XPM Full stack performance management and traffic analysis platform

The user manual

Ver3.3

In May 2019

Catalog

1. Introduction

1.1. overview

This document will introduce in detail the functions and operations of "XPM full-stack performance management and flow analysis system" (hereinafter referred to as XPM), to help users quickly understand and master XPM.

Relevant video data can also be obtained by searching for "XPM" through Tencent video.

1.2. Readers

This document is intended for the following readers:

- XPM Partner support engineer
- XPM End user maintenance engineer

2. Statement of Security and Privacy

2.1. Security statement

2.1.1. Data management and protection instructions

Some functions of this product involve personal or public information or data of users, such as user account, password, email, telephone, terminal IP address, etc. Relevant user data can only be used for the operation, maintenance, fault location or recovery of the product system. Please use the relevant functions within the normal business requirements and within the purpose and scope permitted by laws and regulations. In the process of using and storing users' personal information or data, you should take adequate measures to ensure that users' personal information or data are strictly protected. Including but not limited to the following:

- User management

System administrators at all levels have high authority. When the position of corresponding personnel changes, the corresponding permissions or passwords should be recovered in time to ensure that users' personal information or data are strictly protected.

- Data backup

In order to prevent data from being modified by mistake, resulting in system failure or user data error, this product has the backup function of configuration and account information, and users can backup regularly. The backup content should only be used for data recovery, and it is recommended that you comply with the relevant laws of the country in which you are located to perform this task, so as to ensure that your personal data is fully protected, and it is forbidden to store these contents privately or for other purposes. After the backup expires, the abandoned backup data should be deleted in time.

- Safe handling of public information

To provide service for the public XPM user, because you are in the process of using the XPM, public information may involve sensitive, so, we suggest that you follow the related law enforcement in the country of operation, and take adequate measures to ensure that the user's personal data are protected by fully, especially to download the raw data packet flow back function.

2.1.2. Password configuration and modification declaration

- The user's default password must be modified in time and saved properly after login
- To fully ensure the security of XPM, please be sure to change your password regularly
- To ensure the stability of XPM, we do not provide users with background management accounts and passwords

2.1.3. Security log and account permissions

- XPM is divided into two levels: system administrator and ordinary user. The system administrator is a full-function account, while the ordinary user account is an account created by the system administrator and given access to different functions
- The system management personnel have recorded the operation of adding, deleting and changing the account
- Ordinary users log in the system, log out log records

2.1.4. Traffic mirroring features disclaimer

As a product that takes network traffic as the analysis object and basic data, XPM cannot avoid using network traffic containing sensitive information. We will obtain exemption from users according to the following scheme:

- For users who have purchased XPM, since the ownership of the device belongs to the user, we will not be able to know the sensitive information in the network traffic of any user;
- And to provide services to other users and use XPM system, we will only in the case of authorized users, and is limited to the function demand and analyze and understand the possible sensitive information in the network traffic, if users have any worry, XPM service party may issue the

relevant information confidential documents, the user can also prohibited XPM open may know the function of sensitive information, including: HTTP protocol analysis, SQL, protocol analysis and flow back function.

2.2. Privacy statement

XPM product features and original code developers understand the importance of privacy to you, and fully respect your privacy. We hereby make this privacy statement (hereinafter referred to as "this statement") so that you can understand how we collect, use, disclose, protect, store and transmit your personal data. Please read this statement carefully. If you have any questions, please contact us.

Personal information refers to all kinds of information recorded electronically or by other means that can identify the personal identity of a natural person alone or in combination with other information. This statement sets forth how huawei handles your personal information, but it does not cover all processing scenarios and the products or services discussed, mentioned or introduced in this statement are not available to all or in all geographical locations. How specific products or services handle your personal information shall be published by huawei in the special privacy notice or supplementary statement of such products or services. In addition to this statement, you are advised to read the privacy notice or supplementary statement when using specific products or services. This statement applies only to XPM series products.

This statement will help you understand the following:

I. how does XPM collect and use your personal information

II. How will XPM use cookies and similar technologies

III. Whether XPM will share, transfer and publicly disclose your personal information

IV. How does XPM protect your personal information

V. How does XPM manage your personal information

VI. How will XPM handle the personal information of minors

VII. Third-party links and their products and services

VIII. How is your personal information transferred globally

IX. How can this statement be updated

X. How to contact us

2.2.1. How does XPM collect and use your personal information

- Personal information collected by XPM
  - You may need to provide personal or organizational information when using XPM products or services. You are not required to provide personal information to XPM, but in some cases, if you choose not to do so, we will not be able to provide you with relevant products or services, nor will we be able to respond to or solve the problems you have encountered.
  - We will only collect and use your personal information for the purposes stated in this statement. The following examples illustrate the content and ways in which we may collect personal information:
  - In order to obtain the use authorization of XPM, you need to provide us with the necessary registration information, such as user name, company name, contact method, etc.;
  - In addition, if you regard the information of monitoring indicators and monitoring objects as your personal information, we will upload it to the cloud monitoring service center only when you authorize us to use it.
  - Huawei may collect relevant information such as name, email address and telephone number in order to properly use WeChat or alert remote notification. Huawei will take reasonable and necessary measures to ensure the security of the aforementioned communications;

- How will we use your personal information
  - Register and activate the XPM products and services you purchase;
  - Deliver, activate or verify the products and services requested by you, or modify, provide technical support and after-sales service upon your request;
  - Send you notifications of operating system or application updates and installations;

- Contact you, send you information about products and services that you may be interested in, invite you to participate in huawei's promotional activities and market research, or send you marketing information upon your express consent or request. If you do not want to receive such information, you can unsubscribe at any time;
- You asked us to participate in the data analysis work;
- It has your own purposes.

2.2.2. How does XPM use cookies and similar techniques

XPM products and services may use local storage technologies such as cookies, pixel labels, and web beacons. We treat information collected through cookies and similar technologies as non-personal information. However, if local laws treat IP addresses or similar identification marks as personal information, we will treat such identification marks as personal information.

- Cookie
  - Like other products based on B/S architecture, we will use cookies; However, we will not use cookies for any purpose other than those described in this statement. You can manage or delete cookies according to your preferences. For details, seeAboutCookies.org。
  - If you clear cookies, you will need to fill in the information yourself each time you use XPM. Note also that some XPM services may have to use cookies, and disabling cookies may affect all or part of your ability to use these services.
- Other local caches or stores
  - XPM may use other local storage technologies, such as in-memory caching, or caching files, or HTML5 local storage. Similar to the cookies described above, these techniques are also stored on your device and can be used to record some information about your activities and preferences. However, these technologies may differ from the devices used by standard cookies, so you may not be able to control them with standard browser tools and Settings. However, we can confirm that we have no active and conscious acquisition of such

information, but even so, if you still need to monitor the use of such information, you need to consult the browser provider for relevant control.

- Do Not Track

  - Many web browsers have a Do Not Track feature that publishes Do Not Track requests to web sites. Major Internet standards organizations have yet to set policies for how web sites should respond to such requests. If Do Not Track is enabled in your browser, then XPM products and services will respect your choice.

2.2.3. XPM How to share, transfer and publicly disclose your personal information

- We will not authorize, instruct or acquiesce to any third party to share, transfer or disclose your personal information without the written authorization of the user and without the requirement of law enforcement authorities in the host country that we must cooperate with;
- In case of any legal disputes arising from the violation of this agreement, we are willing to undertake the compensation quantified by the official agency.

2.2.4. How does XPM protect your personal information

We take the security of your personal information seriously and adopt industry standard practices to protect your personal information from unauthorized access, disclosure, use, modification, damage or loss. To this end, we have taken the following measures:

- We take all reasonable and practicable measures to ensure that the collection of personal information is minimized and that no personal information is collected which is not relevant to the purpose. We will only retain your personal information for as long as is necessary for the purpose stated in the cost statement, unless the retention period is extended or permitted by law;
- We will use encryption to ensure the confidentiality of data transmission and storage, and use trusted protection mechanisms to prevent malicious attacks on data and servers that store data;

- Only authorized personnel can access personal information; According to business needs and personnel levels, the number of authorized personnel shall be controlled and the authority management of authorized personnel shall be implemented at different levels. Access to personal data is logged and regularly audited by administrators;
- We will strictly select business partners and service providers, and implement the requirements on personal information protection into the business contract, audit, assessment and other activities of both parties;
- We will do our best to protect your personal information. But we know that no measure is foolproof, and no product or service, website, data transmission, computer system, network connection is absolutely secure. Therefore, we have established strict and exemplary information confidentiality regulations to alert any person or organization that may or may attempt to access your personal information;
- If there is a security accident that causes your personal information to leak, we will inform you in time according to the requirements of laws and regulations: the basic situation and possible impact of the security incident, we have taken or will take the disposal measures, you can autonomously prevent and reduce the risk of Suggestions, your remedial measures, etc. We will inform you of the event by email, SMS, push notification and other means. When it is difficult to inform the subject of personal information one by one, we will release the announcement in a reasonable and effective way. At the same time, we will also comply with the requirements of regulatory authorities, report the handling of personal information security incidents.

