our presence on these social networking sites gives us the direct feedback of client and helps us in spreading the awareness of SmartCOP.

For the year 2012, the first edition of SmartCOP Time give brief information about topics like Virtualization of Computers. About virtual servers and relevant topics etc. Readers will also find the overview about cloud computing, characteristic of cloud computing, Cloud Computing security and its risk associated with it.. Important URLS as usual is the part of this newsletter.



We shall always look forward to improve this newsletter. Improvement will lot depends on the kind feedback from our readers. Hence we request you to be active participant and send us the feedback.

Your feedback and suggestions will be like asset to us and will bring improvement in SmartCOP Times. We also request you to kindly send us articles, views, comments and suggestions. We will take up your article and publish it the best ones in the fourth coming edition of SmartCOP Times. You can reach us at e-mail sales@s-cop.com.

SmartCOP Internet Security
Around the Web:

Skype: smartcop.support

Topic Covered Inside.....

- **Virtualization of Computers**
- **What is Virtual Machine**
- **Cloud computing**
- **Cloud computing security**

Virtualization of Computers

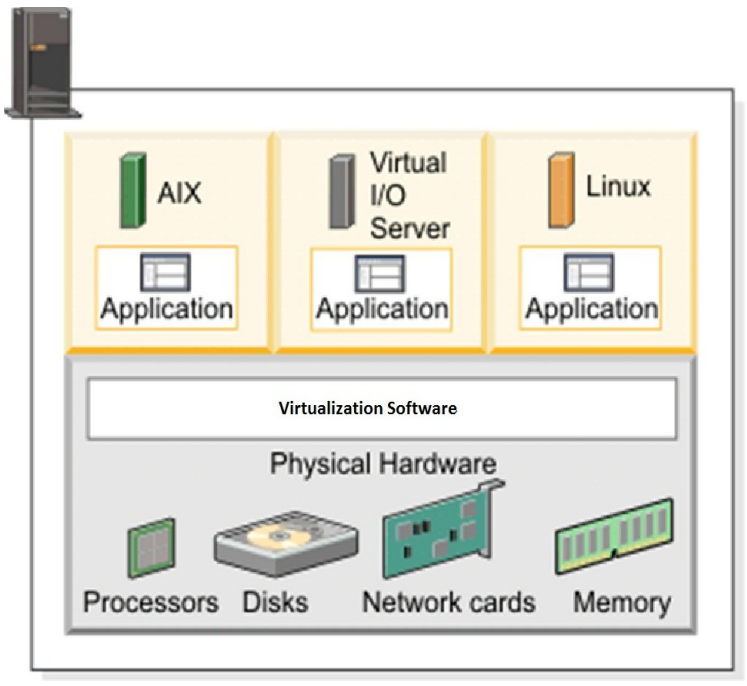
Virtualization: is the creation of a virtual such as an operating system, a server, a storage device or network resources. Operating system virtualization is the use of software to allow a piece of hardware to run multiple operating system images at the same time. The technology got its start on mainframes decades ago, allowing administrators to avoid wasting expensive processing power.

In 2005, virtualization software was adopted faster than anyone imagined, including the experts. There are three areas of IT where virtualization commonly used are Network, Storage & Server virtualization.

Network virtualization: is a method of combining the available resources in a network by splitting up the available bandwidth into channels, each of which is independent from the others, and each of which can be assigned (or reassigned) to a particular server or device in real time. The idea is that virtualization disguises the true complexity of the network by separating it into manageable parts, much like your partitioned hard drive makes it easier to manage your files.

Storage virtualization: is the pooling of physical storage from multiple network storage devices into what appears to be a single storage device that is managed from a central console. Storage virtualization is commonly used in storage area networks (SANs).

Server virtualization: is the masking of server resources (including the number and identity of individual physical servers, processors, and operating systems) from server users. The intention is to spare the user from having to understand and manage complicated details of server resources while increasing resource sharing and utilization and maintaining the capacity to expand later.



Server Virtualization

Virtualization can be viewed as part of an overall trend in enterprise IT that includes autonomic computing, a scenario in which the IT environment will be able to manage itself based on perceived activity, and utility computing, in which computer processing power is seen as a utility that clients can pay for only as needed. The usual goal of virtualization is to centralize administrative tasks while improving scalability and work loads.

What is Virtual Machine : Virtual machine (VM) is an environment, usually a program or operating system, which does not physically exist but is created within another environment. In this context, a VM is called a "guest" while the environment it runs within is called a "host." Virtual machines are often created to execute an instruction set different than that of the host environment. One host environment can often run multiple VMs at once. Because VMs are separated from the physical resources they use, the host environment is often able to dynamically assign those resources among them.

A user interacting with a virtualized server can view the server as a physical machine, in the sense that the user would see access to machines resources like hard disks, RAM, processors and Ethernet connections. In fact, all of these machine resources are virtual. For instance, instead of accessing a real hard disk, the user is accessing a construct of the host environment. This construct then accesses the real disk to record the data.

What is Virtual server

A server, usually a Web server, that shares computer resources with other virtual servers. In this context, the virtual part simply means that it is not a dedicated server -- that is, the entire computer is not dedicated to running the server software.

