

# The IT Infrastructure's Industrialization and Mastering

Z. Bakraouy, W. Abbass, A. Baina, and M. Bellafkih

National Institute of Posts and Telecommunication, INPT, Madinat Al Irfane, Rabat, Morocco

Email: {zineb.bakraouy, wissam.abbass}@gmail.com; {baina, bellafkih}@inpt.ac.ma

**Abstract**—Time and resources are currently under an increasing pressure. As a result, the installation and configuration of new equipment requires a solution that would provide automation for all types of content and portable platform. In fact, as the size of the IT infrastructure increases, the installation activities of desktops and their maintenance would grow proportionately, making it thus difficult to maintain the organizations' Information System (IS) in terms of hardware and software. Incident Management (IM) handles all incidents reported by users through the service desk, technical staff and monitoring. However, not all incidents are similarly critical. Some parts of the IS are actually vital to the business, for example: databases, mail servers, applications, software. The main purpose of this paper is to keep the real-time IS in production and reduce the impact of incidents on the information system.

**Index Terms**—Computer park management; System Center Configuration Management; SCCM; System Center Service Management; SCSM; GLPI; incident management

## I. INTRODUCTION

The IT infrastructure has become key element for any organization [1]. Accordingly, the Service Level Agreement (SLA) negotiation and monitoring are also becoming more and more necessary [2]-[4]. As System Information (IS) grow into more complex systems [5]-[7], their Security, location management and monitoring grows into a more difficult task for the network and system administrator. An administrator must know at any time the state of each equipment and service of the organization's IT infrastructure in order to always provide a high reactivity. Monitoring activities are used to monitor, analyze, alert and act on the normal and abnormal events of the different ISs in production. Moreover, it consists of monitoring the state of the entire IT infrastructure, servers and ISs to anticipate the various incidents and thus quickly diagnose a failure. Today's IM focuses on handling all IT incidents throughout their lifecycle [8], [9]. IM mission is to ensure that the services' normal operations are in accordance with the contractual commitment and that in order to guarantee an efficient service levels.

The implementation of an IM process is an essential step in order to allow:

- Reactivity where users would quickly reach a technician for help. This will allow less waste of time for the user's requesting help and for the technician offering the help.
- The technician's efficiency: it will not be disturbed during a planned activity.
- The capitalization of knowledge [10]: if an incident has been recorded, in case of new occurrence of this type of incident, service technicians know what needs to be done and will save time in handling the incident.
- The prevention: it will be possible to correctly identify a minor incident before that it becomes critical and that this leads to a crisis situation [11]-[13].

IM is a process that consists a part of IS management, including the ITIL17 [14] best practice set. ITIL is a set of best practices, procedures and methods that serve as guidelines for improving the management of services in the IT environment. Depending on its organization, business, size and strategic objectives, the company will implement, in whole or in part, the processes described in ITIL. ITIL Best Practices: In general, information technologies can be very complex. In fact, in order to manage this complexity, it is important to define clear, consistent and well-defined processes. ITIL helps to identify, improve and document the implemented processes which can result in an improved organization of the company. ITIL is a collection of widely used best practices that derive from the expertise and experience of its contributors and members of the ITSM community [15]. This makes it an evolutionary repository based on practical experience. More specifically, ITIL is a structured collection of advice and recommendations focused on customer service. Finally, it is open and fits well with other industry standards [16] (CMMI [17], PMBOK [18], COBIT [19], etc.). It is kind of the core of service management.

In this paper, we provide an overview of the IM an IT infrastructure, then System Center (SC) [20] that is the approach adopted in the platform to expose the High Availability. Of the IT infrastructure based Industrialization, and Mastering of the computer park. The paper is organized as follows: Section II is dedicated to Background, the IM tools. Section III presents the IT Infrastructure's Implementation of the Industrialization and mastering approach (configuration, monitoring and IM) and we discussed it, eventually in Section VI we draw our conclusions (see Fig. 1).