2.2.5. Third party links and their products and services

As of the date of this document, XPM products do not contain any third party commercial products, nor do they contain any links or authorizations of third parties; We will alert you in a prominent position in future releases of such methods that may cause sensitive information to be disclosed, and we will ensure that you do not authorize third party products or code to be used.

2.2.6. How is this statement updated

We reserve the right to update or modify this statement from time to time.

We will inform you of any changes in this statement through software update measures, and we will also inform you of any important changes in a pop-up window when you use XPM.

2.3. How to contact us

All XPM versions downloaded from the Internet and provided with services can communicate with us in real time through the online communication window under the XPM page; You can also email us at tcpiplabs@outlook.com. Normally, we will give you an initial reply within three working days and try our best to answer your questions within one month.

Important: local language versions of the privacy statement may differ from this version due to local laws and language differences. In case of any discrepancy, the local language version shall prevail.

3. Explanation of nouns and product keywords

3.1. Noun explanation

3.1.1. What is performance management

The technologies and products that can carry out abnormal warning, fault location, feature analysis and trend description in the real-time, accurate and stable process of information generation and interaction belong to the category of performance management;

3.1.2. KPI

In the technical theory of XPM, KPI generally refers to the status indicators. Such indicators cannot measure the service quality and business performance, but only express the monitoring objects' status in a certain time point or period. For example, the size of the traffic, the packet rate;

3.1.3. KQI

It is a representation of the operating quality and performance of the monitored objects. It is interpreted in accordance with the definition of performance management as: indicators that can measure the quality of the production or interaction of information by the monitored objects, such as time, error, response, etc;

3.1.4. The bypass mirror

It is a proprietary function of most ndma switches or other network devices, or OVS in the cloud, dedicated to copying traffic on one or some ports and sending it to another port. It is widely used to provide raw traffic data for various types of traffic analysis devices. Because they are not concatenated in the network, the interference to the network is minimal, generating up to 3% of the load on the switch in traditional environments.

3.1.5. APM And NPM/NPMD

The definitions of APM and NPM/NPMD in the industry are mostly based on Gartner. However, we believe that Gartner's definition of these two product types has a certain historical continuity, and it also acknowledges that there is some overlap between the needs of these two technical fields, so we do not recommend Gartner's definition as the standard. Our definition is as follows:

3.1.6. APM

Application Program Performance Management, In principle, APM is defined as adopting agents or technical methods that require authorization of user programs, which can help users monitor and analyze the execution efficiency of applications.

Its biggest advantage is that most of the development language programs, code level performance monitoring; However, the disadvantages are also obvious. That is, due to the tight coupling characteristics of its Agent program, some compatibility, security and other risks cannot be avoided. Therefore, to some extent, it is not suitable for all-weather real-time performance monitoring of your system, but more suitable for occasional debugging or use in r&d and test departments;

In addition, the APM of this method cannot monitor the network hardware that cannot be implanted into the Agent program, so there are many blind spots in the monitoring of network nodes and devices.

3.1.7. NPM/NPMD

Performance management based on network traffic. Note that Gartner's misleading definition of NPMD leads many users to believe that NPM/NPMD products cannot monitor application and business performance, which is a serious fallacy.

Compared with Agent APM, in addition to the inability to monitor the execution efficiency of program code, NPM/NPMD seems to be more suitable and in line with the performance management requirements of most users. Its advantages are mainly reflected in the following aspects:

Complete loose coupling during deployment and use ensures compatibility and security;

When analyzing application components (such as databases), user accounts and passwords are not

required, making it more secure and hassle-free.

The performance of serial network devices can be monitored.。

In short, due to the loose coupling characteristics of flow analysis methods, PM products based on flow analysis are more suitable for deployment and use in production environment.

3.2. Product keyword interpretation

3.2.1. WatchPoint

That is the flow mirror point, also known as the acquisition point, capture point. It refers to the network traffic that is introduced into the network ports of XPM devices through the mirror ports of network devices such as switches or routers, or that is aggregated by TAP and labeled with VLAN;

3.2.2. Server

IP or IP: Port that provides services for a business. The specific input method is detailed in the XPM product internal help.

3.2.3. Client

It refers to one or a group of client IP, which can be a single host, network element, or a group of IP of a branch office. The specific input method is detailed in XPM product internal help.

4. Value and application scenarios

4.1. Product positioning and value

4.1.1. Product positioning: connect operation and maintenance with business with performance index!

For a long time, operation and maintenance have been oriented to IT objects, and language has been in the category of IT.

Business requirement for IT, for example, is stable, accurate, real-time, complete, these are the users to be able to perceive indicators, but the language of IT operations are link bandwidth, CPU utilization, packet loss rate, code BUG, database index, and no correlation between the two languages, but there are also not understanding across we cannot ask the business department or unit leadership to understand IT language, since the business is the lifeline, which is the main body value. Then, we need to explain, translate and apply to the specific daily work in the language that the business department can understand.

The first value of performance management lies in connecting operations and operations with the performance indicators understood by IT operations and peacekeeping businesses, building a bridge of communication for operations and peacekeeping businesses, and creating a language of mutual trust.

4.1.2. Product value: it is an inevitable choice to achieve active and efficient operation and maintenance

In the whole field of operation and maintenance, performance management is the technology field closest to business, and also the technology stack at the top. Output the main indicators of performance management, it is time, error and response directly related to the user perception indexes such as, and all production accident and user complaints, actually also is one of these indicators deteriorated feedback, for example, access to interrupt, caton, slowly, according to incomplete, these accidents or complaints, are monitoring content of the performance indicators.

One of the goals of active operation and maintenance is to fully reduce the accident rate and complaint rate. When many anomalies do not result in accidents and complaints, the abnormal information can be actively received, and based on this, the abnormal information can be predicted, investigated and solved in advance.

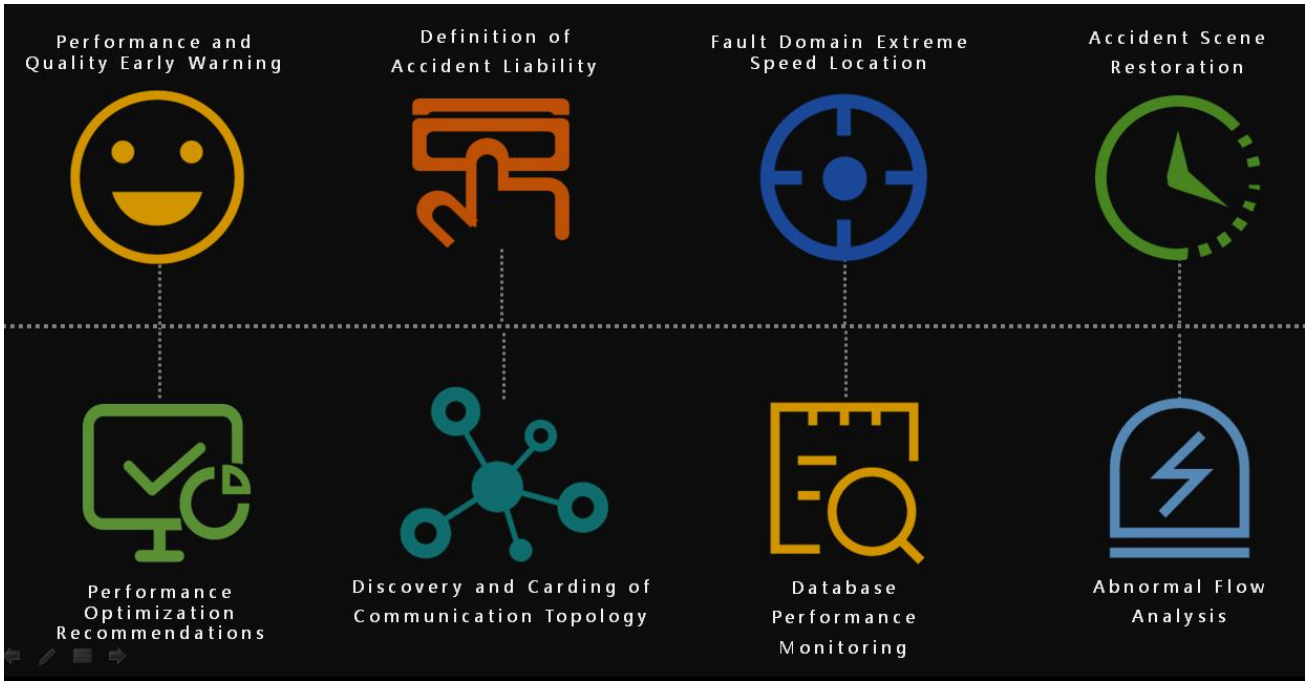
In addition, in terms of capacity and resource judgment, performance management index is also the most core and the most essential reference. Undoubtedly, it is the most effective and scientific method to manage capacity and resources through the deterioration trend of performance index.

