



Best Practices for Optimizing Performance and Availability in Virtual Infrastructures

Table of Contents

Introduction: The Challenges of Virtual Infrastructures	3
Understanding Virtual Infrastructures	4
Achieving Complete End-to-End Visibility.....	6
Nimsoft in the Virtual Infrastructure.....	7
Deploying Nimsoft in the Virtual Infrastructure: 4 Steps to Success	9
Step 1—Laying the Foundation	9
Step 2—Adding the Physical Environment	9
Step 3—Adding the Virtual Environment	9
Step 4—Putting it All Together.....	9
Next Steps: Other Considerations?	10
Running Nimsoft as a Virtual Appliance?.....	10
VMware and Nimsoft Automation Integration.....	10
Managing SOA (Service Oriented Architecture) in Virtualized Environments.....	10
Considerations for Managed Service Providers	10
About Nimsoft	11

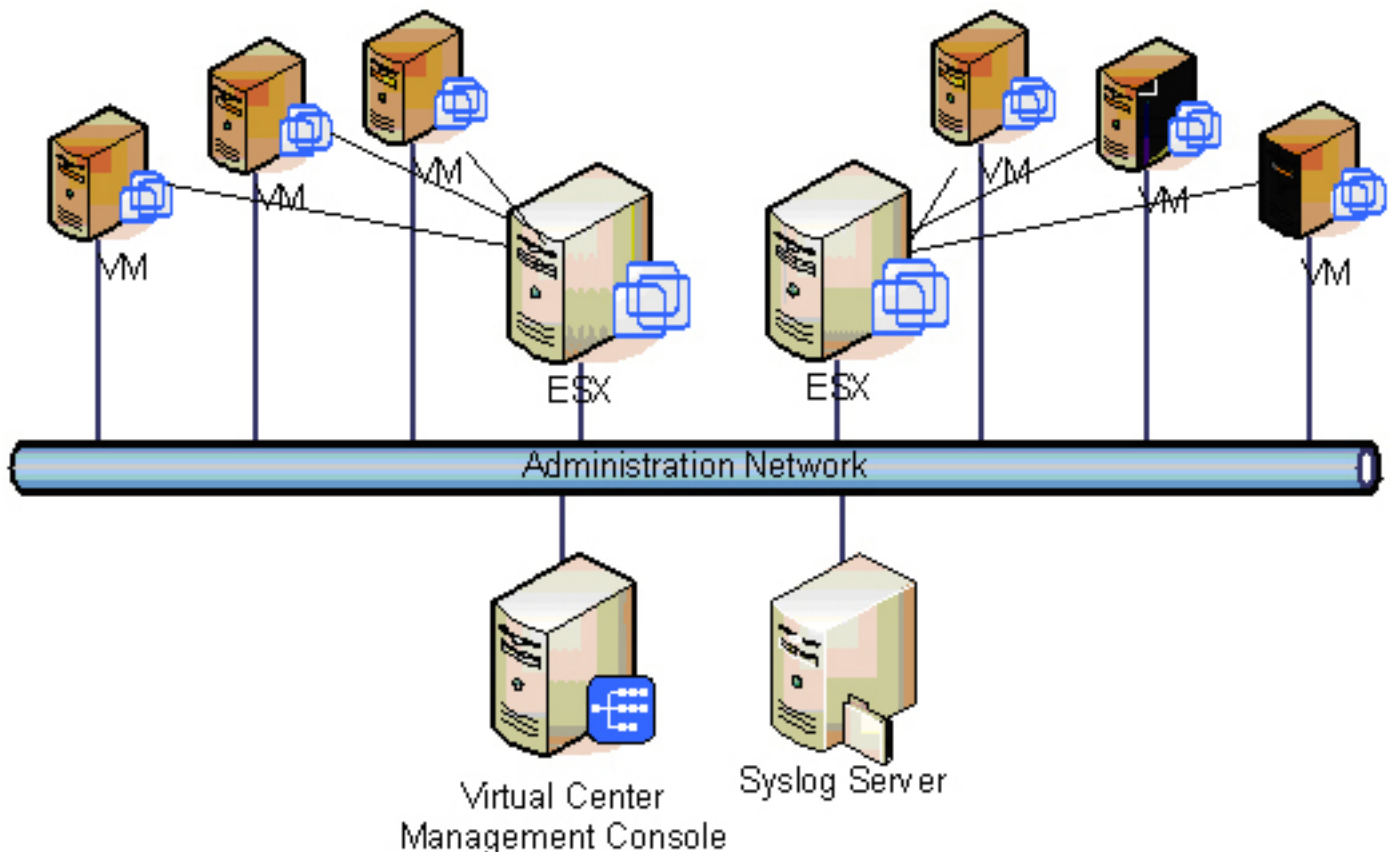
Introduction: The Challenges of Virtual Infrastructures

Many IT administrators have already learned the hard way that managing the performance and availability of services built on virtualization technologies can be difficult, if not impossible at times. All too often, early adopters of virtualization have struggled with limited technology features and stability constraints, while learning new ways to effectively manage capacity requirements.

