Supervisory control and data acquisition systems in virtual architecture built via VMware vSphere platform

MILOS PAVLIK, ROMAN MIHAL, LUKAS LACINAK, IVETA ZOLOTOVA
Dept. of Cybernetics and Artificial Intelligence
Technical university of Košice
Letná 9,042 00 Kosice
SLOVAKIA
milos.pavlik@tuke.sk   http://web.tuke.sk/kkui/

Abstract: - Virtualization techniques are getting more and more popular. They allow multiple virtual servers running on a single physical machine and offer many solutions for building virtual architecture that must meet some requirements, like availability, stability, reliability and etc. If we apply this on a SCADA/HMI (Supervisory Control and Data Acquisition/Human Machine Interface) systems that are running on such a virtual architecture, all of those requirements contribute to some sort of security, of these systems. This article deals with problems like minimization of server downtime after server outage or how to ensure the full functioning system despite the downtime of one or more production servers. Some of these servers provide access to management of real and virtual models in laboratory, so outage of these servers is undesirable. All of these requirements can be achieved via VMware vSphere functionalities.

Key-Words: - platform, cluster, availability, fault tolerance, architecture, vSphere, SCADA, model

1 Introduction

As a part of our research and implementing of VMware software on Dept. of Cybernetics and Artificial Intelligence, we've decided, that we'll try to build the architecture via VMware vSphere 5.0 platform. We have few real and virtual models in laboratory. Models like Intelligent House, Ball in Tube, Magnet etc. All of those models are controlled by PLC's (Programmable Logic Controllers) or by applications that runs from servers. SCADA/HMI (Supervisory Control and Data Acquisition/Human Machine Interface) systems are responsible for data acquisition, supervisory control and also they are in role of human-machine interface which is basically a visualization of system. These systems are using servers (communication, application, web, domain, OPC) and that's why there is need to meet the requirements like availability, stability and reliability. Before we've started to build our virtual architecture, that should meet the requirements, we've decided that the VMware vSphere 5.0 platform will be best for us, because it offers a lot of possibilities for all types or sizes of business. It brings a lot of functionalities through which we can achieve our requirements.

2 VMware vSphere 5.0 platform functionalities

Like it was said above, this platform brings a lot of functionalities through which we can achieve our requirements. The shorten downtime can be achieved via vSphere High Availability. So we needed a cluster, for example High Availability Cluster. It is a computer cluster that is implemented primarily for the purpose of providing high availability of services which the cluster provides. They operate by having redundant computers or nodes which are then used to provide services when system components fail. In normal case, if a server with an application crashes, the application will be unavailable until someone fixes the crashed server. HA clustering remedies this situation by detecting hardware/software faults, and immediately restarting the application on another system without requiring administrative intervention.

Other functionality is VMware Fault Tolerance (FT). It ensures the full functioning system despite the downtime of one or more production servers. The feature is a continuous availability solution for use with some virtual machines.

FT will enable a VM (Virtual Machine) to be protected with no downtime and no data loss due to a hardware failure. FT allows for a VM to have a secondary copy running simultaneously on a second ESX host which is executing every instruction and every input in lockstep with the primary VM. In the event of a failure, the secondary VM becomes the primary within a matter of seconds, while preserving state and without disconnecting any connections to the virtual machine. All traffic is redirected to the secondary. In addition, once the secondary assumes the role as primary, it spawns a new secondary instance on another ESX host and brings full fault tolerance back to the virtual server. Functionality called VMware vMotion eliminates the need for planning application downtime due to scheduled server maintenance through live migration of virtual machines between servers without interruptions or loss of service users [2], [3], [10].

