Network-based modeling and intelligent data mining of social media for improving care. *IEEE Journal of Biomedical and Health Informatics*, 19(1), p.p.210-218.
26. Abdelwahab S., Abraham A., Abraham A. (2015) Data mining approach for modeling risk assessment in computational grid. *Smart Innovation, Systems and Technologies*, 33, p.p.673-684.
27. Stamova I. M., Stamov T., Simeonova N. (2014) Impulsive effects on the global exponential stability of neural network models with supremums. *European Journal of Control*, 20(4), p.p.199-206.
28. Reeder J., Georgiopoulos M. (2014) Generative neural networks for multi-task life-long learning. *Computer Journal*, 57(3), p.p.427-450.
29. Naik C. A., Kundu P. (2014) Power quality disturbance classification employing S-transform and three-module artificial neural network. *International Transactions on Electrical Energy Systems*, 24(9), p.p.1301-1322.
30. DeVille L., Zeng Y. (2014) Synchrony and periodicity in excitable neural networks with multiple subpopulations. *SIAM Journal on Applied Dynamical Systems*, 13(3), p.p.1060-1081.
31. An D., Kim N. H., Choi J.-H. (2015) Statistical aspects in neural network for the purpose of prognostics. *Journal of Mechanical Science and Technology*, 29(4), p.p.1369-1375.
32. Adhikari R. (2015) A neural network based linear ensemble framework for time series forecasting. *Neurocomputing*, 157, p.p.231-242.

Intelligent Operation and Maintenance Monitoring System Based on ITIL Framework

Guangbin Sun

Daqing Oilfield Engineering Co, Ltd, Daqing, Heilongjiang, China

Hongqi LI

College of Geophysics and Information Engineering, China University of Petroleum, Beijing, China

Abstract
So far the centralized operation and maintenance monitoring for equipments is difficult to meet the needs in the applications of the enterprises which have complex business systems. This essay provides a business-oriented operation monitoring system that based on the technology of Keepalived and Inotify and the key process state judgment switch condition as well as triggered the synchronization process by changing the main file attribute to implement the redundant distributed monitoring mode. Integrated the business model into the logic relation of monitoring resources and treated the business view for analysis of system statements have been designed to improve the localization rate of alarming problems. The experimental results show that this system with a certain reference value for engineering application is characterized by its basic data acquisition which has low cost and small interference and meets the real-time monitoring for the complex business resources of the data center.
Key words: BUSINESS-ORIENTED, DISTRIBUTED MONITORING, INTELLIGENT OPERATION AND MAINTENANCE

1. Introduction

Both the expanding of business scale and the development of informatization has not only brought the expanding of the infrastructure construction scale, the software system is becoming more and more complicated, the bottleneck of information construction will also be gradually transformed into the efficiency and stability of the business system. Enterprise business volume and transaction data exponential growth model, the demand for running IT resource's stability and reliability will be increased gradually. Current IT services, operation and maintenance monitoring software are mainly for equipment or specific applications, dominated by operating state detection of server, network, database, middleware. It is difficult for this kind of monitor mode to gather and show the monitored information from different equipment or logical objects, the lack of monitoring index combination to constitute the overall system availability index, unable to quickly pinpoint the fault source when an alarm message is generated by the system failure. The root of the problem is that this kind of operational monitoring is not designed from the operation status of business system which IT operations staff concern most. Therefore, in light of technological needs for enterprise development, operation and maintenance monitoring should be increased from targeted way for business-oriented monitoring. Studies show that business-oriented IT operational monitoring system should meet the following requirements at least.

So far, there are a lot of operation and service systems based on ITIL framework. Generally they are only intended to realize the management for basic structures. The monitoring and management over professional service systems(OA, professional design software) and important classification applications (J2EE application server, Lotus, Domino, Portal, Database & LDAP Web server, URL & Ports, Mail, etc.) are insufficient. Besides, the monitoring over business systems developed for Individualization as well as fault detection are not realized.

The intelligent operation and maintenance monitoring systems are based on the acquisition of different types of monitoring and acquisition of the management data, with the help of configurable business model based on the consistency of the information, so as to achieve the object-oriented business system monitoring. These systems provide their users with customizable reports, charts and other visual data analysis. When early warning occurs, the systems immediately filter the information received, make causal rule judgment, rapidly localize the fault points, and then automatically push the information by text messages or emails to the relevant operation and maintenance personnel, so that the "post intervention" is replaced by "pre prevention" for the operation and maintenance. In this way, not only the operation and maintenance workload is reduced but the intelligence for operation and maintenance is improved as well. The architecture of monitoring system, key technology and operation conditions are described in this paper.