About efficient operations, the core is the main points of the accident or complaint, able to efficiently locate the fault domain, and trying to solve fault, to resume production as soon as possible, in this respect as operational field of superstructure of performance management, is undoubtedly the most has the guiding significance of technology type, its understanding of the performance loss and algorithm, is by far the only effective, the methodology of rapid positioning fault domain.

4.1.3. Relationship with operation and maintenance of big data and AIOPS

Nearly two years, operational data and AIOPS gradually become one of the direction in the field of operations, in essence, these two types of projects, all roads lead to Rome, AIOPS is the basis of operational data, and the operations of big data in the source data, the most practical value of the data type is the performance data, there is no performance data of the operational data and AIOPS, like didn't check equipment to help medical units, doctors and drugs, there is no place.

4.2. Overview of application scenarios



4.2.1. Application scenario 1: performance and quality warning

As mentioned earlier, each IT unit has KQI representing performance and quality, which are also directly related to the business and perception as part of the business quality and user perception. Then, as long as these KQI are monitored, in principle, early warning of business quality and user-perceived anomalies can be made, and accident rate and complaint rate can be reduced.

In the alarm function of XPM, the KQI of all objects monitored by XPM can be comprehensively alarmed by artificial threshold or intelligent algorithm. The setting and notification of artificial threshold and intelligent algorithm alarms are described in detail later.

How to set alarm threshold? Please refer to

4.2.2. Application scenario 2: accident liability definition

In some large and medium-sized units, IT work is usually composed of multiple relevant departments. Therefore, due to the inability to clearly define the responsibility after the accident, the work arrangement and responsibility division often appear prevaricates.

For example, the problem of slow access of a certain business may be related to network operation

and maintenance, business operation and maintenance, database, software development, and even special line of the operator. If the network cannot be clearly defined in the first time after the accident, is it the network? Application? Database? It not only affects the efficiency of locating fault domain, but also affects the time of resuming production.

How to define accident liability? See also.

4.2.3. Application scenario 3: fault domain speed location

After the accident, locating the fault area quickly is an important link to find the root cause and solve the fault. But because there are so many IT units involved in accidents or complaints, traditional basic monitoring and manual methods are stretched thin without professional methods to help us locate fault areas.

- Problems with basic monitoring:

  Basic monitoring schemes based on SNMP protocol, no matter for commercial software or open source projects, are essentially management and monitoring for the running state of equipment, and are seriously lacking of performance index KQI. Basic surveillance, for example, is the way networks are monitored, more like highway checkpoints, toll gates, or rest areas. As for the traffic flow on the expressway, there is no way to monitor the speed, violation or accident. Just like the camera and intelligent analysis system on the expressway, XPM focuses on monitoring the indicators running on the highway, rather than the traffic flow or type at the checkpoint.

- Manual command problems:

  Manual commands are the easiest way between, but also the least reliable and the least accurate. It can measure the on-off of the network or the continuance of the service and the delay of the link after the occurrence of the accident, but it can't do anything for the application to deal with the delay, response, error and the accidental accident that cannot be repeated, let alone achieve the warning effect. Foreign statistics show that only 9% of accidents or complaints can be analyzed and located by manual command, while the remaining 87% of accidents or complaints cannot be handled by manual command.

4.2.4. Application scenario 4: accident scenario reduction

Some complex and difficult network operation and security accidents can accurately and completely restore the indicators, even the original data package, which is the only way to troubleshoot, locate and solve problems. In this regard, XPM provides rich data support.

KPI/KQIGraphical data:

- KPI/KQI Graphical data:

  XPM provides graphical data support for KPI/KQI of all monitoring objects that can be output in real time, and all of them can be supported for at least half a year. Therefore, when an exception occurs to a monitoring object, the user can find the KPI/KQI that causes the exception of the monitoring object by tracing back the KPI/KQI graph of the monitoring object or related monitoring object.

- Communication pair or session data:

  XPM's built-in database stores quintuples of communication pairs or application layer sessions for each communication analyzed, application layer header, and KPI/KQI for that communication or session. Therefore, when a complaint or failure occurs to a monitoring object or IP, users can extract KPI/KQI of the communication or session when a complaint or accident occurs by queryip or application layer information (usually URL or SQL) to provide more detailed analysis of the object data.

- Original data message:

  Enable the TSE network traffic tracing function of xpm-h (which is not supported by xpm-v), and pre-set the conditions that need to store the original traffic, and XPM can store the qualified original data packets in the disk array of the local server. When an accident or complaint occurs, the user can extract the original data packet of the accident or complaint from the local server according to the five-tuple information, or through the communication path, and open it through Wireshark and other offline analysis tools to view the most basic and detailed original data information. In many cases, raw data packets are the only basis and the only evidence to solve difficult security and operation accidents.

4.2.5. Application scenario 5: performance optimization recommendations

XPM has strong optimization suggestion ability for user network, application and business, which can be divided into three application scenarios :

- Network optimization Suggestions:

  By ranking the KQI of the server, client and branch by TOP N, users can quickly find which server or client/branch has the worst performance. Moreover, performance bottlenecks and risks can be found by combing the communication chain of these worst objects, and network optimization can be carried out based on this;

- HTTP application optimization recommendations:

  For Web Server and middleware using HTTP protocol, XPM can find the time point with the worst performance by backtracking the KQI graph of a day, a week or even a month, and then drill down to the HTTP session and URL with the worst performance from this starting point. In addition, through the TOP N function of URL, the URL with the longest processing time and the most error return codes can also be found in a period of time, and based on this, Web or middleware optimization can be carried out;

- Database SQL optimization recommendations:

  XPM can conduct fine-grained SQL performance monitoring for Oracle, SQLserver and MySQL, the three major databases. Therefore, when we trace back the KQI graph of the database and find the time point with the worst performance, the SQL with the longest processing time at that time point can be obtained by drilling. Through the sorting function of TOP, users can also locate the slow SQL or the SQL with the most return codes in a period of time, and propose optimization Suggestions to the development department based on this.

4.2.6. Application scenario 6: communication topology discovery and carding

And foundation of network topology discovery based on SNMP protocol equipment, XPM topology discovery and carding function, completely is based on the real, communication of information and formation of fine grained, therefore, can help users find the unknown communication port, found business chain configuration errors, or find some network security risk of host:

Topology carding of service chain is very important for network operation and maintenance. The

main reason for this demand is that business departments often do not actively inform the network departments when modifying the IP or Port configuration of the service chain, which causes the network operation and maintenance departments to locate and remove obstacles based on the wrong service chain, greatly affecting the work efficiency and quality.

Therefore, we strongly suggest that XPM users should take the initiative to comb the business chain of each core business on an irregular basis. Meanwhile, in order to increase the actual monitoring effect, the Dashboard of the business chain should be established based on the combed business chain to achieve real-time monitoring effect that can be displayed on the large screen.

4.2.7. Application scenario 7: database monitoring

To separate the database monitoring module as an application scenario is introduced, first, because the database assets is the most core, the most important assets of each user, we need the performance of the real-time online monitoring method, second, because the traditional database monitoring method, the interference is mostly used method, the database security is found more or less, or the risk of performance loss. For example, loading Agent in database, or requiring administrator account and password to fetch data regularly.

However, XPM's database monitoring module, because it adopts bypass flow analysis method, has no interference with the database. Users only need to configure the IP of the database to realize real-time analysis of each SQL of the database and realize the warning function of the overall performance, which is very practical, easy to use and easy to use.

4.2.8. Application scenario 8: abnormal traffic analysis

Although XPM is a performance-oriented solution, its basic principle is still real-time network traffic analysis, so XPM can output very rich network communication indicators KPI. These kpis include not only native kpis such as traffic, packet, session, ARP packet rate, but also all kinds of proportional indicators unique to XPM, such as attempted connection rate, connection closing rate, packet rate, etc.

Although these kpis are not directly related to service quality and user perception, their exceptions may represent a security risk or operation and maintenance risk. Therefore, it is also

crucial for operation and security departments to warn, locate and analyze the exceptions of these kpis.

5. Version description

5.1. Three versions of XPM

XPM is divided into three major versions, XPM-H, XPM-S and XPM-V. The versions differ as follows:

- XPM-S：standard edition. It can be deployed on ordinary X86 architecture servers or even personal computers without special hardware requirements
- XPM-H：High performance version. It is suitable for oversize Internet users or telecom operators to monitor the traditional architecture and Underlay architecture. It requires specific standard hardware support, and XPM-H performance can be close to line speed.
- XPM-V：Virtual hosts can be deployed in cloud environments, and VMs can load Ubuntu Server 14 or higher. The specified traffic can be analyzed and monitored through SPAN or RSPAN functions of OVS bridge in cloud environment.