Virtual Web servers are a very popular way of providing low-cost web hosting services. Instead of requiring a separate computer for each server, dozens of virtual servers can co-reside on the same computer. In most cases, performance is not affected and each web site behaves as if it is being served by a dedicated server. However, if too many virtual servers reside on the same computer, or if one virtual server starts hogging resources, Web pages will be delivered more slowly.

Server Virtualization

Server virtualization is the partitioning of a physical server into smaller virtual servers. In server virtualization the resources of the server itself are hidden, or masked, from users, and software is used to divide the physical server into multiple virtual environments, called virtual or private servers.

One common usage of this technology is in Web servers. Virtual Web servers are a very popular way of providing low-cost web hosting services. Instead of requiring a separate computer for each server, dozens of virtual servers can co-reside on the same computer.

Server virtualization has many benefits. For example, it lets each virtual server run its own operating system and each virtual server can also be independently rebooted of one another. Server virtualization also reduces costs because less hardware is required so that alone saves a business money. It also utilizes resources to the fullest so it can also save on operational costs (e.g. using a lower number of physical servers reduces hardware maintenance).

There are several ways to create a virtual server, with the most common being; virtual machine, operating system-level virtualization, and par virtual machine.

Commonly Used software for Virtual Machine are :

1. VMWARE Virtualization software.

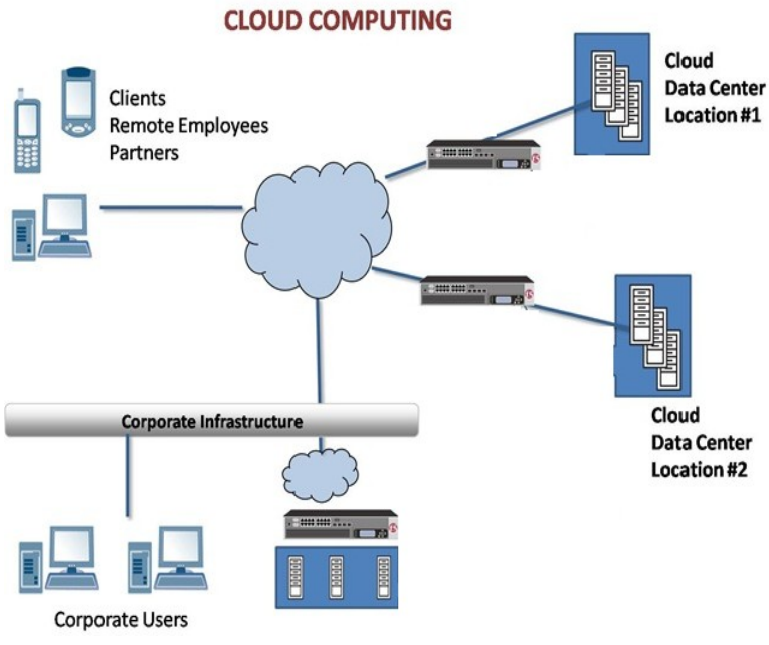
2. Virtual Box Software.

Cloud computing

Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet).

Overview

Cloud computing is a marketing term for technologies that provide computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. A parallel to this concept can be drawn with the electricity grid, wherein end-users consume power without needing to understand the component devices or infrastructure required to provide the service.



Characteristics Cloud computing exhibits the following key characteristics:

Empowerment of end-users of computing resources by putting the provisioning of those resources in their own control, as opposed to the control of a centralized IT service (for example)

Agility improves with users' ability to re-provision technological infrastructure resources.

Application programming interface (API) accessibility to software that enables machines to interact with cloud software in the same way the user interface facilitates interaction between humans and computers. Cloud computing systems typically use REST-based APIs.

Cost is claimed to be reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure. This is purported to lower barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained with usage-based options and fewer IT skills are required for implementation (in-house).

Device and location independence enable users to access systems using a web browser regardless of their location or what device they are using (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.

Multi-tenancy enables sharing of resources and costs across a large pool of users thus allowing for:

Centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)

Peak-load capacity increases (users need not engineer for highest possible load-levels)

Utilization and efficiency improvements for systems that are often only 10–20% utilized.

Reliability is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.

Security could improve due to centralization of data, increased security-focused resources, etc.

Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer.

Cloud computing security

Cloud computing security (sometimes referred to simply as "cloud security") is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

Seven cloud-computing security risks

Cloud computing is picking up traction with businesses, but before you jump into the cloud, you should know the unique security risks it entails

Cloud computing is fraught with security risks. Smart customers will ask tough questions and consider getting a security assessment from a neutral third party before committing to a cloud vendor.

Here are seven of the specific security issues ,customers should raise with vendors before selecting a cloud vendor.

1.Privileged user access. Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs. Get as much information as you can about the people who manage your data. "Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access," .

2. Regulatory compliance. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are "signaling that customers can only use them for the most trivial functions,"

3. Data location. When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.

4. Data segregation. Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. "Find out what is done to segregate data at rest," Gartner advises. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability,"

5. Recovery. Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. "Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure. Ask your provider if it has "the ability to do a complete restoration, and how long it will take.".

6. Investigative support. Investigating inappropriate or illegal activity may be impossible in cloud computing. "Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible."

7. Long-term viability. Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application,"