---

Manuscript received April 1, 2019; revised September 1, 2019.  
Corresponding author email: zineb.bakraouy@gmail.com.  
doi:10.12720/jcm.14.10.884-891



Fig. 1. Best practice ITIL [14]

## II. BACKGROUND

There is a set of software with the function of remotely managing the computer park of an organization. These programs have several functions:

- Allowing the IT departments to manage remotely their entire network without the need to send a speaker, reducing thus intervention costs and delays.
- Inventory tools in order to better manage the organization's IT grow.
- Preventive actions that would avoid computer malfunctions.
- License management reducing the cost of the unused software.

These functions are not distinct but are related. The economic aspect plays in favor of such applications but however require a heavy investment, due to their high prices. Inventory tools make it possible to better understand the organizations' grow also allows knowing precisely the number of computers connected to the network, their hardware and software configurations and their dates of installation. Thus, making it possible to follow the machines by monitoring their evolution.

Open Computers and Software Inventory Next Generation offers the inventory of IT infrastructures. This application makes it possible to precisely inventory hardware and software in an efficient way. It also allows the broadcasting and managing applications directly via an internet browser and interfaces with other applications such as GLPI [21]. This application is released under GNU GPL license and thus inexpensive to set up.

GLPI (Free Management of Computer Park) is a free management solution of Computer Park and Service Desk which is released under GNU GPL license. It provides a knowledge base for managing the incident tickets of the hardware and software. A web interface is included in order to manage the organization grow through an inventory solution type "OCS Inventory NG" [22]. It is an inexpensive and easily implemented solution. GLPI is a Full Web application developed in PHP, it presents various functionalities: From a general point of view, it allows a multi-park management and a management of the criteria of the objects' uniqueness. Under its Web interface is a database in SQL format for backing up and restoring data (data can be exported in various formats:

PDP, CSV, SLK, PNG, SVG, XML). This configuration allows the inventory of computer fleets (internal peripherals, disk space...), monitors and printers with management of consumables and connections to computers, network hardware with management of connections to peripherals, Software Park with license management and expiration date and reservations for inventory equipment.

Integrated virtualization management and management solution for mid-sized businesses or organizations providing:

- A single administration console for workstations, servers and applications.
- Software and hardware inventory.
- The distribution of software and updates (OS, applications and drivers).
- Workstation and server monitoring through the integration of System Center Operations Manager.
- Collection of incident notifications and problem solving.
- Complete management of virtualized environments by integrating System Center Virtual Machine Manager.
- Activity and monitoring reports, customizable.

System Center Configuration Manager (SCCM) [23] is an IT asset management solution (change management and configuration) that provides inventory (hardware and software), application delivery and security updates, remote support of workstations and servers, in traditional or virtualized environments.

System Center Operations Manager (SCOM) [24] is a monitoring solution that optimizes the administration and operation of Windows, Unix and Linux environments by offering:

- Complete collection of events and performance counters.
- Monitoring of these elements and proactive alerts.
- Reporting and trend analysis features.
- Tasks and knowledge specific to certain systems or applications, through management packs (for Microsoft environments or other providers).
- Management of physical or virtual environments in the same console.

The objectives of the SCOM deployment for an organization are:

- To stay informed about the state of servers, applications and workstations.
- To improve the efficiency of IT operations through proven practices built into management packs.
- To generate service level and performance reports to help analyze the operating status of the information system.

System Center Service Manager (SCSM) [25] is an offer (available in the first half of 2010) to automate user support processes, incident and problem management, as well as configuration management, changes in regulations and conformity to them. SCSM 2010 uses and aggregates information contained in Active Directory, System Center Configuration Manager 2007, and System Center

Operations Manager 2007, and integrates ITIL and Microsoft Operations Framework (MOF) process automation best practices. System Center Service

Manager can significantly reduce the number of support calls (see Table I).