2. The Status quo of Operation and Maintenance Monitoring

2.1. The current situation in operation and maintenance monitoring

Now the domestic and foreign operation monitoring systems for monitoring information data collection can be divided into two types: Agentless and Agent. The Agent system adopts the commands of the operating system itself, with the lowest of system resources and minimal impact on the system. It supports the front-end filtering, temporary data storage. The Agentless system fully supports SNMPV1-3 and the mixed way to read data, and various ways to collect traffic data such as Netflow/NetStream/Sflow /Dataflow.

The small and medium-sized monitoring systems mainly employs C/S model of software development platform in monitoring system design patterns. When

monitoring volume and scale is large, the operational performance of the software monitoring platform with C/S and its scalability are not only affected, and more hardware resource will also be consumed to support large data monitoring and process. Usually, when problems occur in software and hardware systems, the danger of complete collapse will also occur in the monitoring system.

The B/S software system has the advantages of easy monitoring extension and relatively independence of data collection. With the characteristics of wide distribution, easy maintenance, strong sharing and lower cost, it is suitable for those IT resource environment with large volumes of data to be handled.

No matter what kind of systems to be designed, the basic technical requirements for operation and maintenance monitoring should be met: small disturbance of the original system, low cost and good scalability and extensibility, timely responses and using the system resource as small as possible at the same time. Therefore, the following aspects should be considered: 1) access to information 2) interference elimination 3) information associated 4) fault recovery[1]. Disaster recovery and architecture of redundancy design of operation and maintenance monitoring system are also important factors for real-time management, monitoring, maintenance of IT information resource.

2.2. Common Monitoring Software

Now commonly used monitoring tools includes: Ganglia, Zenoss Core, Nagios, etc.Ganglia is used for measuring thousands of nodes monitoring project. Each computer runs daemon called gmond which collect and sent metrics. The process collects metrics from the operating system and specifies the host. The receiving host can show all metrics and transfer the streamline form of the data in the hierarchy. Gmond which consume less load system, and by the methods of the clock consistent, eliminate the network jitter and the influence of the performance of the node for collecting datas[2].

Zenoss Core, an enterprise IT intelligent monitoring software, is used for detection and management of the company's IT environment of various kinds of assets including servers, network structure. Once the model is created, it can monitor and report on the status and performance of IT infrastructure resources. Zenoss provides events and errors management system associated with CMDB to help improve the management efficiency of various events and reminders[3].

Nagios is a monitoring system to monitor system status and network information. It can monitor the specified local or remote host and service, provide exception notifications. WEB browser-based interface for viewing network status, a variety of system problems, logs,etc[4].

3. Design of Monitoring System

3.1. Design of System Software Framework

Business-oriented IT operation and maintenance monitoring system is a kind of upper monitor concept. The monitoring on computer room environment, network monitoring, server monitoring and the application software of monitoring points are regarded as the basic underlying supporting points. The design of B/S pattern framework is composed of four layers of technologies, as shown in Figure 1: 1) monitoring layer, including all data center objects to be monitored.2) information acquisition layer, using proxy mode or no agent public services way to get operating performance data by monitoring engine scheduling.3)data processing layer, is responsible for the collected raw data resources through aggregated data, extraction, filtration, synthesis, and then writes to the database.4) presentation layer, provides a unified intelligent monitoring data show. This layer is completely in B / S mode to show the various monitoring and management module, users can log in from a unified entrance designated authority.

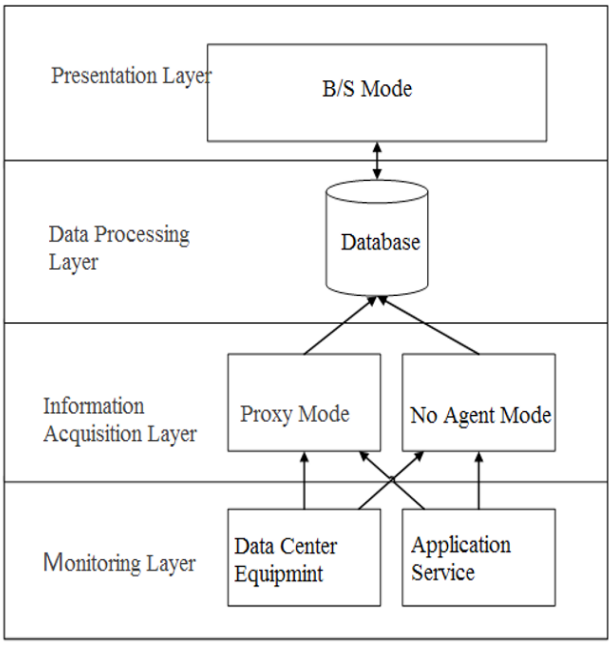

Figure 1. Framework of the Systema

3.2. Design of Function Modules of the System

According to the monitoring requirements of data center, designers decompose the function modules of redundantly distributed monitoring system, as shown in figure 2.