Fortunately, some platforms now offer clustering solutions that are mature enough to automate the balancing of workloads across physical resources. When combined with disciplined capacity planning and sound deployment configurations, it is possible to achieve fast, scalable, and highly available IT services using virtualization platforms.

Initial virtualization deployments are typically basic configurations that consist of a couple physical servers and a dozen virtual machines on a shared, flat network. Often, organizations find that these deployments are only suitable for testing and development, and are not able to meet the needs of demanding production environments very well. Consequently, IT teams need to invest in and effectively deploy such solutions as centralized storage, cluster technologies, networking, and systems management in order to realize successful virtualization initiatives.

Once these IT investments are made, the many benefits of virtualization, such as ease of management and use, are often quickly realized. After these initial successes, however, IT management often starts to be concerned about the growing sprawl of business critical virtual machines and the lack of visibility required to effectively understand the performance of these IT services.



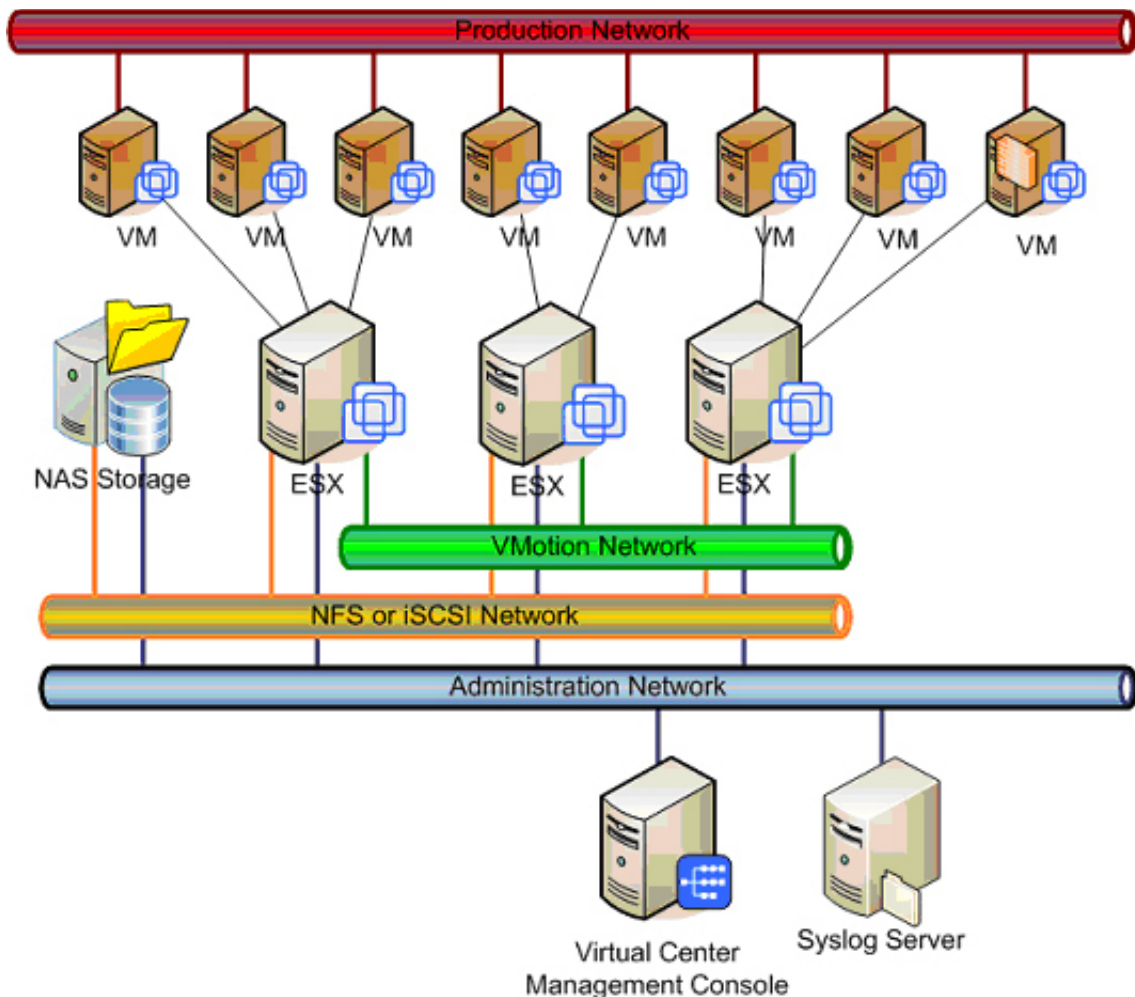
Understanding Virtual Infrastructures

This section offers an overview of all the infrastructure components that comprise an effective, high-quality virtualized IT service.