TABLE I: COMPARATIVE OF IT INFRASTRUCTURE MANAGEMENT TOOLS

	GLPI	GLPI/OCS	SC
Entreprise	INDEPNET.org		Microsoft
Version	0.83	2.0.5	2012/2016
Technician service	Yes ( all tasks)	Yes (all tasks)	Yes (Among of tasks)
Deployment Model	Client Server	PHPMyAdminSQLite Manager	MAS
Licenses	Open Source / Free	GNU version 2.0	Part Free/Part Proprietary
Free Try	Yes	Yes	Yes

### III. MANAGEMENT OF THE COMPUTER PARK USING SC

Using the Internet allows organizations to open their computer equipment to their partners and suppliers. The IT infrastructure is a collection of hardware and software resources available to a company in the automated processing of information. Several tools were used to monitor applications but did not provide a consolidated view of the situation and often incidents were reported by users before the consoles gave the alert. On the other hand, no reliable inventory of applications and software was available. To ensure the monitoring and sustainability of its resources, organizations must conduct an efficient management of the IT equipment. In one hand, this task allows listing and locating the equipment of the organization. On the other hand, it tolerates performing maintenance tasks and assistance to users. A qualified person can perform these operations, but often this work is beyond his or her competence. To overcome this, it is necessary that one or more tools be set up within the company to have regular monitoring of the computer and sometimes anticipate the failure of its resources.

#### A. Industrialization and Mastering of the IT Infrastructure

SCCM provides a holistic solution meeting the infrastructure's large size and its needs. Indeed, large organizations need to deploy a master of more than 500 machines to deploy. SCCM is a Microsoft cost-effective solution that ensures a complete follow-up answers to the needs of large organizations. It allows customizable system image deployments where the final OS can be fully shaped and to also incorporate different sequences tasks that allow configuring the operating system as a whole like the management of the Windows license, the addition to the active directory, the pre installation of drivers, different passwords or updates.

Once these task sequences are done, SCCM allows booting by PXE and massive deployment thanks to multicast without intervention of a technician since the control can be done from the SCCM console. Deployment via PXE is fully controllable through the

dashboard provided by SCCM and these different monitoring points. Subsequently these task sequences offer flexibility as it is easy to modify, delete or add a deployment rule. There is also the possibility to manage the software that we want to incorporate into our operating system that can be done at the same time as the deployment for example generic applications to any system or after deployment using the software center that allows you to add software and manage software versions and their own updates. SCCM also includes an entire dashboard system that probes and has indicators on all the actions that SCCM produces but also to know their states, it is also possible for the administrator to create these own queries and reports. Therefore, there is also an entire inventory and fleet management environment. It searches and locates all devices (servers, client PCs, and smartphones) connected to your network through Active Directory and installs the client software on each node. It creates an inventory database with records of each resource, installed software, and hardware characteristics. It uses this data to direct application deployments to device groups or users.

The main features of SCCM are:

- Deploy operating systems, software applications and software updates.
- Monitor and correct computers to apply compliance settings.
- Monitor hardware and software inventory.
- Manage computers remotely.

For the correct operation, Configuration Manager needs at least:

- An application server
- A SQL Server database
- A customer

For designing a "clean" architecture, the best is to have two servers, one as a domain controller, where there will be the Active Directory and the DNS and the second where will be the database and the application Configuration Manager. The specificity of Configuration Manager is the site boundary that defines the perimeter that must physically be managed by an SCCM site. When you assign an SCCM site boundary to a site, it is a way to

define what it will handle. There are also distribution points that are specific to SCCM, distribution points are a site system role that acts as a relay for clients to access content / sources (applications, updates, packages, operating system...).

SCCM needs a number of prerequisites for installing a stand-alone site, which are:

- Creating a System Management container at the root of the domain and delegate its administration to the Configuration Manager server
- Extending the Active Directory Schema on the Domain Controller
- Setting security permissions on the System Management container
- Enabling Active Directory Publishing for the Configuration Manager Site
- Installing SQL Server on the second server

SCCM allows creating an operating system image by importing install. wim file into the Software Library. Relate to Fig. 2.