Among them, the main monitoring server constitute the function display and data processing layer of the system design framework which is to realize the main (standby) monitoring system switching, Web client configuration management, pushing alarm information, monitoring view display module function. The main (standby) monitoring server receives performance data from the distributed slave machine within a defined period of time and writes to the history database. When the main monitor engine crushes, the engine is switched from the alternate engine and take over the system services. Database filtering and integration module, business model logic module realizes the visual view display. Configuration management module completes the primary and backup monitoring engine interface operation.

Distributed slave computer constitutes information acquisition layer which achieves the collection of monitoring service data according to the equipment and application types. When the engine schedule fails to implement the monito- ring service in the defined time, the main monitoring engine will complete the active acquisition instead. It supports to add monitoring business online without affecting the other slave computer monitoring and collection.

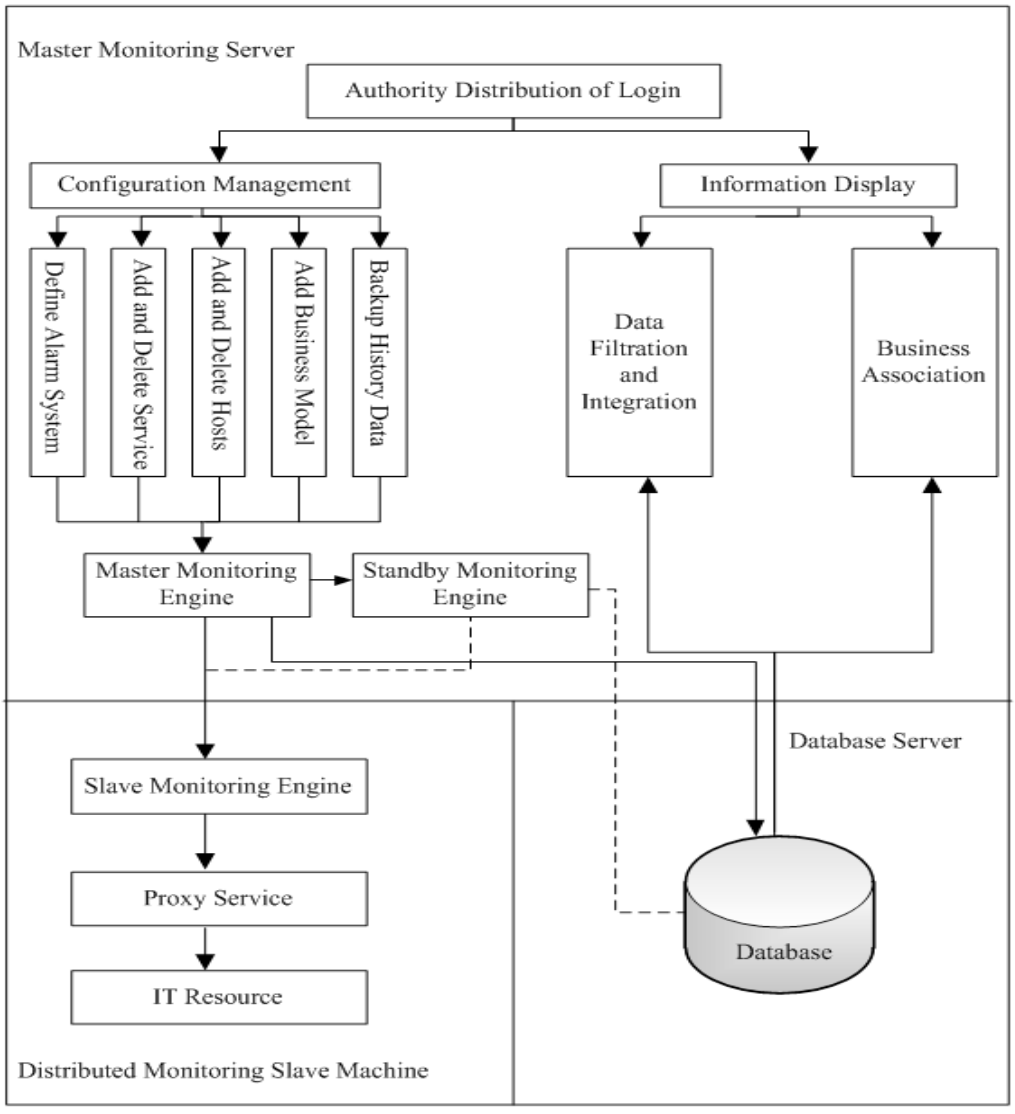

Figure 2. Function Modules of the Distributed Monitoring System

The database server is the data processing layer which realizes the historical data query and backup. The contents of management configuration file record parameters as a table. The B/S terminal performance data display, business status, alarm information, statements of historical data was read directly from the database server to complete the processing.

4. Realization of the Key Technologies

4.1. Distributed Monitoring

Monitoring the engine can realize the remote ma-

nagement and monitoring services with the assistance of the daemon. The principle is invoked automatically plug periodically to detect server status and maintain a queue, all the state information from plu-gin returns into the queue. Reads the head information from the team and process, writes the state of the result into Mysql database by Ndo2db process.

