

ITSM Based Server Monitoring System

Swapnil Hiramani Sonawane^{1*}, Shruti Patil²

¹M.E. Student, Department of Electronics and Telecommunication Engineering, Shree. L.R. Tiwari College of Engineering Mumbai, India

²Professor, Department of Electronics and Telecommunication Engineering, Shree. L.R. Tiwari College of Engineering Mumbai, India

Abstract: Resource availability is one of the most important factors and requirements in the Business-Critical application. Technologies are required to increase the availability of the server and Business-Critical applications to deal with new services. This project proposed a more flexible scheme using ITSM lead to an efficient solution for Server Monitoring 24 by 7. The ITIL (IT Infrastructure Library) publishes guidelines provided on how to design, manage, IT support services. ITIL is the most wider used & recognized IT Service management ITSM framework. ITSM lays down the best practices that need to be implemented at the time-of-service support, such as IM (Incident Management) And PM (problem Management). ITIL holds a wide list of guidelines and process metrics. Servers being the core position of every business-critical application, this project showcases how to monitor servers through Agentless (WMI). We have use WMI (Windows Management Instrumentation) protocol to monitor the server resources such as CPU, Memory, Status and to collect the data, processes which can increase server availability, efficiency. The project outcome proved that successful integration to ITSM and server monitoring.

Keywords: ITSM, server monitoring.

1. Introduction

Technologic to increase the efficiency and productivity of server monitoring. Due servers deliver business-critical applications for their end-users. Such as SAP, Database servers, web application server, and many more. Availability and performance of each server are critical even one of the server fail, then a huge impact on business. Therefore, to monitor server performances and identify the failure component early stage and fix before turning in big threat to business. ITSM based server motoring help in motoring the entire infrastructure. It as well provides an intensive report on the last 24 hr, 7 days, 6 months on the capacity to maintain the servers without any impact.

ITSM based Server Monitoring is the operation of monitoring the server's system resources like CPU, Memory, Network, HDD, services, Port, etc. ITSM based Server Monitoring also helps in capacity and availability planning by monitoring the servers. ITSM based Server Monitor application helps in automating and self-healing the process of server monitoring. Server performance monitoring also helps to identify status application downtime and response time.

Why is it important to Monitor Server performance?

- To Improve the server availability & performance.
- To prevent the incident, happen & reduce server downtime.
- To improve server capacity & load monitoring.
- To detect and prevent any issues, self-healing capability.

ITSM (Information tech. service management) is used by the organization to plan, operate, design, control and deliver IT services offered to end-user.

Why is it important to IT Service Management?

- It Provides a Clear output by Individual Contributions and Business Results.
- It Creates a business Structure
- It is an enabler of Self-Service and Self-Help.
- It is an enabler of the Automation of Operational Activities.
- It is Helps to Identify Improvements areas

The core part of the IT Service Management Service Desk

A Service Desk is a primary function area defined by the ITIL, it is a single point of contact for both end-users and IT staff. The service desk satisfies the objectives of a business.

2. Incident Management Process

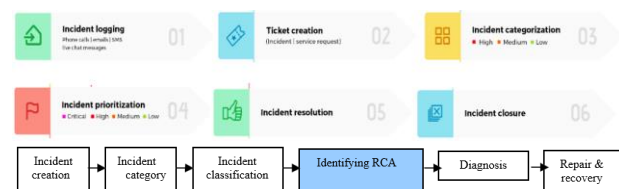


Fig. 1. Incident management work flow

Incident Management aims to quickly identify the root cause and as quickly as resolve the incident and affected server need to as normal.

Figure 1 shows the IM workflow which can be used to resolve the incident. Typical incidents reported to service desk either by monitoring tool automatically generated by server monitoring or by end-user.

In this paper, we are considering server monitoring incidents only. The incident record is classified for various reporting purposes such as urgency, impact, Assign to, etc. Then failed component identified by Service desk Eng. associated hardware

*Corresponding author: swapnilhsonawane@gmail.com

or software responsible for the incident. L1, L2, L3 support Eng. work on the incident and resolved the problem. After resolving the problem incident ticket will be closed and informed to the server monitoring team. In this paper, we propose techniques to automate and improve various Server motoring with help of ITSM. We describe our approach with the help of an example and outline our contributions.