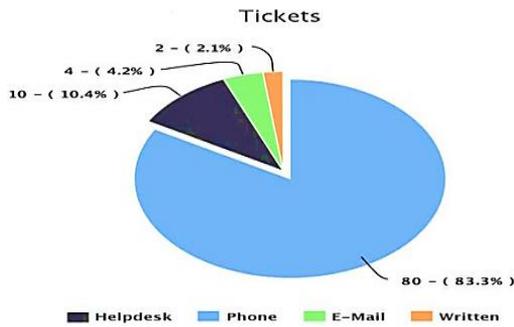


Fig. 2. Tickets' status

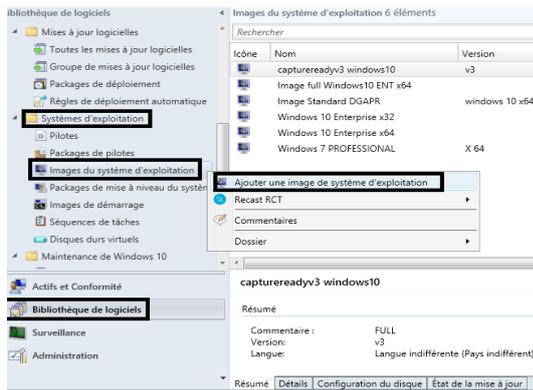


Fig. 3. Image of the OS

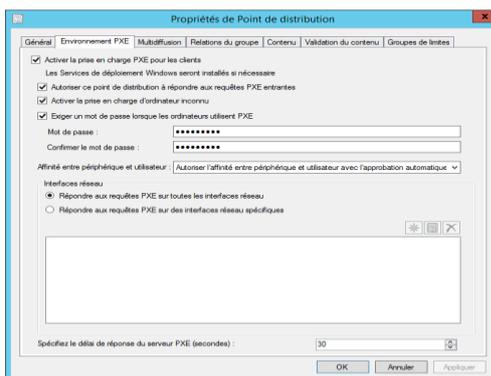


Fig. 4. Properties of point of distribution

Then, the server responds to all PXE requests on all these network interfaces as depicted in Fig. 3-Fig. 4. We have also set a delay of 30 seconds to check information during boot.

SCCM manages the notion of subnets and is based on the network identifier. Moreover, it allows creating groups of limits that will serve two functions:

- Defining the assignment of a customer based on its location to an SCCM Site. This configuration is necessary when automatic site assignment is used so that the client can correctly switch to the site to which it belongs.
- Using the needed content for deployment. For example, one or more distribution points or one or more points of migration of the user state.

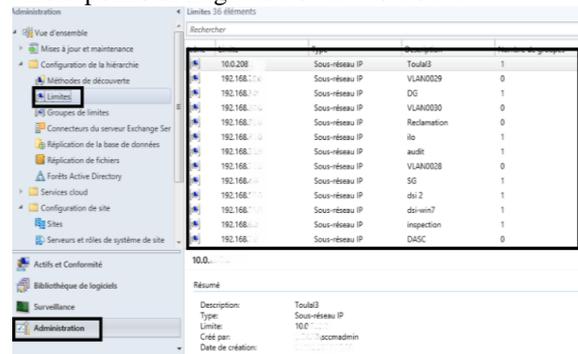


Fig. 5 Subnets of network

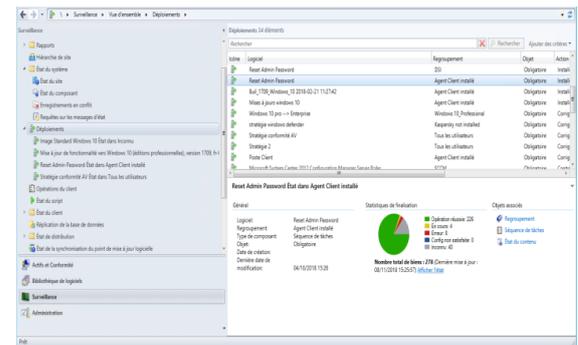


Fig. 6. Sequence task created

Grouping allows restricting the application of tasks. As shown in Fig. 6, 527 entities are mastered entities on SCCM (see Fig. 7).