The scale of monitored resources is increasing, and the monitoring system also needs to improve its flexibility and extensibility. Therefore distributed data collection model is often used to adapt to the growing business needs. As shown in Figure 2: in distributed monitoring slave machine module, monitored object can be divided into application software, server, database, network and other five types. Slave monitor machine complete reading their specified information index, and send the information to the master monitor machine in the set time. NSCA is an external component package which can be performed on the remote Linux/Unix host mandatory testing and send results to the monitor host. Execute nsca process on the mainly(standby) monitor machine ,the process of send_nsca executed on the slave machine will monitor data and sent to the main (standby) machine through the specified port. In this mode, as a result of the decentralized collection process of monitoring data, the stability of the whole monitoring system is improved. Even if a slave machine is down, unable to send monitored resources data over a set time after the threshold, master machine can take over the task of collecting information. Compared to centralized monitoring methods, distributed monitoring approach reduces the load on the monitoring host, improve the reliability of data acquisition system.

4.2. Synchronization of Active/Standby Monitoring Systems

The synchronization of active/Standby monitoring systems is a necessary condition to achieve control engine stable, reliable redundancy switching. The synchronization condition and resource consumption issues have to be considered during the process of active/standby synchronization.1)Synchronization condition is the synchronization process of the active/standby working in what conditions, and when complete the specified file or directory, commonly used linkage trigger, scheduled, manual operation mode.2) Resource consumption refers to the resource consumption of network, memory, CPU and the process in the active/standby synchronization. The monitoring computer's work is to obtain information passively and the database server stored procedures and concurrent user interface WEB access from the monitor engine of the distributed master slave machine. Therefore, we use the key profile properties changes as the trigger conditions in the monitoring system design to realize the standby machine synchronize automatically, and reduce duplicate file synchronization process and system resource consumption. We use Rsync and Inotify to complete Trigger Synchronous of the active/standby machine. As shown in Figure 3.

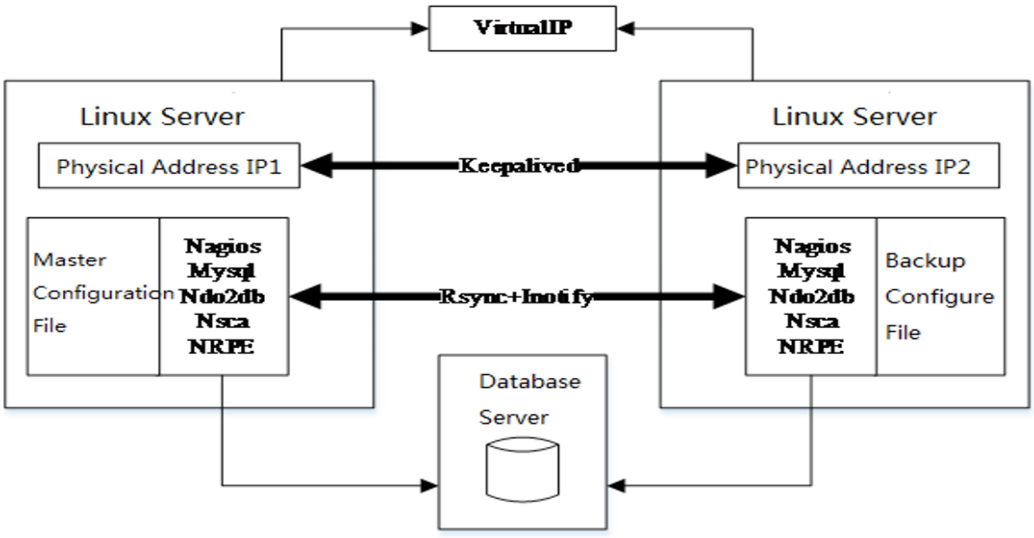

Figure 3. Synchronization and Automatic Switching between Primary and Standby Monitoring Machine