In this example, there is a minimum cluster configuration of three VMware ESX hosts hosting eight virtual machines. However, the industry average for ESX hosts is eight to twelve virtual machines each. It's common practice to share a single CPU core between two or three virtual machines. More I/O intensive virtual machines should require a minimum of one or two cores each.

Memory is very important in virtualized environments. It's common practice to install as much RAM as possible on the ESX servers (e.g. 128GB or 256GB) and allocate enough RAM to run each virtual machine in physical memory.

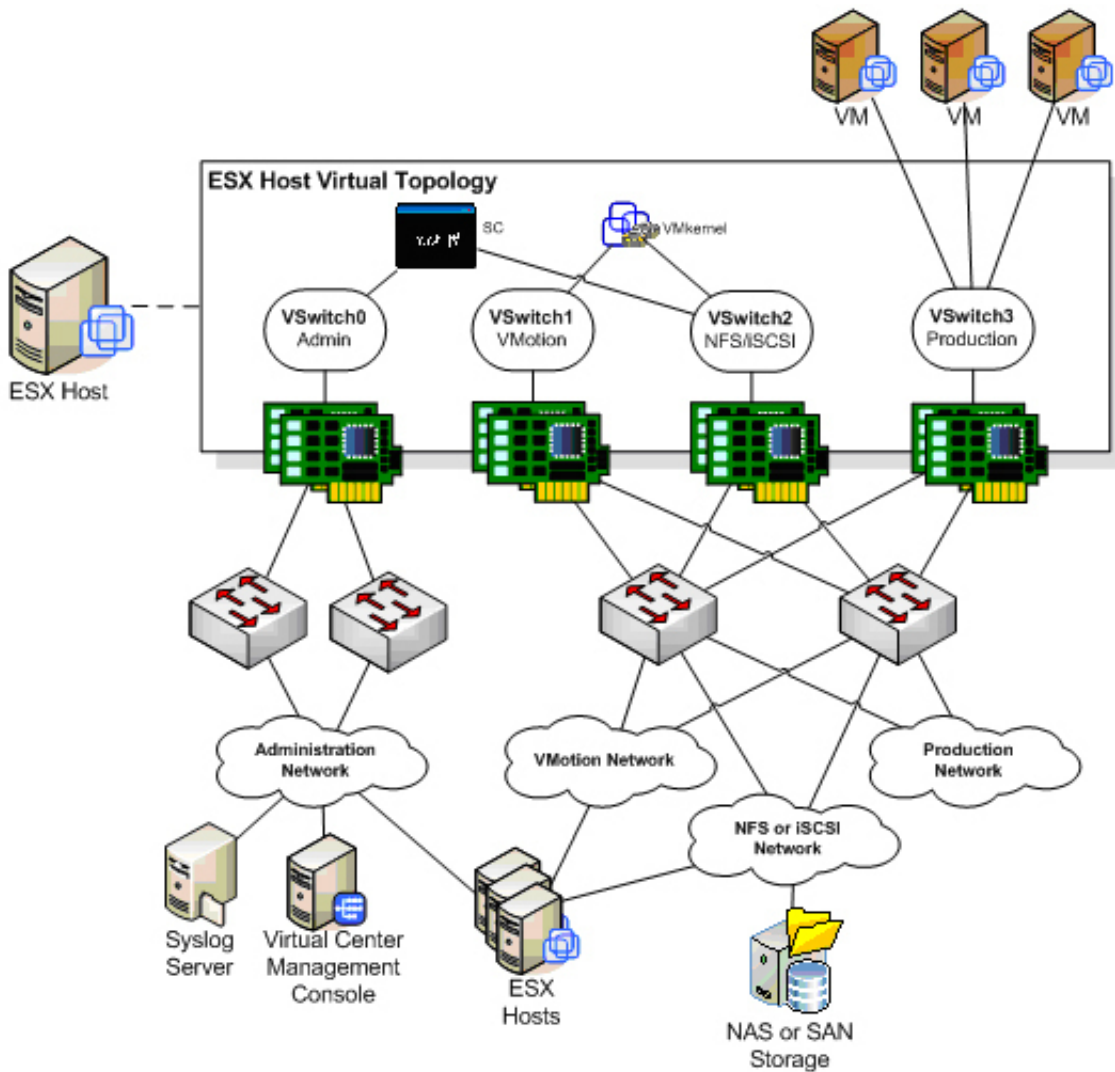
Centralized storage is essential in virtualized environments. Fibre Channel connectivity is still recommended for best performance, although iSCSI is a popular low cost alternative that also performs very well. NFS NAS-based storage is best used for backups, snapshots, logs, shared files, data stores, etc. Using integrated SAN/NAS solutions enables optimized backup/recovery features, but these implementations must be carefully planned to ensure there is no impact on application and systems performance. Some organizations address this challenge by deploying dedicated storage resources for virtualization and physical platforms, and another storage resource dedicated to applications and databases.