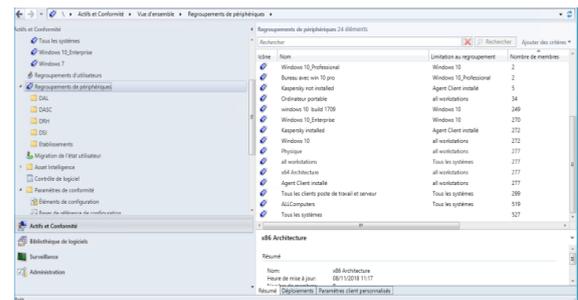


Fig. 7. Grouping

B. Monitoring

SCOM which is a monitoring allowing immediate reactions and remedies. Thus, ensuring optimal

functioning of the IT infrastructure. It also facilitates the management of an IT infrastructure. The features of SCOM are as follows:

- End-to-End Service Monitoring Operation Manager that monitors applications, infrastructures and user's satisfaction to manage services throughout their lifecycle.
- Microsoft Operation Manager Knowledge Base which leverages the knowledge of Microsoft's Server, Client, and Application teams in order to accelerate problems' resolution.
- Reliability and secure operations ensuring the smooth operation of IT departments and applications.
- Operational Efficiency representing an integrated and interoperable solution, aiming at simplifying the administration of the IT infrastructure.

SCOM is based on the principle of a program called "agent" which is installed on different machines in order to be supervised. This agent sends relevant information to the monitoring server and scans multiple sources of information, such as the logs, performance counters and application-generated codes. The supervision server keeps the information in a database which allows having the history of the alerts. Actually, when alert conditions are largely met, the server raises alerts. It comprises a filter mechanism that allows filtering and analyzing the arrival of different information. Rules based on the context and the configuration makes it possible to send a notification (by mail, SMS, etc.). This generates tickets of incident and triggers an action in order to execute a script for example correcting the anomaly detected without intervention. SCOM relies essentially on "Management Packs" which contains a set of information rules necessary for the supervision of any type of application.

This display shown in Fig. 5 displays all active alerts (not closed). In this view, you can select an alert to display its details, such as the rule or analysis that generated the alert and the managed object that has the problem (see Fig. 8-10).

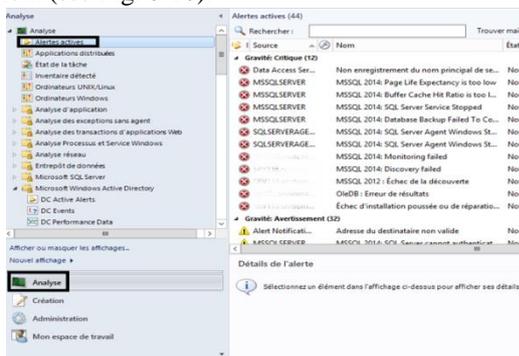


Fig. 8. Active alerts

SCOM allow as shown in Fig. 6 visualizing the dashboard:

- Server RAM
- CPU servers
- Server disk space
- Network

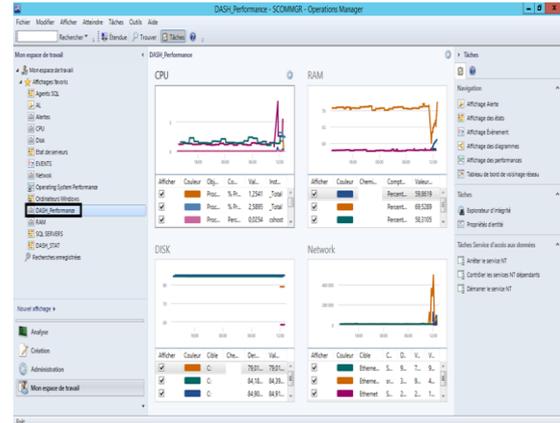


Fig. 9. Dashboard of SCOM

The Synchronization of Software Updates is necessary for the good implementation of the Updates.

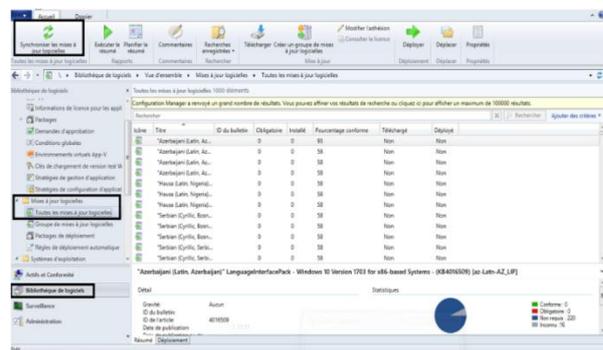


Fig. 10. Software updates

### C. Incident Management

System Center Service Manager (SCSM) is an integrated platform automating and adapting best practices for the organization's IT management. The solution is based on the ITIL V3 standard. SCSM includes processes for IM and problem resolution, change control, and IT lifecycle management. Quick tour of native SCSM features:

- IM (helpdesk)
- Problem Management
- Management of change requests
- Portal for creating and monitoring incidents / requests for end users
- Analytics portal for helpdesk operators and anyone involved in IT change requests
- A complete Dashboard that can be integrated into a SharePoint site
- Creating custom reports with SQL Server Reporting Services
- SCSM relies on SQL Server
- SLA Management

Ticketing is the key to resolve the incident. We chose to determine the impact of an incident that is calculated according to criteria defined in the service contract (SLA) according to a minimum of three levels:

- High: a large number of users is impacted or it is a major application that is concerned.

- Middle: a limited number of users is impacted or it is a standard application that is concerned.
- Low: only one or very few users are impacted or it is an office application that is concerned.

SCSM allow us to create tickets by two ways: From the console of SCSM or from the Portal which is installed in IIS Server: (see Fig. 12-14).

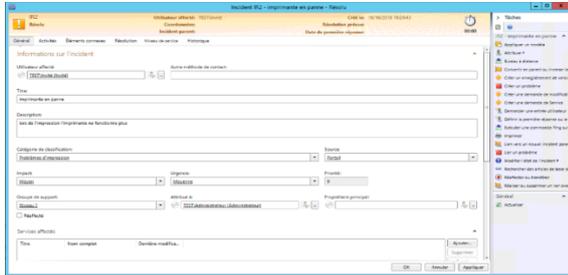


Fig. 11. Template of Ticket

The Configuration Management Database is a pillar of a good information system it is recommended by ITIL. SCSM give as a base of knowledge to build the CMDB:

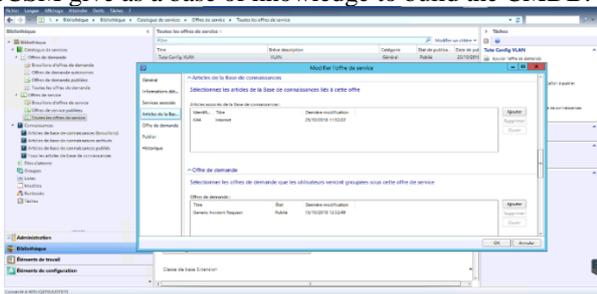


Fig. 12. Base of Knowledge

The IM is based on Time. We must act on the indicators observed in order to better control the maximum time to resolve major incidents and better respect SLAs. An indicator measuring the customer satisfaction rate that will be evaluated through the SCSM tool once the ticket has been closed by the user who declared the incident where the technician who solved it.

SCSM has two metrics:

- Completion Time defined when the service is requested,
- Resolution Time defined when the Help Desk validates the ticket.

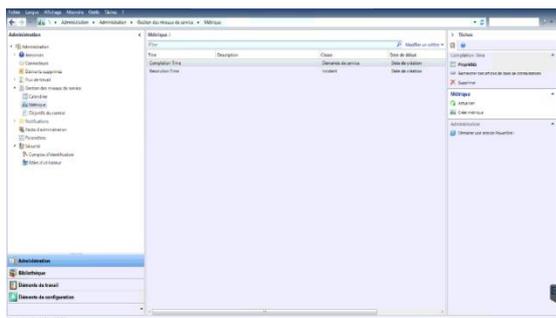


Fig. 13. Metrics of SCSM

SCSM has given us the option to make a Portal which has served us as communication interface to directly generate tickets from users.

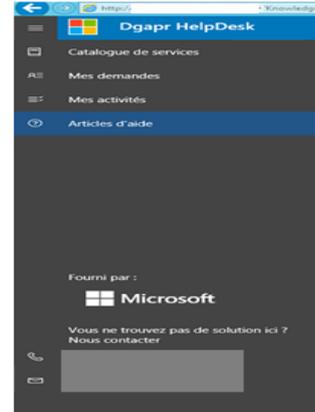


Fig. 14. Portal of SCSM

#### IV. CONCLUSIONS

In this paper we have acknowledged an implementation of IT Infrastructure industrialization and monitoring based on a managing software and tool. It has allowed users to proceed via a dedicated interface, to state the malfunctions of their workstation.