We need to create a script background running in the system, to achieve the monitoring of inotifywait process for adding, deleting, modifying other attributes to the specified directory or file and able to trigger the rsync to complete file synchronization of the active/standby machine.

Trigger: trigger condition is the creating, modifying, deleting the files in the specified directory $src_

Master_host. Part of the statement:

/usr/local/bin/inotifywait -mrq --timefmt '%d/%m/%y %H:%M' --format '%T %w%f%e' -e modify, delete, create, attrib $src_Master_host | while read files

Synchronize directory file: Specify the active/standby machine to synchronize files or directories, as shown in Table 1:

Table 1. Synchronize Files

Directory or file	Explanation
Httpd.conf	Apache Configuration File
Php.ini	PHP Configuration File
/var/www/html/	Program Directory
/etc/xinetd.d/.nrpe	NRPE Configuration File
/usr/local/nagios/	Monitoring Engine Configuration File

The automatic synchronization process when file attribute changes, is able to realize the consistency of data and content from external access, the process is also constitute a prerequisite for stable active/standby switching.

4.3. Redundant active/standby Monitoring

The automatic switching between redundancy monitoring host and backup machine, and maintain external access IP address consistently is key point to provide consistent continuous monitoring service. It requests that the systems can access the network constantly after the switching between redundancy monitoring host and backup machine.

Figure 3 shows the design of redundant monitoring: Physical address of the master computer is IP1, the physical address of the slave computer is IP2, and set external access to virtual address with Virtual IP. Since Keepalived management of virtual IP is achieved through multicast and priority, the machine with a higher priority has the right of management to the virtual IP (default master server). To implement automatic switching of external virtual IP, need to set the background program to start monitoring. It is called by the keepalived process, if the specified host state fails in the time interval, then turn off the monitor server keepalived process, making preparation keepalived to take over this virtual IP.

Add some code in the monitoring host configuration file keepalived.conf:

```
vrrp_script chk_master_status
{
 script "/root/shell/Smartoms_host_status.sh"
 interval 10
 weight 2
}
```

Smartoms_host_status.sh can detect running state of the key process. The output is the logic and of all key process state. If any process specified is in stop state, the trigger to close the keepalived process of this monitoring server to achieve automatic switching.

Due to the normal operation of distributed monitoring system, some key daemons are needed to ensure the overall function and stability of the system. Set the following key process for triggering the host standby switching condition, as shown in Table 2:

Table 2. Primary Process of Monitoring System

Status	Explanation
Mysql status	Database Operation Process
Nagios status	Monitoring Engine Process
NRPE status	Remote Agent Process
NSCA status	Distributed data Process
Httpd status	Apache Process
Ndo2db status	Database Written Process
Inotify_status	File system Trigger Process

4.4. View of Business Model and Locating of the Alarms

Business-oriented monitoring is to complete the process of consistency between application system and the basic information. Multi-level compre hensive analysis for the manage data collected from-different types of monitors and collector, and construct business-oriented view of the system. So that the global IT operation and maintenance personnel can take control of the operation state from the juris-

diction of various business system , including thestructure, hierarchy and relationships of business systems and IT resources. OA business view is shown in Figure 4:

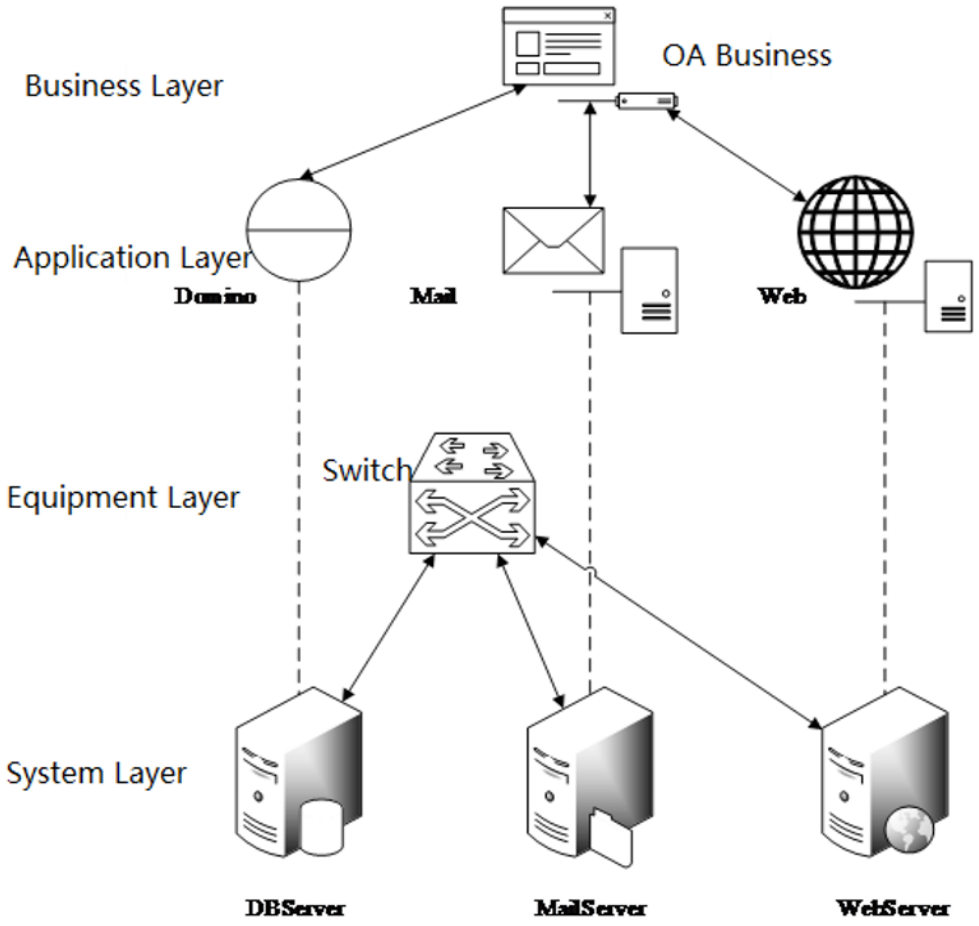

Figure 4. View of OA Business

The business view system layer: including database servers, file servers, WEB servers. Device layer: Switch Ports. Application Layer: variety of services and processes, including Domino, Web sphere, Mail and so on. Business Layer: OA business systems. Basic data corresponding to the various layers of view information: including switch usage, the corresponding port traffic, membership servers and operation state of disk array. Application layer data: opening state of the key processes, port status, opening states of the service, utilization process, greatest resource consumption process, and number of concurrent sessions.

Business model is described by configuration files, visual icons and the connection of monitoring resource are automatically generated after parsing the file in which the data format of XML as visualized page data is output from the fusionchart.js. At the same time, according to the data and operation state analysis document retrieval service, here are some descriptions of part of the definition:

;The total number of business models

;The name of each application model

;Alarm levels

;host IP

;Switch port;

;Connection direction 0: Host to switch 1: Switch to the host

;Enable service status for retrieval

;Enable monitoring service index retrieval

The following requirements have to be met to achieve business-oriented view and logical connection: 1) Definition of membership host with monitoring service.2) Definition of what constitutes a complete business service monitoring.3) Relationship of business system model. As shown in Figure 5.