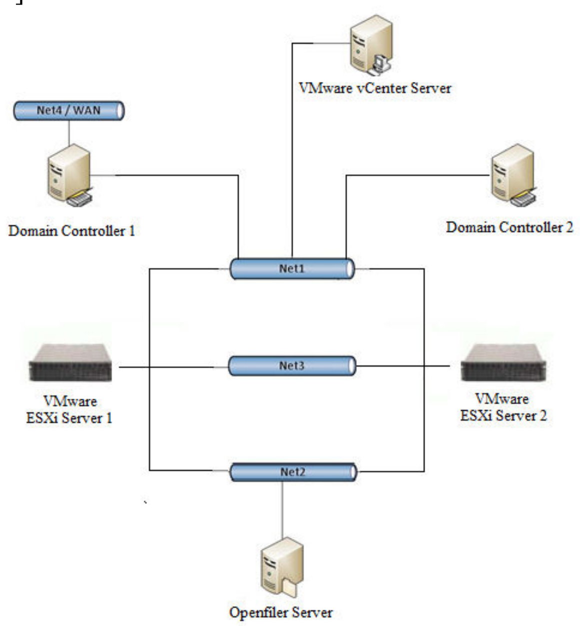

Fig. 1 Example of High Availability Cluster in Laboratory

This platform supports a VSA (vSphere Storage Appliance) which is a way how to provide shared storages without any need to purchase a physical SAN or NAS. It combines storages directly attached to two or physical servers and combines it into a single (iSCSI) storage pool. vSphere Storage Appliance runs on multiple servers simultaneously, so you can have the confidence that data is available to any of your workloads, even when a server fails. With vSphere's availability features, we can restart virtual machines automatically when a server fails, use fault tolerant protection so applications run uninterrupted, and perform maintenance with zero impact to the end user by migrating applications live from one server to another using vMotion.

3 SCADA/HMI systems and building virtual architecture

Like it was said in introduction we have few real and virtual models in laboratory. Models like Intelligent House, Ball in Tube, Magnet etc. All of those models are directly controlled by PLC's and supervisory controlled by client through HMI which is, in fact, visualization of controlled system. Supervisory control is only one part of functions of SCADA system, another is data acquisition which means the data collecting form production (models, sensors, sub-systems) and provide them to higher layers (management, information systems). All applications were running on different physical machines with their own storages and databases and some were sharing the same machine. Physical machines were in fact servers. Applications which use the same server for behavior, can invade each other, for example because of updating one of the applications CPU (Central processing Unit) usage is at hundred percent, etc. The risk is greatly reduced by dividing the applications onto different virtual computers. Virtualization gives flexibility, so the operating system does not depend on particular piece of hardware. It is not necessary to build a 'final solution' because systems can be expanded on the fly, without influence to operated services [4], [6].

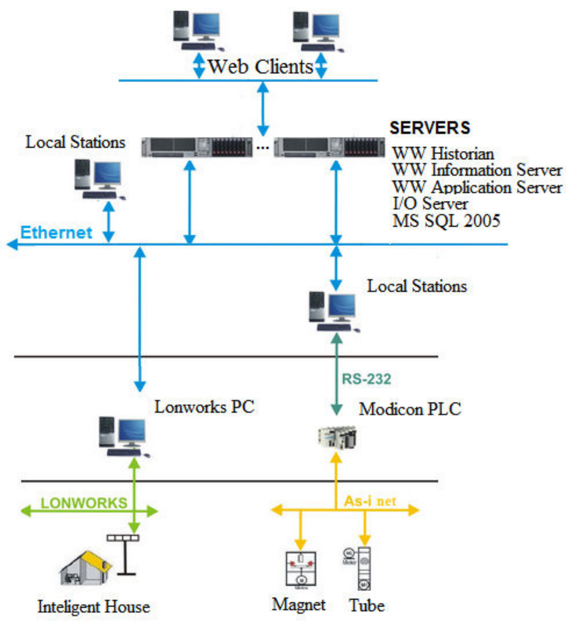

Fig. 2 Initial architecture in laboratory

ISBN: 978-1-61804-108-1

Virtualization also offers the ability for creating the duplicate of servers that where one is for development and for deployment for specific applications and the second is for runtime and also for demonstration and promotional purposes.

3 Problem Solution

First of all, by the analysis of the laboratory environment we‘ve found that the most risky point of infrastructure are servers on which are installed services that are necessary for running the laboratory. That’s the problem with few our servers (Wonderware Information Server, Factory Talk View Point Portal, databases), if failure occurs on some of them, we lose access to the model management and databases and this is unacceptable. First of all we had to install new basic infrastructure, with three ESXi hosts (147.232.61.61, 147.232.61.71, 147.232.60.126) and vCenter Server (147.232.61.34) through which we can administrate all hosts and virtual machines. All virtual machines will be installed on ESXi hosts. Now, because we wanted our server to be as available as possible, we had to install High Availability cluster. For proper functioning of the HA cluster (High Availability) it‘s necessary to ensure that the data of individual virtual machines installed on production ESXi Servers were stored independent of these servers, because if virtual machine failure occurs, data from virtual machines will be unavailable and it won‘t be able to start the virtual machines on the other ESXi server [10]. We’ve made three solutions here:

First solution was the iSCSI data storage server built with Openfiler 2.99 software that is running in separate virtual machine.

Second solution was connection between two laboratories, where in second is SAN (Storage Area Network) storage. Connection was realized through NFS (Network File System). This server has, in comparison with other mounted file storage, faster data access, easier management and configuration.