For general users:

- A provision of a user portal to create and track their incidents and requests for service and to inform them of the planned changes in their IT environment,
- Provision of self-help solutions.

For employees of the Information Systems Directorate (ISD):

- Management of the incidents detected by the users;
- Setting up a knowledge base to share incident resolutions and failures within the ISD, reduce their resolution times, and sustain the knowledge;
- Management of the components to permanently inventory the means installed computers (hardware and software), their interactions (database management configuration) and the link with service commitments made by the ISD

So we can conclude by report of the benefits of this solution as below:

- High availability, solution reliability
- Secure and standardized infrastructure to adapt more quickly to changes
- Simplification of infrastructure management
- Speed of implementation in the face of changes
- Reduced delivery times
- Flexibility and elasticity in adapting to needs
- Ability to measure the quality of service
- Disinclusion between technologies and materials: no longer adhering to aging technologies by using virtualization techniques
- Reduced need for physical equipment to reduce the cost of ownership (network, storage, servers)

## REFERENCES

- [1] M. D áz, C. Mart ín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing," *Journal of Network and Computer Applications*, vol. 67, pp. 99-117, 2016
- [2] Z. Bakraouy, A. Baina, and M. Bellafkih, "System multi agents for automatic negotiation of SLA in cloud computing," in *Proc. Innovations in Bio-Inspired Computing and Applications (IBICA) Advances in Intelligent Systems and Computing*, Morocco, 2017, pp. 234-244.
- [3] Z. Bakraouy, A. Baina, and M. Bellafkih, "Autonomous SLAs negotiation based on Agreement-Broker: Services availability," in *Proc. 5TH Edition International IEEE Congress on Information Science and Technology (CIST)*, Morocco, 2018, pp. 48-53.
- [4] Z. Bakraouy, A. Baina, and M. Bellafkih, "Availability of web services based on autonomous classification and negotiation of SLAs," in *Proc. 6th International Conference on Multimedia Computing and Systems (ICMCS)*, Morocco, 2018, pp. 1-6.
- [5] A. Botta, W. Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: A survey," *Future Generation Computer Systems*, vol. 56, pp. 684-700, March 2016
- [6] W. Abbass, A. Baina, and M. Bellafkih, "Survey on information system security risk management alignment," in *Proc. International Conference on Information Technology for Organizations Development*, Morocco, 2016, pp. 1-6.
- [7] K. Aziz, D. Zaidouni, and M. Bellafkih, "Real-time data analysis using spark and hadoop," in *Proc. 4th International Conference on Optimization and Applications (ICOA)*, Morocco, 2018, pp. 1-6.
- [8] S. Garg and A. Misra, "Automation of incident management processes and benefits of hosting servers on cloud," in *Proc. IEEE International Conference on Current Trends in Computer, Electrical, Electronics and Communication (ICCTCEEC)*, Mysore, India, September 2017, pp. 1-6.
- [9] Z. Bakraouy, W. Abbass, A. Baina, and M. Bellafkih, "MAS for services availability in cloud of things network: Monitoring and reactivity," in *Proc. 12th International Conference ON Intelligent Systems: Theories And Applications (SITA)*, Morocco, 2018 (Under Publication)
- [10] A. Q. Gill and E. Chew, "Configuration information system architecture: Insights from applied action design research," *Information & Management in Press, Corrected Proof*, 2018
- [11] W. Abbass, A. Baina, and M. Bellafkih, "Improvement of information system security risk management," in *Proc. 4th IEEE International Colloquium on Information Science and Technology*, Morocco, 2016, pp. 182-187.
- [12] R. Baskerville, P. Spagnoletti, and J. Kim, "Incident-centered information security: Managing a strategic balance between prevention and response," *Information & Management*, vol. 51, no. 1, pp. 138-151, 2014.
- [13] W. Abbass, Z. Bakraouy, A. Baina, and M. Bellafkih, "Classifying IoT security risks using deep learning algorithms," in *Proc. 6th International Conference on Wireless Networks and Mobile Communications*, Morocco, 2018, pp. 1-6.
- [14] J. Quesnel, "Comprendre ITIL 2011: Normes Et Meilleures Pratiques Pour Evoluer Vers Iso 20000," Éditions ENI, 2012
- [15] R. Gupta, K. H. Prasad, and M. Mohania, "Automating ITSM incident management process," in *Proc. 5th Int. Conf. Auton. Comput.*, 2008, pp. 141-150.
- [16] J. Aguiar, R. Pereira, J. B. Vasconcelos, and I. Bianchi, "An overlapless incident management maturity model for multi-framework assessment (ITIL, COBIT, CMMI-SVC)," *Interdisciplinary Journal of Information Knowledge and Management*, vol. 13, pp. 137-163, 2018.
- [17] F. S. Silva, F. Santana, F. S. F. Soaresac, et al, "Using CMMI together with agile software development: A systematic review," *Information and Software Technology*, vol. 58, pp. 20-43, February 2015
- [18] E. Karaman and M. Kurt, "Comparison of project management methodologies: Prince 2 versus PMBOK for it projects," *Int. Journal of Applied Sciences and Engineering Research*, vol. 4, no. 4, 2015.
- [19] ISACA, COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, 2012.
- [20] N. Naeem, Learning System Center App Controller, *Packt Publishing Ltd*, Birmingham, UK, 2015
- [21] GLPI. [Online]. Available: <http://www.glpi-project.org>
- [22] OCS. [Online]. Available: <http://www.ocsinventory-ng.org>
- [23] S. Martinez, P. Daalmans, and B. Bennett, "Mastering system center configuration manager," *Wiley/Sybex*, 2017.
- [24] J. Hernantes, G. Gallardo, and N. Serrano, "IT Infrastructure-Monitoring Tools," *IEEE Software*, vol. 32, no. 4, pp. 88-93, 2015.
- [25] L. T. Ellermann, K. Wilson, K. Nielsen, and J. Clark, "Microsoft system center optimizing service manager," *Microsoft Corporation*, 2013.