Network bandwidth, connectivity, segmentation, and traffic shaping configurations are also key to the performance of virtualized environments. 1Gbps+ network interface cards can be combined to load balance network traffic and provide high availability. Segmentation of the data access, VMotion, administrative, and production traffic improves the reliability and security of communications. Leveraging the new Cisco protocol communications support in ESX servers also improves the performance and management of the network environment. Administrators should also carefully consider the network demands for each virtual machine and the aggregate demand on the ESX host.

Virtual machines also perform better when they are grouped into resource pools based on similar operating systems, applications, and workloads. The careful distribution of resource pools across DRS clusters is also essential to improving performance and scalability.

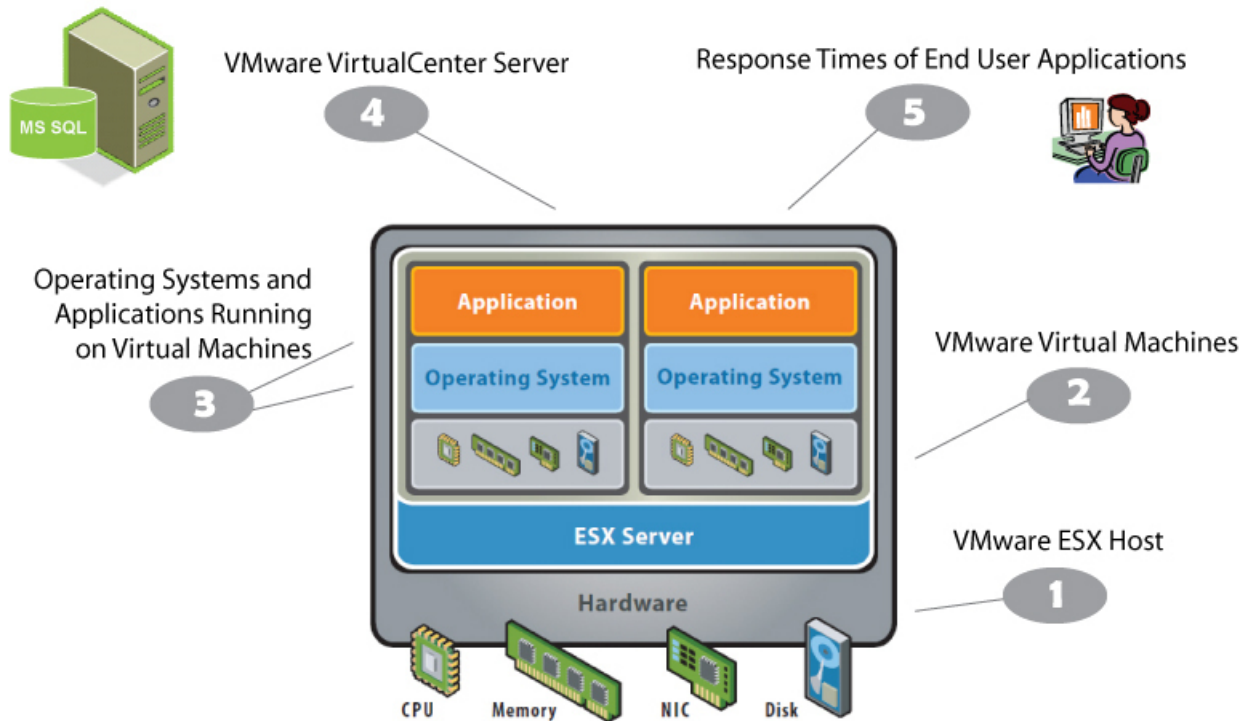
The following diagram depicts an ESX host for the sample infrastructure outlined above. This configuration is optimized for high availability, performance, and security. Each virtual network is isolated, redundant, and highly available.



Achieving Complete End-to-End Visibility

Although a finely tuned, clustered virtual infrastructure can balance the workload among ESX hosts very effectively, IT service performance and availability issues can still arise. While virtual machines can automatically migrate between ESX hosts within a cluster, depending on defined CPU and memory requirements, this capability is not always enough to ensure reliable IT services.