Compare item	XPM-S	XPM-H	XPM-V
Version name	Standard Edition	High Performance Edition	Virtual Machine Edition
Applicable User	The vast majority of users	Telecom Operators/Large Internet	Private Cloud
Form of delivery	Software Mirror	Hardware or software	Software Installation Package
Include an operating system	√	√	×
Applicable environment	Traditional Architecture,Underlay	Traditional Architecture,Underlay	Private Cloud Overlay
Network/Server/Client	√	√	√
HTTP module	√	√	√

Oracle module	√	√	√
SQLserver module	√	√	√
MySQL module	√	√	√
URL transaction module	√	√	√
Traffic Storage and Backtracking	×	√	×

6. Product characteristics and advantages

6.1. Non-interference, loosely coupled, safer deployment method

Safe, fast and non-interference deployment method is one of the key issues for users to choose safety products for peacekeeping operations。

- All monitoring indicators and functions of XPM are based on bypass mirror traffic of switches. This method of "traffic replication" can not only ensure that the business environment is not disturbed in the deployment and use process, but also ensure that XPM can adapt quickly even if the business environment changes. Therefore, compared with Agent, XPM can adapt quickly. Method, dial-up method, user account and password method, bypass traffic analysis method are recognized as one of the safest and most convenient source data acquisition methods in the industry.

6.2. Network-wide, Business Chain-wide, Architectural Monitoring Capability

XPM has excellent non-blind spot monitoring capability and is the highest integrated performance monitoring platform in the industry so far. This advantage is reflected in:

- Network-wide monitoring capability:

  XPM can help network operation and maintenance, and realize the performance monitoring and traffic analysis of all network nodes, servers, clients and subnets. In this respect, XPM has all the functions and characteristics of NPMD product types;

- Full-service company monitoring capability:

  After loading HTTP module, DB module and URL module, XPM can also realize the performance monitoring and flow analysis of every application component, even every sub-service, or operation step in the whole business chain.

- Full Architecture Monitoring Capability:

  XPM-H and XPM-S can monitor the performance of traditional architecture, while XPM-V version

can be deployed in the virtual machine environment, cooperating with OVS, to achieve performance monitoring and traffic analysis of private cloud tenants and other virtual machines.

6.3. Product design for monitoring object and operation and maintenance scenarios

The essence of XPM is traffic analysis software and data package analysis tool. But we also know that most of these two kinds of software are quite complex to use. So, how can we master XPM quickly with lower learning cost and lower difficulty? Object-oriented management of data, Scene-Oriented design of functions, is undoubtedly the most advanced, most in line with the essence of XPM product design ideas.

- Functional Design of Object-Oriented Monitoring System:

  How to organize and manage data and how to present it to users

  Unlike traditional data package analysis tools, XPM does not present all kinds of information and indicators in network traffic to users in the most primitive state, but classifies these information into each monitoring object based on IP, port, URL and other features, carries out statistical analysis, and makes it gorgeous and customizable. Front-end interface, showing users a complete enterprise-level monitoring product value;

- Logic of Use for Operations and Maintenance Scenarios

  It is to conform to the operation and maintenance department's working logic from macro to micro, and in the design of XPM, the logic is to start from the alarm or query of the monitoring object, drill step by step to the communication pair or session, and even the offline data package.

- In short, whether it is data management or functional logic, XPM is designed from the user's perspective. It strictly implements the design concepts from macro to macro, from outline to detail, so as to minimize the difficulty for users to learn and use XPM.。

6.4. High Performance Real-time Large Data Scheme

The reason for emphasizing high performance and real-time is that similar products, or some open source projects, have more or less insufficient performance, or need to intervene in the phenomenon of manual analysis, but obviously higher processing performance, and real-time online analysis ability without manual intervention, more in line with the user's excellent commercial products. Requirement.

- about high performance:

  The most basic understanding is the ability to grab packets, but a more realistic understanding is that in the face of continuous network traffic, XPM can start from grabbing packets, to session restore, to KPI/KQI analysis, to communication pairs, and session storage, each program maintains extremely high code quality and processing performance, ensuring that it does not occur in any link. Loss of Packets, Sessions, Data, or Data Errors;

- about real-time property of products:

  Real-time online processing capability without manual intervention is the basic requirement of early warning KPI/KQI. Compared with some products which need manual intervention to obtain some KQI, XPM can perform online real-time analysis, early warning and positioning functions for hundreds of monitoring objects and thousands of KPI/KQI without manual participation. This characteristic is also far ahead of other similar products in China.

6.5. Perfect service plan to ensure full play of value

As a complex real-time big data product, we believe that even if users have the time and energy to learn it, it will take a long time to master it. Therefore, we need to do our best to ensure that XPM can play its functions beyond the group and enrich when users will not use or have no time to use XPM. Practical value. To this end, we specially designed practical functions and professional services to avoid the above-mentioned situation and fully protect user investment. About the characteristics of XPM products and solutions, we focus on the above five points, because there are many contents, so we summarize them again, that is, to sum up.

- Deployment is safe and fast, which is the commonality of all flow analysis principle products.

- There are many unique advantages of XPM in this aspect: full architecture, no blind spot performance monitoring capability
- Easy to learn, easy to use, gorgeous product design
- High performance ensures higher data accuracy, and users can rely on XPM analysis results.
- Perfect service functions and methods to maximize user protection investment