Third solution consists in using the VMware VSA (vSphere Storage Appliance). It combines storages directly attached to two or physical servers and combines it into a single (iSCSI) storage pool. This solutions has a few requirements like VMware vCenter Server, 4 NICs (Network Interface Card) and local storages in Raid 10 configuration. The vCenter Server is running in virtual machine so it must not run on any of ESXi hosts that are hosting the VSA appliance. In other words it must not be within the same Cluster as VSA appliances. We’ve decided that Raid 10 configuration, (only supported) is a bit minus and ineffective because of local storage capacity loss. For testing of this solution was used virtualized environment. It means that we’ve installed virtual ESXi servers (vESXi, 147.232.61.143, 147.232.61.144) on our physical ESXi server and installed the VSA. We’ve made new VSA cluster and all necessary virtual machines were installed on vESXi.

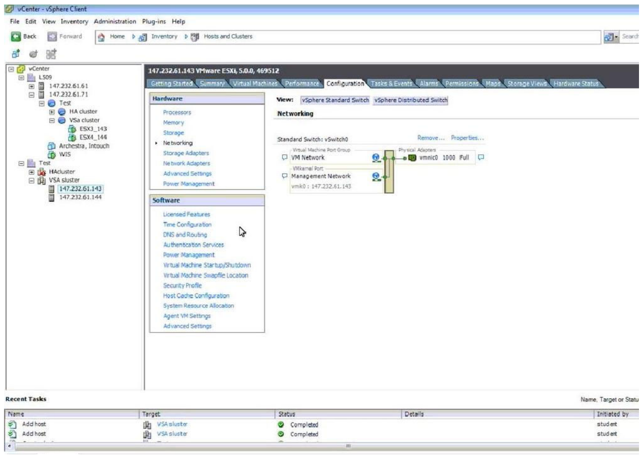

Fig. 3 VSA cluster in VMware vCenter Server

Other requirements for installation of High Availability cluster were installation of Domain controllers, installation of hypervisors, and installation of VMware tools, vMotion, and vStorage and distributed virtual switch. The vMotion functionality provides a migration of virtual machines real-time between ESXi hosts with the minimum connection outage. For this purpose we had to add a new network interface, through which the ESXi host communicates during migration of virtual machines. The distributed virtual switch centralizes and controls the virtual network infrastructure between virtual machines and data storages. The problem is in usage of tens of virtual machines, data storages and usage of migrations of virtual machines, where all of this traffic can make a mess in network infrastructure. Again we’ve made two concepts. The first was virtual High Availability cluster, where everything that we needed physical was virtualized. So everything for High Availability cluster creation, like two ESXi servers, iSCSI data center and domain controllers, were virtual machines, running on one vESXi server which is on physical ESXi server. After testing this solution we’ve made second concept with physical ESXi servers [6], [11], [12].

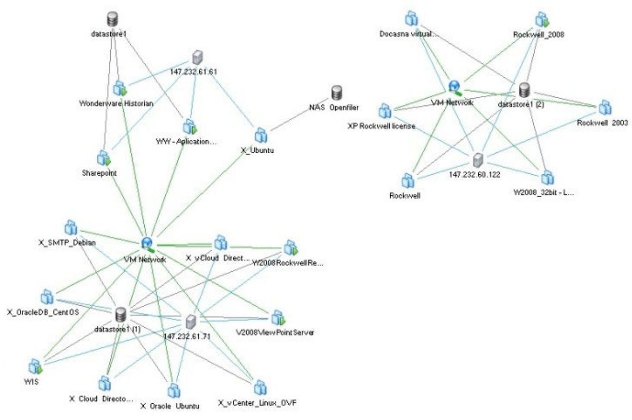

Fig. 4 Map of infrastructure in vCenter Server

Now after we've created a High Availability cluster, we've installed our virtual machines. A part of them are production servers running in virtual machines and the other, bigger, part are virtual machines for testing purposes (developing environments, testing environments). Now we could use the High Availability functionality which minimized downtime of virtual machines, even after the hardware failure of one of the ESXi servers because virtual machines are automatically started on the other ESXi servers. After that we wanted to apply the Fault Tolerance (FT) functionality on our selected server (Wonderware Historian). We had to be sure that VMware High Availability feature is allowed on this virtual machine. After turning on the FT functionality a copy of our server on the other ESXi host has made. FT uses the vMotion for the transfer between these two virtual machines. So the Wonderware Historian is on ESXi host 147.232.61.61 and its copy (secondary) is on ESXi host 147.232.61.71. These functionalities made our servers very available, reliable and stable, which are the requirements for our SCADA/HMI systems running on virtual architecture.