Performance issues generally arise due to one of two issues. First, the combination of ineffective application configuration or design and unexpected usage levels can be one source of performance degradation. Second, changes to or failures in the underlying virtual or physical platform infrastructure can also create performance problems. Complete end-to-end visibility is required for effective capacity planning, troubleshooting issues, as well as reporting the availability of the IT Services.

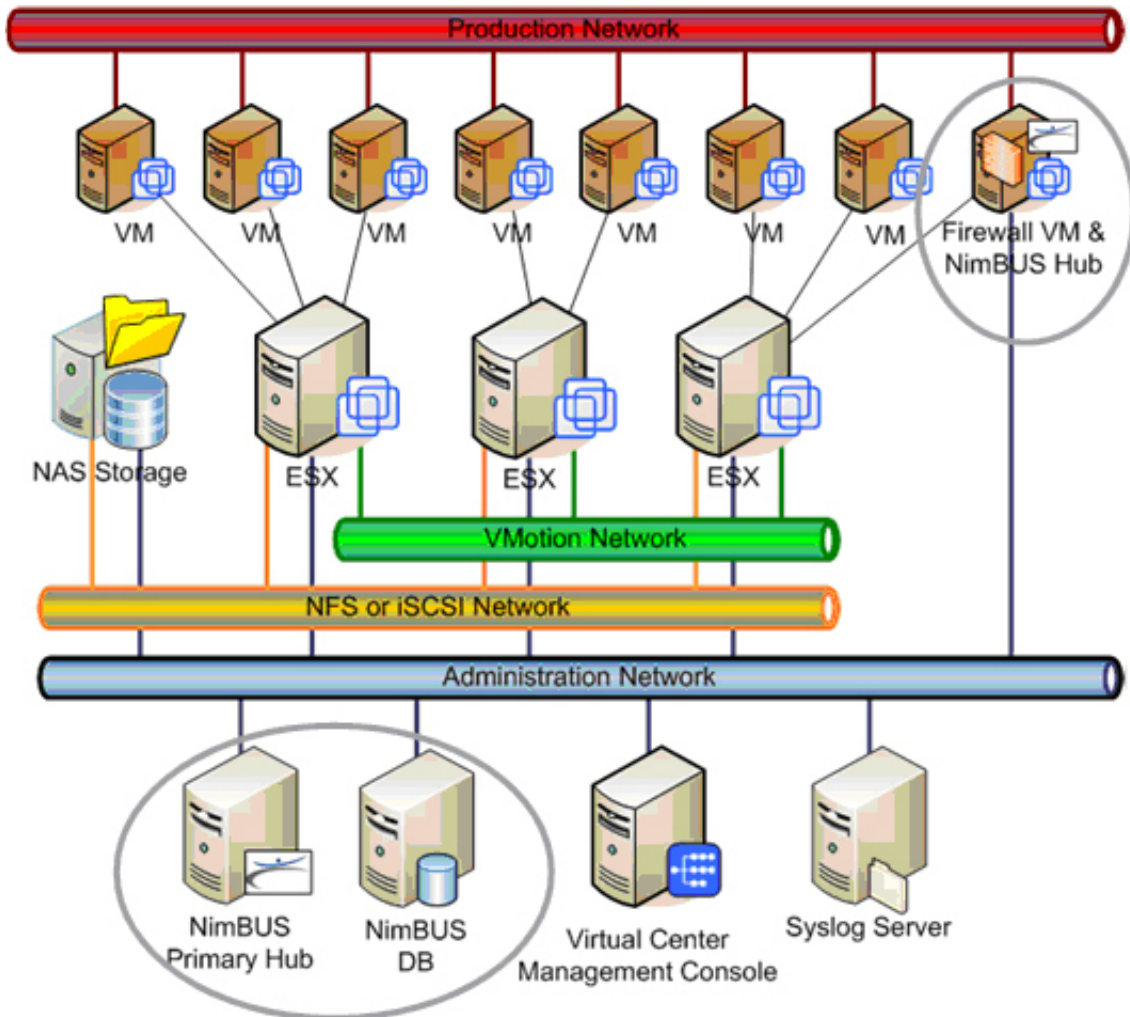


For a complete picture of the performance and capacity of a virtual infrastructure, administrators must be able to collect and analyze metrics from all of the following components:

- VMware ESX hosts
- VMware virtual machines
- Operating systems and applications running on virtual machines
- VMware Virtual Center Server health
- End user response times
- Networking devices and bandwidth
- Systems and application logs
- Storage devices, NAS, and SANs