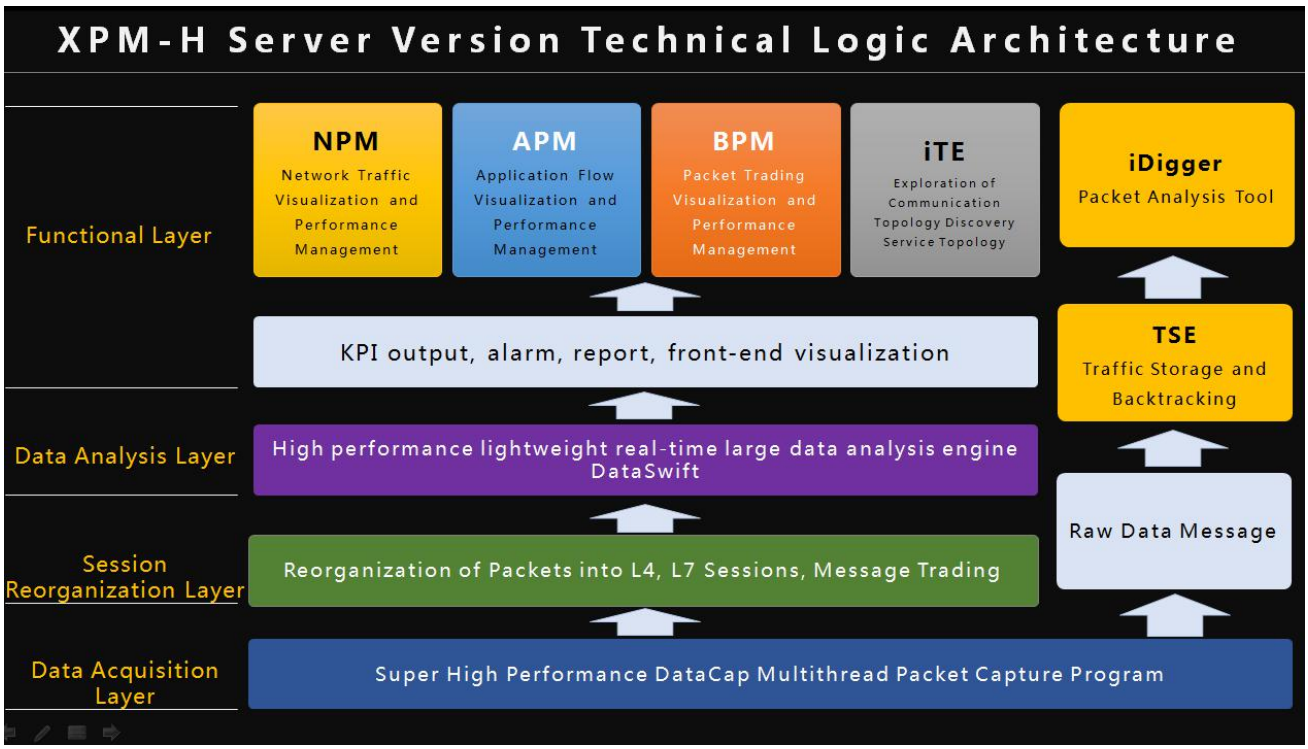
7. Product architecture

7.1. Integrated B/S architecture

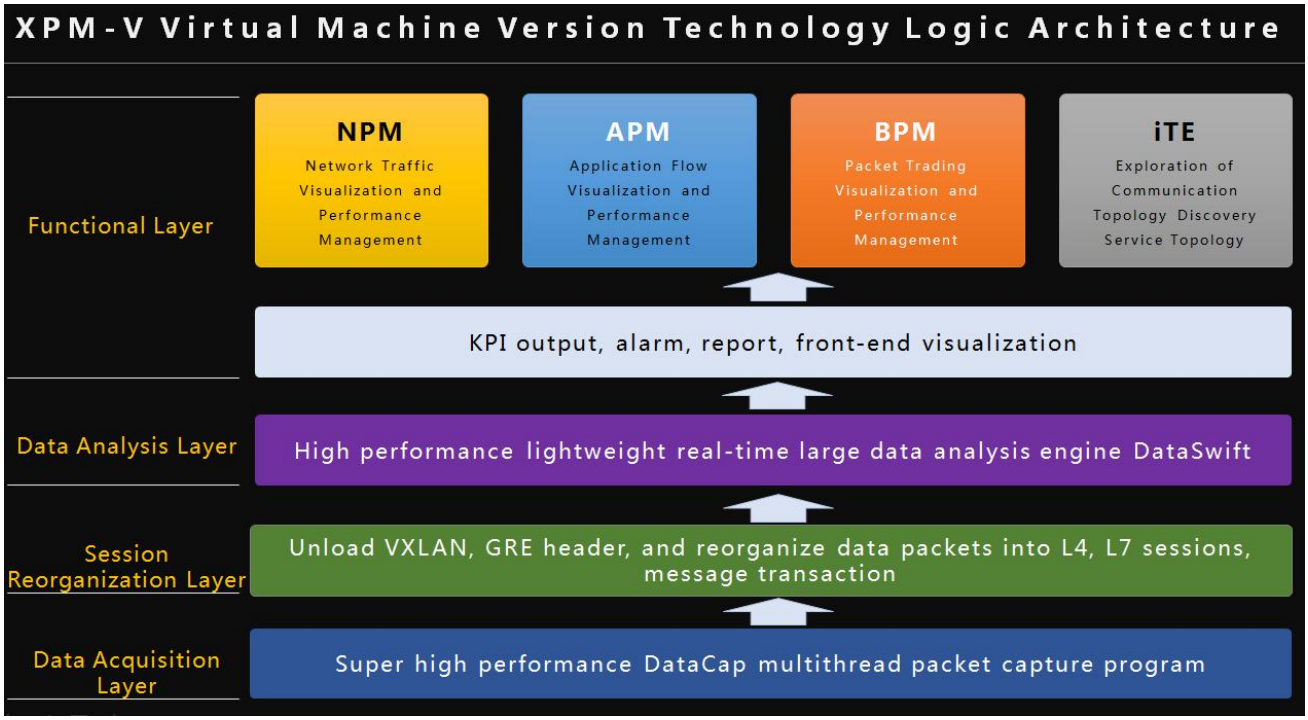
XPM adopts a standard B/S integrated architecture, all programs and functions are completed in one device or a virtual machine unit. Its advantages lie in:

- There is no need to deploy data acquisition points, analysis servers and other devices separately, and the cost of use and deployment is greatly reduced.
- The interference to network and business has been minimized.
- The reliance on network quality is minimal. For example, when adopting multi-layer architecture, if the network quality is not good, the data of the front-end data acquisition server will be lost in the process of transmitting back to the analysis server.
- Real-time is best. Because there is no need for preprocessing, the real-time output of XPM front end can achieve 10s refresh granularity, which is the highest real-time efficiency in the industry.

7.2. Xpm-h version logical architecture



7.3. XPM-S and XPM-V version logical architecture



7.4. Virtual Machine Install XPM-V Version

The functions of XPM-S and XPM-V are basically the same. The difference is that:

- XPM-S is hardware installation, XPM-V is virtual machine installation in cloud environment.
- XPM-S is a mirror ISO installation with its own operating system.
- XPM-V is a software program installation, which requires VM to pre-install Ubuntu Server 14 or later.

8. Product acquisition and installation

8.1. Product acquisition

All versions of XPM can be downloaded from our company's official website.

All of them can be obtained through our company's official channels; only by landing on our company's official website, registering as XPM users, and contacting our company through the IM of the website, we can get the corresponding software version.

If you need to get the hardware version of XPM-H, you need to contact our company or authorized agent and get it after paying the full amount.

8.2. Product installation

It will be provided to users along with the software mirror of XPM, which will not be repeated here.

9. Product deployment

As a kind of traffic analysis software, the core problem of XPM deployment method is how to connect mirrored traffic to XPM. However, there are obvious differences between traditional architecture and private cloud architecture. Therefore, different software versions and different methods should be adopted to adapt to different environments. Regarding version selection, I would like to emphasize it again here.

- XPM-S: Standard Edition. It can be deployed on ordinary X86 architecture servers or even personal computers without special hardware requirements.
- XPM-H: High performance version. Suitable for oversize Internet users or telecom operators to monitor traditional and Underlay architectures; need specific standard hardware support, XPM-H performance can be close to line speed;
- XPM-V: Virtual hosts can be deployed in cloud environments, and VMs can load Ubuntu Server 14 or higher. The specified traffic can be analyzed and monitored through SPAN or RSPAN functions of OVS bridge in cloud environment.

9.1. XPM-S version hardware requirements

The XPM-S version has no special requirements for hardware, and since the XPM-S version of the mirror installer already has its own operating system, users only need to prepare common standard X86 servers. Following is the performance standard of XPM-S version implemented with lower hardware configuration.

9.2. Processing Performance Standards for XPM-S

With the following hardware standards and traffic standards, XPM can turn on all functions to achieve stable, no obvious performance deficiencies due to operating carton.

- Hardware standard: Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz 4 threads, 8GB memory, 500GBSATA2 desktop hard disk; RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller
- Traffic standards: Network flow≤950Mbps; TCP/UDP sessions≤70,000 个/秒。

9.2.1. XPM-H version hardware requirements

If you don't load the traffic traceback function, you can configure the hardware for XPM by referring to the following criteria

Configuration scheme	Mirror Flow	CPU	Memory	Disk Array	NIC
1	＜200Mbps	≥i54C	8GB	1T*2, RAID 0,1,5,6	2*GE
2	＜500Mbps	≥E3V44C	16GB	1T*4, RAID 0,1,5,6	2*GE
3	＜1Gbps	≥E3V44C	32GB	1T*4, RAID 0,1,5,6	2*GE, 2*10GE
4	＜2Gbps	≥E5V412C	32GB	1T*8, RAID 0,1,5,6	2*GE, 2*10GE
5	＜5Gbps	≥E5V412C	64GB	1T*12, RAID 0,1,5,6	2*GE, 2*10GE
6	＜10Gbps	≥E5V416C	64GB	1T*18, RAID 0,1,5,6	2*GE, 2*10GE

- Memory and hard disk standards should be enterprise/server level, and PC level hardware is not recommended;
- If the load flow backtracking function is used, it is recommended that the number of hard disks in the above parameters be doubled.
- Network cards need to meet the following standards.

type	driver	Main Chip
Trillion	e1000e	82574L
		82571EB
		82579LM
	igb	I350
Ten trillion	ixgbe	82599ES
XPM system does not support Gigabytes and Gigabytes as working ports at the same time, but the working ports are Gigabytes and the management ports are Gigabytes.		

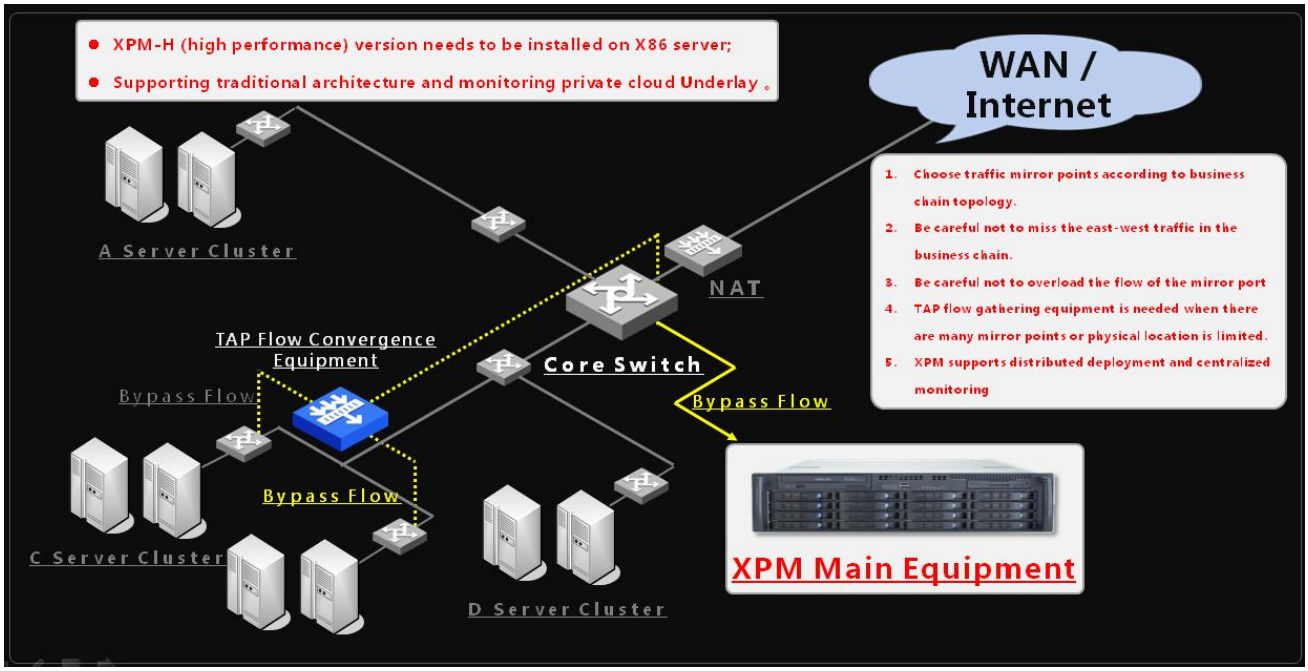
9.2.2. How to access mirror traffic

Traditionally, traffic mirroring is relatively simple, but the following points need to be noted:

- Select switches that need mirroring according to monitoring objectives. For example, if you need to monitor the performance of the ERP business chain, you need to connect the traffic

of each application component of the ERP business to XPM.

- If the eastward traffic needs to be monitored, the eastward traffic port of the downlink port of the switch needs to be connected to XPM.
- If the switch has a dual hot standby structure, it is important to note that the flow of both switches should be introduced into XPM.
- If more ports need to be accessed, special attention should also be paid to whether the mirror port is overloaded with traffic.
- If the traffic is unable to access XPM due to geographical location, or if the mirror traffic is too large to exceed the number of network cards in XPM, TAP traffic aggregation device can be used. Different mirror traffic can be tagged by TAP device. XPM will identify different network traffic according to VLAN tag.
- When multiple XPMs are deployed, an XPM can be defined as the primary monitoring device, which manages and monitors other XPMs.



9.3. How to monitor the performance of private intracloud tenant units

Chapter 6.1 deployment method can be used to monitor the north-south flow of private clouds, but for the East-West flow of private clouds, deployment and monitoring should be carried out according

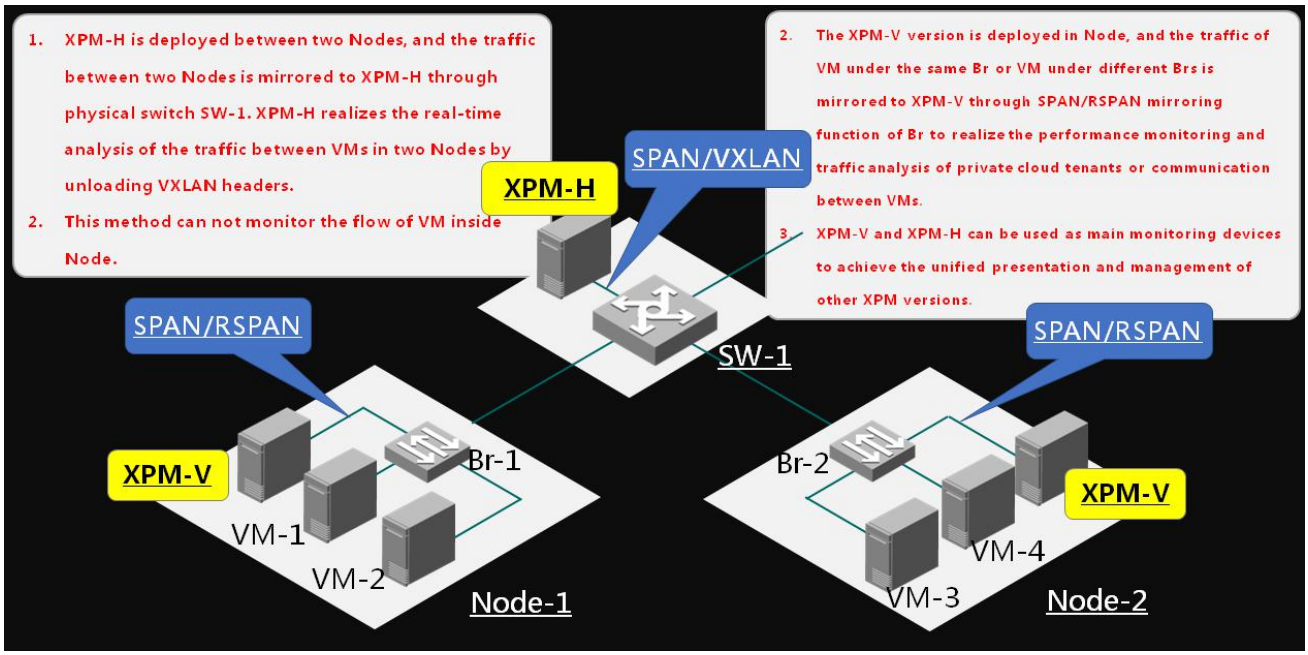
to the following methods.

9.3.1. XPM-H or XPM-S versions monitor virtual machine traffic between different nodes

XPM-H version of the server will be installed, deployed in the physical switch bypass connecting the node, and the network traffic surprise of the physical switch will be mirrored to XPM-H, XPM-H can carry out traffic analysis and performance monitoring for the traffic passing through the physical switch and virtual machine. The effective part of these traffic is UDP traffic encapsulated by VXLAN, which can be analyzed by XPM.

9.3.2. XPM-V version monitors east-west traffic of virtual machines in private clouds

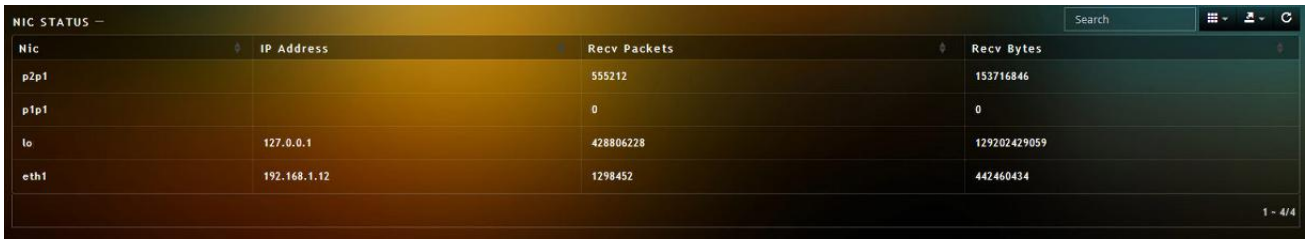
- The east-west traffic between each VM in the node machine can be accessed to XPM-V under the same Br through SPAN mirror function of Br or other XPM-V under the remote Br through RSPAN mirror. However, considering the impact of traffic transmission on private cloud environment, RSPAN is recommended to be used as little as possible and more XPM-V should be deployed. Combined with SPAN method;
- After deploying many XPM-Vs, we can set any XPM-H, XPM-S and XPM-V as the main system to achieve the unified management and presentation of each XPM version.



9.4. Verify that traffic is accessed correctly

9.4.1. See if mirror traffic is accessed

Path:【System Settings】—>【System Settings and Management】—>【Network Card Status】; The interface is as follows:



- A network card that receives network mirror traffic without an IP address; a management network card that has IP
- Watch the number of packets received and bytes received by network cards without IP addresses; the number of traffic and packets is obviously large, that is, working network cards, and vice versa, idle network cards.
- Keep in mind the name of the network card with traffic but no IP. Next, we need to use the name of the network card in the watch point settings.
- If the traffic of all network cards without IP is not large enough to manage the network card, it means that the mirror traffic is not accessed, and it needs to be re-checked whether the traffic is accessed correctly.

9.4.2. Whether to turn on VLAN analysis settings

If we use traffic aggregation equipment to do traffic aggregation, and set VLAN labels for different mirror traffic to distinguish different mirror traffic, we need to turn on VLAN label recognition function.

- Path:【System Settings】—>【System Settings and Management】—>【VLAN Analysis Settings】, The page is as follows:

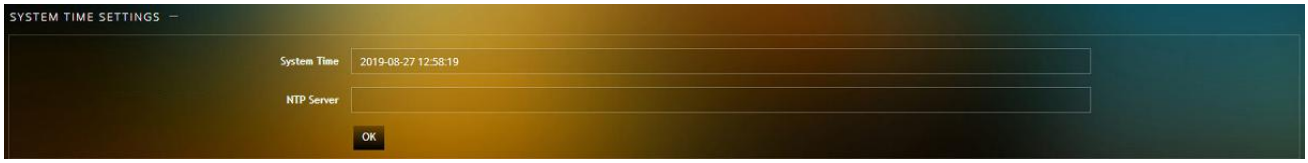
- Operation: Select [Open Analysis] and click OK.