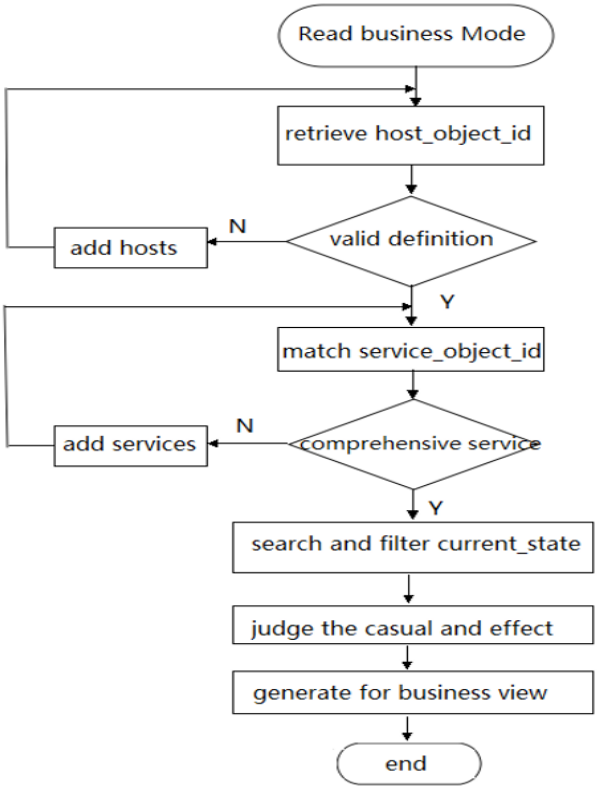

Figure 5. Logic Association of Business Monitoring

In abnormal alarm visualization of business mo-del, each service_object_id is matched by corresponding services, and filter current_state in the service. Business logic constitutes view alerts and push trigger condition.

Centralized monitoring system can realize the alarm information notification to the corresponding index of responsible person. While the responsibility can't make a quick judgment about locating the root of the problem, possible business impact and the steps of the process need to be addressed. In the business-oriented monitoring alarm, the monitoring service indicators covered by the business model as a key parameter in locating alarm, using the monitoring measurement and the status of services to build business visualizations. Through correlation analysis, system can display and push the alarm location and the affected scope of business.

Event correlation analysis is that according to the rule analysis the successively, causality between events to realize failure classification and find the reason of events. Especially in the large and medium-sized with more IT resource monitoring points of service, we can analysis the causes for the faults by filtering, judging and associating the causal rules and notice the staff and management in the corresponding according to the severity level of the alarm information.

(1)Filter: any alarm information of monitoring services can be pushed to the responsible person, but to avoid "alarm storm", the same type of monitoring services alarm is shielded after the number exceeds a set threshold, which rose to a serious incident alarm status and push it to system.

(2)Judgment of casual rules: any monitoring point operation is closely related with state of the process, application or device which depends on. To some degree, it logically constitutes the causality of events. After judging the rules, it can simplify the error source of judging process, and blocking some low-level alarm push. If the network outage can cause all monitoring alarm to the host device, after judging the rules, it can only notice the responsible person for network and system.

(3) Association: refers to the complete view of the business model of the alarm mode. The final alarm after filtering and judging is associated with business model, displaying alarm status and pushing alarm information service based on the business liability.

5. Experiment and Test

Monitoring system deployment, test environment is to rely on the oilfield Design Institute's data center. According to the requirements that put forward in the course of the system application by technical personnel, as well as with demand of building of intelligent management platform, the monitoring range is divided into general monitoring content and business-oriented monitoring, as shown in Table 3 and Table 4.

Table 3. General Monitoring Index

Linux/WinServerServer
Database (Mysql/DB2/Oracle/Mssql)
Network Equipment
Application Solfware(AutoCAD,ISA)
Middleware (FTP/HTTP/POP3)
Log Backup
Disk Array

Table 4. Business-oriented Monitoring

OA Business
Sametime Business
OA Backup Business
Mobile office application business
Portal
AUTOCAD Business
ISA Business
Engineering design platform business

Among them, the general monitoring index is based on data center information metrics collection

Server index of server is to realize the system information collection through VBS and WMI interface, including Ping, CPU, Mem, Proc, Service, User, etc. Linux server executes statistics command in the form of proxy and returns data information. Database key indicators include Cache_hit, Query, Links, Cost_sql, Lock, Latch, Full_scan, IO and other information. Using Snmp way to get network information indicators include Men, Cpu, Traffic, Uptime and so on.The other general monitoring indexes can achieve information collection in the way of NRPE or Nsclient++ proxy. Managing the general monitoring content in a manner of device group and associating business system information in the way of module to realizing monitoring display in two ways. And in the data layer, trigger link and ITIL service flow process retains a scalable API. data acquisition of common indicators for monitoring 24 * 5 (hour * day) and testing services to the timestamp timed scheduling delay, and select 15 indicators randomly from a distributed slave machine monitoring service to test the mean. As shown in Table 5:

Table 5. Business-oriented Monitoring

Database(Mysql)		Application Software		Server	
Index	Duration	Index	Duration	Index	Duration
Aborted_clients	0.33	Autocad_2006	0.55	Cpu	0.33
Com_commit	0.67	Autocad_2010	0.99	Disk	0.75
Keybuffer_read_hits	0.11	Autocad_2014	0.39	Memuse	0.11
Keybuffer_write_hits	0.60	ContentsBack	0.39	Net_traffic	0.77
Max_connections	0.09	Fileback	0.92	Port_1352	0.28
Opened_files	0.55	GetRaid	0.32	Port_143	0.68
Opened_tables	0.99	IIS_W3SVC	0.75	Port_21	0.38
Qcache_hits	0.45	ISA_2006	0.10	Port_25	0.38
QPS	0.39	TCP_conn	0.60	Port_389	0.37
Queries	0.92	URL_web	0.09	Procs_basic	0.18
Query_cache_hits	0.74	SpecialProcCDMS	0.54	Procs_core	0.39
Select_full_join	0.67	SpecialProc_OA	0.99	Service_basic	0.76
Slave_running	0.84	SpecialProcOA_BACK	0.39	Service_core	0.24
Table_locks_waited	0.60	SpecialProcOLE	0.38	Uptime	0.77
Threads_created	0.93	SpecialProcPDA	0.35	Ping	0.60

In the Nagios monitoring engine no-load operation, do scheduling delay test on the Nagios daemon, which measured, Max_latency=0.92s, Min_latency=0.15s, Mean_latency=0.54s.Table 5 shows that in the database Mean_latency = 0.59s, application software Mean_latency = 0.52s, server Mean_latency = 0.46s.It shows that in accordance with the distributed monitoring slave machine engine, scheduled for execution by the monitoring service to keep a low latency characteristics.

At the same time, we tested the resource consumption of proxy service in execution the information acquisition plug-in in the monitoring host. Configuration of monitoring host: Processor: Intel(R) Xeon(R) CPU E5645 @2.4GHz (2 cores), Memory: 4.00GB, System type: 64 bit operating system. The test data are shown in Table 6.

Table 6. Resource Consumption of Monitoring Proxy

Usage / Process		CPU Usage（%）			MEM Usage（MB）		
		Max	Min	Mean	Max	Min	Mean
NSCP	Concu	2	0	0	20.69	1.30	5.69
	Idle	1	0	0	12.31	1.12	3.56
NRPE	Concu	1	0	0	19.38	1.59	7.95
	Idle	1	0	0	11.97	1.14	4.76

Proxy service processes were tested during concurrent execution and idle CPU and MEM occupancy rate, CPU_mean = 0, maximum MEM_mean = 0.2%. It can indicate that in the monitoring information collection process, service scheduling, agency services and plug-in execution overhead low feature which is being the prerequisite to ensure the small disruption to monitoring host.

6. Introduction to System Functions

Design of business-oriented operation and maintenance monitoring system is according to the system function module decomposition. The following functions can be realized: 1) Monitoring information rights protection, users can view the corresponding monitoring data only after having the permissions to log in. Multi-level business show: log-in permissions is divided by the way of the working group and realize isolation and independence of data between departments. Permission can be divided into three categories from the user point of view: ordinary users, customization and advanced users.2) By configuring the slave monitor machine, operations of add, delete, start, stop of the monitoring object can be completed dynamically and implement monitoring host configuration management by the Web client.3) All monitoring data shows in chart, users can judge the performance of monitored object based on historical curve. Monitoring resources is divided by the type of group or business and realize the management of data report.4) Realize alarm mechanism of monitoring system and mobile communication services company docking. In the process of system operation, business responsibility is noticed timely by monitor abnormal alarms.

7. Conclusion

The design of business-oriented operation monitoring system provided by this paper can realize the monitoring on the basic resources from data centre and its application. It also provides the functions of monitoring information within the business scope as well as fast fault-location alarm. By monitoring on redundancy of the designed structure of the host, the overall system reliability is improved. The way of collecting information by distributed machines enhances the scalability and stability of managing the object under monitoring. Further research on monitoring system and ITIL management model, the network topology auto integration will be made to realize the intelligent system for IT operation service management.

References

1. Mansouri-Sanmani M, Sloman M.(1993) Monitoring Distributed Systems. *IEEE Network*, 5(2), p.p.20-30.
2. Massie M L, Chun B N, Culler D E. (2004) The Ganglia Distributed Monitoring System: Design, Implementation, and Experience. *Parallel Computing*, 30(7), p.p.817-840.
3. Kalochristianakis M, Varvarigos E A. (2010) Open Source Integrated Remote Systems and Network Management with OpenRSM. *Proc. Conf. on Systems and Virtualization Management (SVM) 2010 4th International DMTF Academic Alliance Workshop*, p.p.33-36.
4. Katsaros G, Kubert R, Gallizo G.(2011) Building a Service-oriented Monitoring Framework With Rest and Nagios. *Proc. Conf. on Services Computing (SCC) 2011 IEEE*, p.p.426-431.