Nimsoft in the Virtual Infrastructure

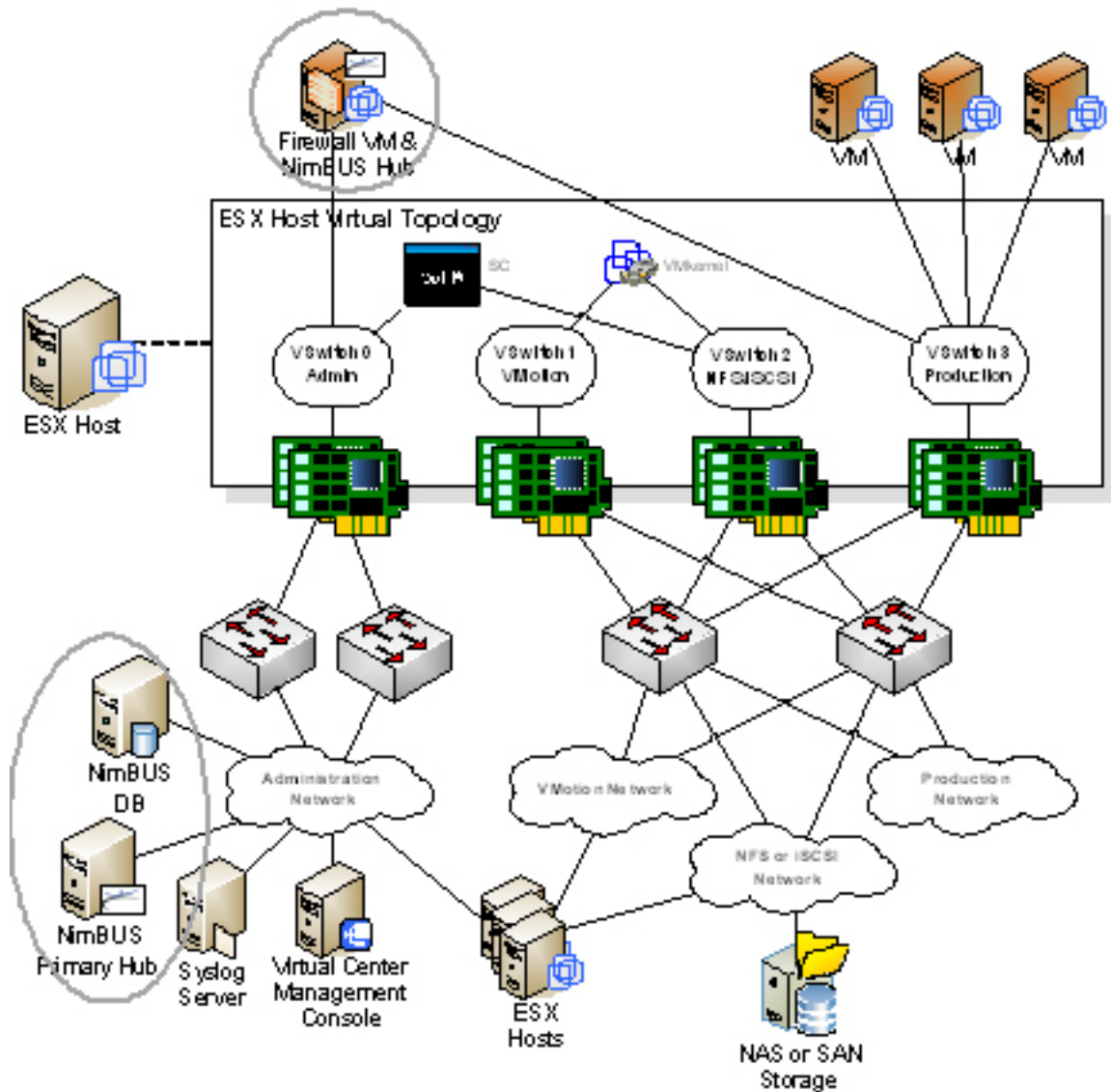
Nimsoft products from Nimsoft uniquely address the challenges of comprehensive monitoring in virtualized environments. With Nimsoft, administrators can monitor the entire ecosystem—including the virtualization components, the resident business applications, and end user response times—to effectively understand and manage service levels in virtualized environments.



Deployed in the same virtual infrastructure example provided earlier, a typical Nimsoft deployment would consist of the hub server, which would be deployed on a physical server and monitor all the physical and virtual infrastructure components. In addition, CPU, disk, and memory (CDM) probes and various network, OS, and application probes would be deployed to collect information from all physical infrastructure components. The VMware probe would be deployed on the Virtual Center server (along with CDM and OS probes) to collect all virtual infrastructure metrics. The VMware Log Monitoring probe would be installed on the Syslog server to alert on events recorded in the logs.

A secondary hub server could be installed on a virtual machine (such as Linux or Windows) to collect metrics from the operating systems and applications in the virtual machines, then forward the data back to the primary hub server for reporting, alerting, and analysis behind a firewall.