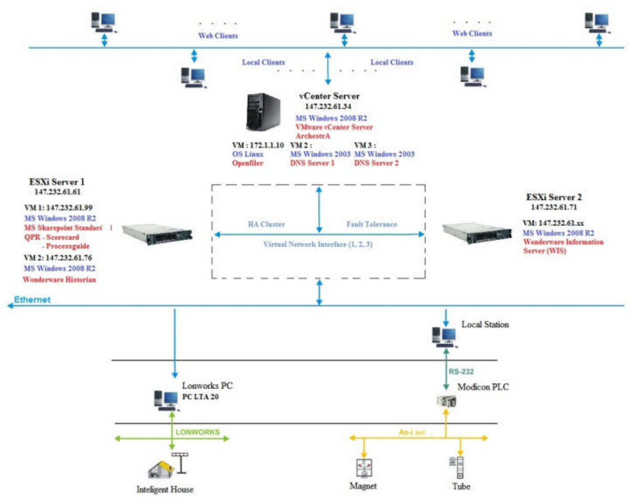

Fig. 5 SCADA/HMI systems running on new architecture built via VMware vSphere 5.0 platform

4 Conclusion

New built virtual architecture brought a lot of benefits for our laboratory and department. We have highly available, stabile and reliable architecture, built via VMware vSphere 5.0 platform, which enrich the matter of security of our SCADA/HMI systems and made them safer. Research and work on architecture building brought new perspective on some form of security of our SCADA/HMI systems. Engaging in high-availability cluster minimized downtime of virtual machines, even after the hardware failure of one of the ESXi servers, because virtual machines are automatically restarted on the other ESXi server, by means of vCenter High Availability feature. Testing of vSphere Storage Appliance and Openfiler software was possibility to solve problem with shared data storage, because it is a way how to provide shared storages without any need to purchase a physical SAN or NAS. Virtualization technology has now become a part of department and laboratory and it is a big addition in supporting aging HMI/SCADA technology and applications. We have designed and implemented a new hardware, network and software architecture in the laboratory using VMware vSphere 5.0 Platform and virtualization benefits, which were applied in a complex hierarchical information-control system with emphasis on control level HMI/SCADA.

5 Acknowledgments

This publication is the result of the project implementation Development of Centre of Information and Communication Technologies for Knowledge Systems (project number: 26220120030) supported by the Research & Development Operational Programme funded by the ERDF (30%) and KEGA 021TUKE-4/2012 project (70%) and VMware Global Education and Research Programs

References:

[1] Bottomley, J, *The Risks of Over-Virtualization - why virtualization is not high availability*, International LinuxWorld Magazine, 2006.

[2] Božek, P., Barborák, O., Key benefits of virtual technology, *Intellektual'nyje sistemy v proizvodstve*, Vol. 15, No. 1, 2010, pp. 115-119.

[3] Clark, C., Fraser, K., Hand, S., Hansen, J. G., Jul, E., Limpach, C., Pratt, I., Warfield A., *Live migration of virtual machines*, Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation, 2002.

[4] Franeková, M., Rastocny, K., Safety evaluation of fail-safe fieldbus in safety related control system, *Journal of Electrical Engineering*, VOL. 61, NO. 6, 2010, pp. 350-356.

[5] Landryová, L., Babiuch, M., Fojtík, D., Challenges and Software Aspects in Engineering Education, *The 9th IFIP World Conference on Computers in Education*, 2009, pp. 143-204.

[6] Pavlík, M., Karch, P., Miháľ, R., An industrial information portal based on Virtualized Web Server, *Scientific Conference of Young Researchers of Faculty of Electrical Engineering and Informatics Technical University of Košice*, 2011, pp. 225-228.

[7] Pavlík, M., Zolotová, I., Hošák, R., Benefits of virtualization in HMISCADA systems, *System Theory and Control proceedings of the 14th International Conference SINTES14*, 2010, pp. 379-384.

[8] Sarnovský, J., Liguš, J., Reliability of Networked Control System Using the Network Reconfiguration Strategy, *Acta Electrotechnica et Informatica*, 2011, pp. 58-63.

[9] Sutiene, K., Vilutis, G., Sandonavicius, D., Forecasting of GRID Job Waiting Time from Imputed Time Series, *Electronics and Electrical Engineering*, Vol. 114, No. 8, 2011, pp. 101-106.

[10] Zolotová, I., Pavlík, M., Building a High Availability Solution in Laboratory Environment, *Management Science and Engineering*, 2011, pp. 621-625.

[11] http://www.vmware.com/pdf/vmware_ha_wp.pdf

[12] http://www.vmware.com/products/vsphere/small-business/overview.html