**Z. Bakraouy** born in Rabat. She obtained her DUT in 2012 at ENSET Rabat in software engineering and networks, and Bachelor's degree in 2013 at ENSET Mohammedia in computer system and network, then Engineer degree in 2015 at ENSA El Jadida in Telecommunications and Networks Engineering. She is currently in her fourth year of her PhD in networking studies at INPT Rabat. Her research interests center around the availability in critical infrastructures. Her current research is how to use Multi agent system for negotiation of SLA and to build an Available system: infrastructures, platforms and services.

**W. Abbass** was born in Rabat, Morocco. In 2012, she received her B.S. degree from the University of Science of Tetouan (USTC), in Software and network engineering and in 2014 her M.S. degree from the University of Science of Marrakech in Information systems security. She is currently pursuing a Ph.D. degree at the National Institute of Posts and Telecommunications (INPT) in Rabat. Her research interests

include Network security, software security, risk management and A.I

**A. Baina** received the PhD thesis in Computer Science from the University of Paris 6, France, in June 1994. His research interests are in the area of critical infrastructure, including: Critical Infrastructure, Electrical Grid, Critical Information Infrastructure, Information Security, and Access Control. He is Assistant Professor in computer science At «National Institute of Posts and Telecommunications», in Department of Mathematics, Computer Science, and Networks (MIR), Rabat, Morocco since 2010.

**M. Bellafkih** born in Oujda, Morocco. He received the PhD thesis in Computer Science from the University of Paris 6, France, in June 1994 and Doctorat Es Science in Computer Science (option networks) from the University of Mohammed V in Rabat, Morocco, in May 2001. His research interests include the network management, knowledge management, A.I., Data mining and Database. He is Professor in The National Institute of Posts and Telecommunications (INPT) in Rabat, Morocco since 1995. M. Bellafkih does research in Computer Communications (Networks), Information Systems (Business Informatics) and Software Engineering.