The following diagram illustrates the corresponding ESX host server configuration to the example virtual infrastructure discussed above. The secondary Nimsoft hub on the firewall virtual appliance interfaces between production and administration networks to communicate metrics back to the primary hub server. In this segment, multiple virtual appliances should be used to best secure the environment, using one virtual machine per customer production environment.



Deploying Nimsoft in the Virtual Infrastructure: 4 Steps to Success

Step 1—Laying the Foundation

Install the Nimsoft Primary Hub and Database Servers

Traditionally, these have been deployed on physical servers in the administration network, but they are now commonly being deployed as virtual machines.

Step 2—Adding the Physical Environment

Install the Networking and SNMP Probes

Traditionally installed on the primary Nimsoft hub server, these probes are used to collect traffic and interface metrics on the administration, data, and VMotion networks.

Install Server CDM, OS, and Application Probes

All servers in the supporting administration network should have the following monitored: CPU, disk, memory, OS, and application. This should include the Virtual Center server, Syslog servers, and any other management servers, such as Bladelogic or Opsware.

Configure SNMP Storage Monitors

Nimsoft currently only supports monitoring of storage resources via SNMP. Real-time monitoring of the storage processors and fibre channel switches (if used) are critical to understanding overall performance and troubleshooting issues.

Step 3—Adding the Virtual Environment

Nimsoft for VMware Probe

It is considered best practice to install one VMware probe on each Virtual Center server. If not using a Virtual Center server, this probe is usually placed on the Nimsoft primary hub server, with up to 32 ESX hosts registered to it.

Virtual Center Health

Installing the CDM, Windows OS (ntservices), and various application probes in the previous step is only the first step to monitoring the Virtual Center server. It is also critical to monitor the logs, events, and processes of the Virtual Center server.

Virtual Servers—Virtual Machine OS and Application Probes

All virtual machines must also have OS and application monitoring probes to provide visibility to application issues. These probes are usually configured to report metrics to the secondary hub.

VMware Log Monitoring Probe

This probe can be installed on the Nimsoft hub server in conjunction with the integrated Nimsoft syslog server, or it can be installed on a different syslog server. Since VMware does not allow any probes or agents to be installed on the ESX host server, all VMware application and host system logs must be forwarded to a syslog server.

Step 4—Putting it All Together

End User Experience

Best practice guidelines advise that administrators have the end user response probes hosted in their own dedicated virtual machine. These probes can replay user sessions recorded on an application. The scripts can be instrumented to substitute variables from external sources, as well as report on the performance of specific steps and objects expected within the session. Administrators should build and test this solution in development and QA environments and then include this solution in every application released to production. This will ensure that any new changes to the application will not unexpectedly affect the production monitoring configurations. In addition, this approach will provide an essential tool for validating the applications in development and QA environments.

Alerting Configurations

After all the agents, probes, and associated configurations have been made, the next step is to identify and configure the alerting conditions required to notify the relevant IT operations teams.

Reporting—Dashboards and SLAs

After all the alerting conditions have been configured and tested, the last step is to create IT service dashboards, and performance and service level management reports. Included in this step is the setup and configuration of the service delivery portal for end users. This portal can be used to display all the appropriate dashboards, reports, and alerts to users with proper credentials.

Next Steps: Other Considerations?

Running Nimsoft as a Virtual Appliance?

While Nimsoft does not yet offer an official Nimsoft virtual appliance, customers have been building their own Nimsoft virtual appliances instead of hosting them on dedicated physical servers. Those who take this approach should be careful to ensure that the Nimsoft hub server can communicate consistently with the Virtual Center, network, secondary hubs, etc. even if VMotion migrates processing to a different ESX host.

VMware and Nimsoft Automation Integration

Nimsoft recently announced automation integration support with the VMware platform. The published documentation can be downloaded on the <http://www.nimsoft.com> Web site or by your account representative. The same VMware API used by Nimsoft to collect performance metrics from the virtual infrastructure can now also be used to trigger automation activities based on application, OS, end user, and physical performance conditions.