3. Server Monitoring

In the current era of increase in computer infrastructure and size, the network has become a major component to communicate for day-to-day life. So network monitoring developed rapidly but, on the server, no adequate attention was given. In this paper, we introduce a server monitoring system, which not only monitors the hardware and software of the system but also monitors the security of the server’s information.

At present, there are two types of server management protocol in the server management field One is common WMI - Windows Management instrumentation, which is proposed by Windows. And the other is SNMP. The two protocols are corresponding to two different management programs. WMI has become the most popular windows management protocol for its simplicity and scalability. Almost all of the windows server’s support WMI.

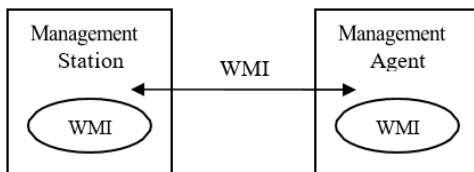


Fig. 2. The WMI-based management model

In Server Monitoring, two types of technologies are used to collect and monitor the availability and performance of devices.

Agentless Monitoring: In the Agentless model, a Proxy Server is installed to monitor other devices. The Proxy Server remotely accesses and pulls information from other devices. This type of monitoring requires no separate installation and is easy to deploy.

Agent-based Monitoring: In Agent-based model, the Agents

should be installed on all the devices and information about the device is collected and sent to the centralized Server. Every Agent communicates with the Proxy Server and the Proxy Server consolidates the data, posts the information to the centralized Server. This requires more installations. The http/s protocols should be open for communications to occur. There are two types of Agents, Wintel and Non-Wintel Agents.

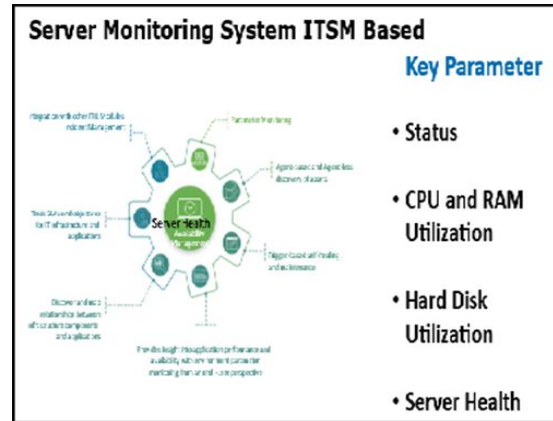


Fig. 3. Parameters sever monitoring

4. Architecture Design

Project designed to collect and monitor availability and performance data across your entire enterprise using agent-based or agent less technology. Operations Management is designed to monitor and analyze network performance. Operations Management enables to capture any failure in network, to regularize the maintenance tasks on the data center components whether they are on the premises or on cloud.

#	Attribute	Agent-based Discovery	Agentless Discovery
1	Ease of deployment	Requires installation of agents on each target system. Particularly difficult in large organizations which has various branches	No installation is required.
2	Breadth and depth of metrics	Monitors a wider variety of metrics. Provides deeper and more granular insights into inventory and performance of IT assets	Monitors relatively lesser variety of metrics. Provides relatively superficial insights into inventory and performance.
3	Resource overhead	Can consume a certain amount of computing resources on the target system. Performance of legacy or resource-constrained systems is impacted.	No resource overhead on the target system.
4	Network overhead	Network overhead is minimum	Uses up a larger amount of bandwidth
5	Network dependence	Dependency on the network is less. Some agents can operate even when momentarily disconnected from the monitoring station.	Always requires network connectivity
6	Expandability	Advanced Capabilities can be encapsulated within the agent	No such capability
7	Maintenance	Involves occasional patching, discovering, and troubleshooting of agents on the target system side. Particularly difficult in a large organization which has various branches.	No maintenance issues.
8	Governance issues	For deploying agents in certain organizations, approval might be required from a higher authority.	No approval issues.