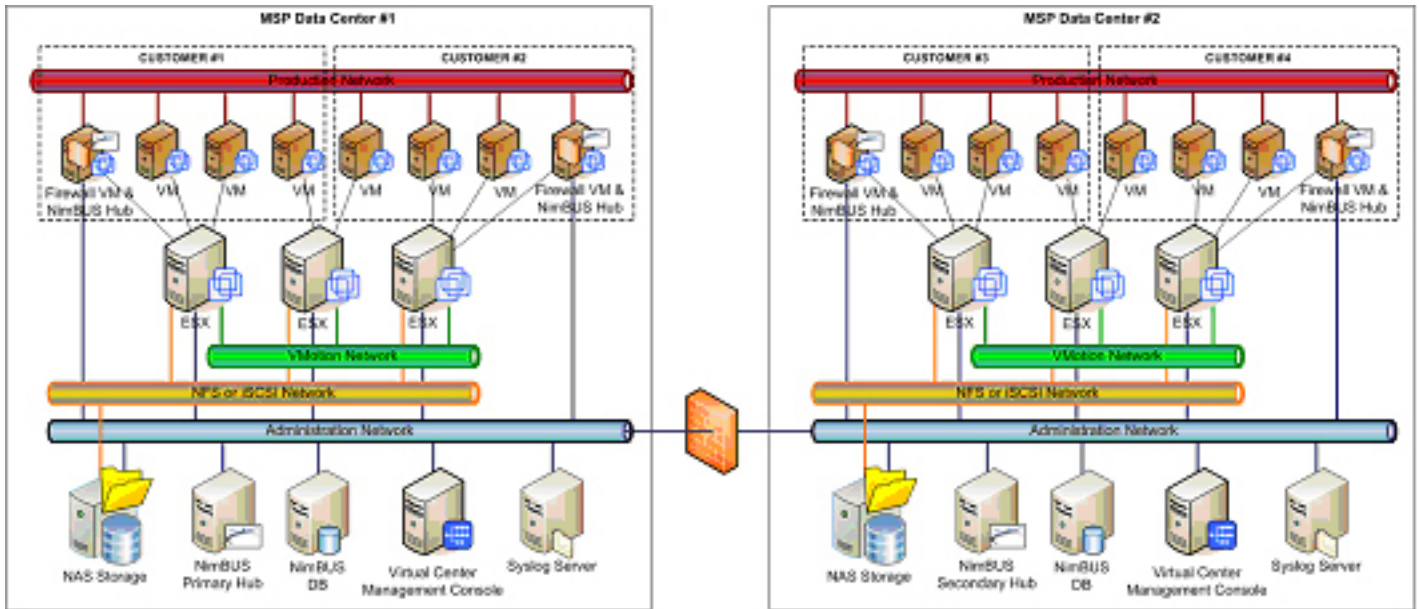
Managing SOA (Service Oriented Architecture) in Virtualized Environments

As IT Operations managers continue to adopt virtual appliances for IT application services, solution architects are now starting to design service oriented architecture (SOA) applications using virtual machines. SOA models typically break down the application into logical mini-applications that service requests from a common universal bus. These mini-application components are now being hosted within light-weight virtual machines, which can be grouped together to provide an IT service.

Considerations for Managed Service Providers

While we've already covered many considerations that benefit MSPs specifically, there are a few additional factors to consider in planning Nimsoft deployments:

- MSPs often offer the monitoring of applications in virtual machines as valuable add-on services. Core underlying physical and virtual infrastructure components can be included in the base platform for monitoring SLA's and services, using these additional tiers for further revenue generating opportunities.
- MSPs can offer physical servers and hardware-based appliances that contain a core virtual machine. This virtual machine can feature a Nimsoft secondary hub server and other important services, such as VPN as well. When the physical server is powered on, it automatically launches the virtual machine stored on the appliance. This approach has enabled some Nimsoft MSP customers to offer virtual machines and hardware appliances.
- For easier management and configuration, MSP's should use a Nimsoft hub server for each customer. Nimsoft products are easily scaled using a hub and spoke model, where the primary hub server is hosted within the MSP administration network and all secondary hub servers at the spoke level represent customer infrastructures. Spoke hub servers are often also stacked in a topology that represents geographic locations, like in various MSP or customer data centers.



About Nimsoft

Nimsoft is the fastest growing provider of next generation performance and availability monitoring solutions for the complete physical and virtualized IT infrastructure. The Nimsoft solutions redefine the standards for ease of use and speed of deployment—providing outstanding return on investment and unparalleled customer satisfaction. Over 800+ customers in 36 countries rely on Nimsoft solutions to monitor their IT based business applications and services. These customers include mid-market and global organizations, such as Barclays Capital and Amway Corporation, Bay Area Rapid Transit, Ladbrokes, MTU Aero Engines, TriNet, TRW Automotive, and hundreds of leading managed service providers such as CDW Berbee, Easynet and Rackspace Managed Hosting. For more information, visit www.nimsoft.com.

National Toll Free
 877 SLA MGMT (752.6468)
 Phone: 650.570.5401
info@nimsoft.com
www.nimsoft.com

United Kingdom
 + 44 (0) 845 456 7091

Norway & Northern Europe
 + 47 22 62 71 60

Germany
 + 49 89 208 039100

Australia
 + 61 (0)2 9236 7216