9.4.3. Setting up a time server

- View the system time of XPM to see if it is the same as that of the user's computer; the system time of XPM is in the upper right corner of the page, as shown below:

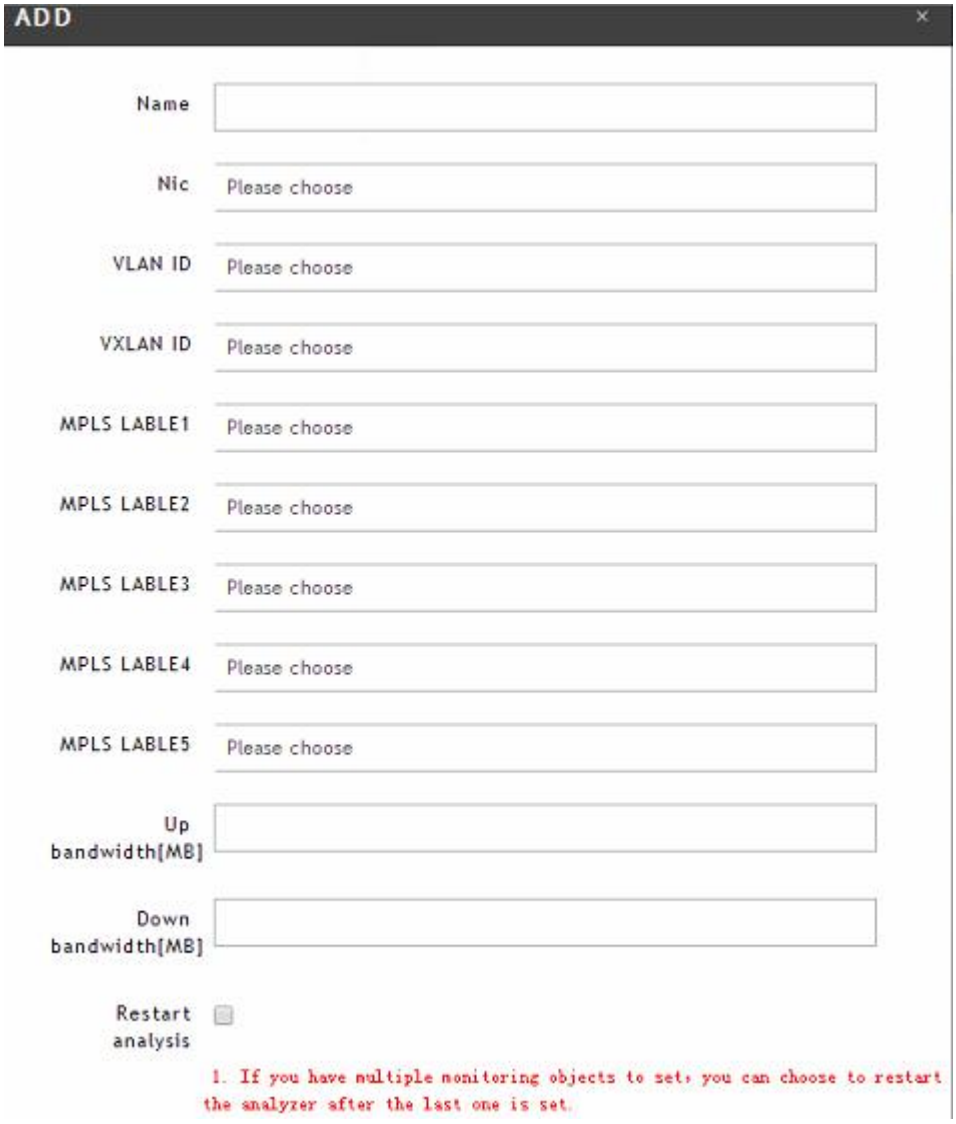
If the time of XPM system is inconsistent with the time of user's computer, please confirm it.

- If the user's Intranet has a time server, you need to set up time synchronization with the time server in XPM.
- Path:【System Settings】—>【System Settings and Management】—>【system time setting】, The page is as follows:



9.4.4. Setting up watch points

Path: [Home page] -> the second function on the right -> [Monitoring Object Settings] -> [Watch Point Management and Settings] -> Click on the [+] in the upper right corner of the list to add the following window to pop up:



- In Item 2 [Name of Network Card], we choose the working network card with larger network traffic recorded by us.
- If there is a flow aggregation device that has VLAN tagging settings for different mirror traffic, you need to select item 3 [VLANID].
- 【Uplink bandwidth】 and 【downlink bandwidth】 are bandwidth of mirror traffic used to output bandwidth occupancy.
- To add or modify watch points, you need to restart the analysis program. Therefore, if there are multiple watch points to be set, you can select the check box of Restart Analysis after they are all set up; if there is only one watch point, you can immediately select the check box of Restart Start Analysis.

9.4.5. Verify that the IP information provided by the user is correct

Before setting up monitoring objects, we must first verify the authenticity and accuracy of IP information provided by users. There are two validation methods.

9.4.6. Verify the existence of communication

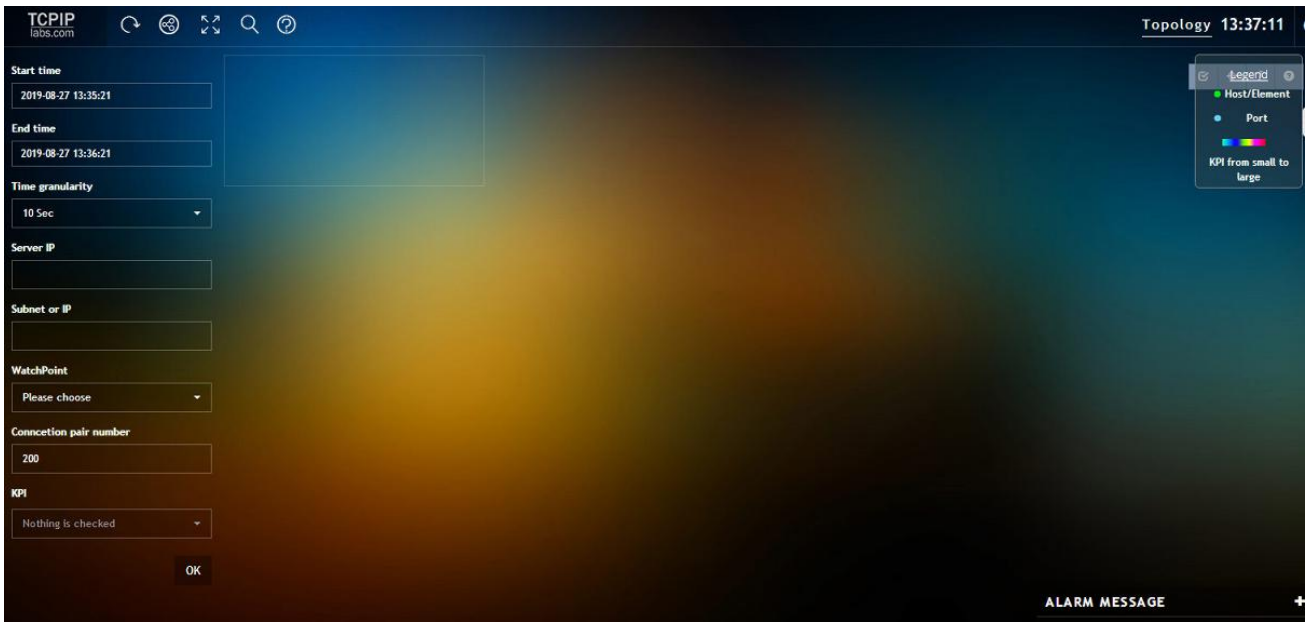
Path: In the upper part of the page, [shortcut toolbar], [search query], [server], enter some IP information provided by customers, click OK; as follows:

XPM will output the communication pair containing the IP. If there is no output, it means that the IP is not communicating, or the IP provided by the user is wrong. The function is as follows:

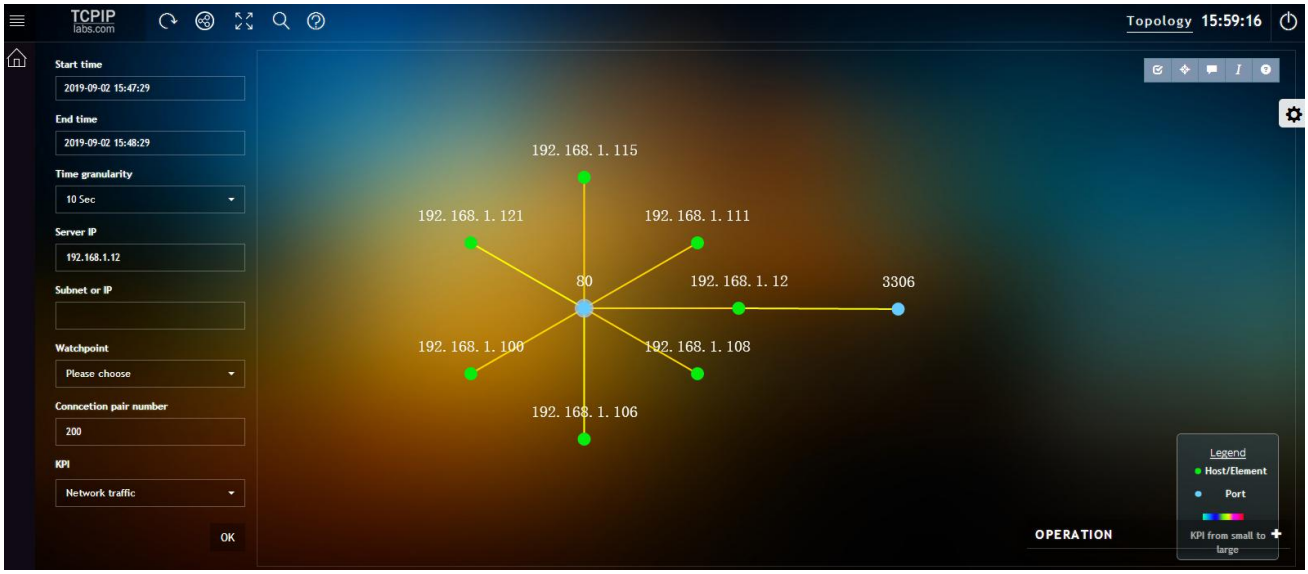
Starting time	ServerIP	ClientIP	Network traffic	Attempt connection
08-27 13:20:10 ~ 08-27 13:30:00	192.168.1.12	192.168.1.106	35.08Mb	8
08-27 13:20:10 ~ 08-27 13:30:00	192.168.1.12	192.168.1.121	28.50Mb	20
08-27 13:20:10 ~ 08-27 13:30:00	192.168.1.12	192.168.1.108	8.98Mb	8
08-27 13:20:10 ~ 08-27 13:29:50	192.168.1.12	192.168.1.100	682.38Kb	13
08-27 13:20:10 ~ 08-27 13:30:00	192.168.1.12	192.168.1.111	654.26Kb	13
08-27 13:21:20 ~ 08-27 13:28:50	192.168.1.12	192.168.1.90	643.58Kb	0
08-27 13:21:10 ~ 08-27 13:30:00	192.168.1.12	192.168.1.115	50.36Kb	0

9.4.7. Verify that business chain relationships are correct

Path: At the top of the page, [shortcut toolbar] -> [Topology query] will jump to the following page:



- In the left input box, the communication logic of the IP can be output by inputting time, IP and other information according to conditions. Note: Open the display IP (in the blue background toolbar in the upper right corner of the blank).
- In the graphics, the green dot is IP and the blue dot is Port. Double-click on the green or blue dot, the system will automatically sort out the next IP and Port with which the user communicates.
- By comparing this group of communication relations with the IP information provided by users or business departments, we can find the wrong or incomplete communication relations.



9.5. Common problems of traffic access

If there is no traffic access in XPM, no IP traffic that should occur, or incomplete traffic mirror, please find the reasons from the following points:

- If the eastward traffic needs to be monitored, the eastward traffic port of the downlink port of the switch needs to be connected to XPM.
- If the switch has a dual hot standby structure, it is necessary to pay attention to introducing the flow of both switches into XPM.
- If more ports need to be accessed, special attention should also be paid to whether the mirror ports are overloaded with traffic.
- Access traffic exceeds network card bandwidth
- Access traffic exceeds the bandwidth filled in when applying for authorization
- The traffic to be looked up is encapsulated by tunnel protocols, such as VXLAN, MPLS, etc.

10. KPI And KQI instructions

10.1. Deeply understand the relationship between KQI and KPI

- Each KQI has a specific causal relationship with several kpis, which is also one of the basic theories of warning and positionin;
- In IT architecture of different units, the correlation sensitivity (tolerance) of KQI and KPI is different. In a healthy IT architecture, the less sensitive KQI is to KPI anomalies, the better (tolerance is better); otherwise, the worse. That is, the exception of KQI must be because of KPI, and the deterioration of a KPI does not necessarily affect the relevant KQI; Therefore, the exception of a KPI does not necessarily result in accidents and complaints. Meanwhile, due to too many kpis, it is a kind of thankless logic confusion to invest limited energy and resources into thousands of KPI analysis, and the effect is often not good. This is one of the reasons why operations remain passive after many organizations deploy large open source monitoring projects;
- Since business accidents and user complaints are based on KQI, accurate measurement of the KQI of each IT unit can in principle achieve accurate accident warning and rapid fault domain positioning;
- However, to make long-term prediction and root cause mining, IT is necessary to accurately find the inevitable regular relationship between specific KQI and specific KPI in a specific IT architecture, which is also one of the basic goals of current operation and maintenance of big data and future AIOPS.

To sum up, the establishment of a clear operation and maintenance system guided by KQI is one of the core ideas for the formation of active and efficient operation and maintenance.

10.2. What are XPM's kpis and KQI?

10.2.1. Network KPI and KQI

Traffic KPI	Packet KPI	Connect to session kpis	Performance class KQI
Flow/in/out	Package rate	Amount of session	Load transfer time
TCP traffic /UDP traffic	Packet loss rate	Amount of TCP session	Application processing delay
Server traffic is not defined	Server/client packet loss rate	UDP session amount	Server/client communication latency
Client traffic is not defined	Into the package rate	Number of session interrupts	Server/client handshake delay
The server traffic distribution has been defined	The package rate	Number of attempted connections	Server/client retransmission takes time
The client traffic distribution has been defined	Packet size distribution	Number of closed connections	Connection interruption rate
Bandwidth occupancy rate of upstream and downstream	Packet ratio	Attempted connection rate	Connection response rate
ARP packet rate		Close connection rate	
ARP traffic		Session interruption rate	

10.2.2. Application layer KPI with KQI

Web/APP	The database	HTTP Middleware	Custom protocol	URL Business

				transactions
URL content	SQL statements	URL content	Application layer content	URL content
Traffic/session volume	Traffic/session volume	Traffic/session volume	Traffic/session volume	Traffic/session volume
400/500 Error rate	Return code error rate	400/500 Error rate	Outage probability	400/500 Error rate
No response rate	No response rate	No response rate	No response rate	No response rate
URLLoading time delay	SQL To deal with time delay	URLLoading time delay	Application processing delay	URL Loading time delay
Client latency	Client latency	Client latency	Client latency	Client latency
Server latency	Server latency	Server latency	Server latency	Server latency
Network communication delay	Network communication delay	Network communication delay	Network communication delay	Network communication delay
Web To deal with time delay		Web To deal with time delay		Web To deal with time delay

10.2.3. Interpretation of performance index KQI and direction of fault domain

Monitoring object	KQI name	KQIexplain	Main fault domain direction
The network link Network equipment Service groups branch	Apply response latency	Application processing is time consuming and generally refers to all applications and services	The application
	Server/client link delay	With XPM as the midpoint, the client/server network link delay	Network, or network device
	Server/client	Client/server host protocol	Host, or operating system

	handshake delay	stack construction delay	
	Load transfer delay	Transfer latency of load data, usually varying by the number of bytes	According to the number of bytes, whether normal
	Connection reset rate	The rate at which TCP connections are interrupted	NAT devices, or operating systems
	Connection unresponsiveness rate	The client's TCP connection is confirmed by the server	NAT devices, or operating systems
HTTP application Web middleware	**The Web handles latency**	**The time taken by the Web server to process HTTP session requests**	**Web application**
	HTTP non-response ratio	The percentage of HTTP session clients that did not receive a return code	Web service, or communication interruption
	HTTP error return code ratio	Percentage of 400/500 errors in all HTTP sessions	Web applications, or Web services
Oracle SQLserver MySQL	**SQL processing latency**	**Time taken by DB to process each SQL**	**Specific SQL statements, or database services**
	SQL unresponded ratio	The rate at which the SQL session client did not receive the return code	Database service, or communication interruption
	SQL return code ratio	The ratio of SQL statements with non-zero return codes	Database services, specific SQL statements

10.2.4. Explanation of KPI and KQI Algorithms

See Annex 2 for details.

11. Four data formats for XPM

11.1. Graphical data

All KPI/KQI of each monitoring object set by the user in XPM have corresponding graphical data for monitoring visualization and alarm threshold algorithm. Its storage strategy is:

- 10s granularity, 4h storage time
- 1m granularity, 1d storage time
- 10m granularity, storage time length 7d
- 1h granularity, 1y storage time

When users trace back graphical data through the backtracking function, the minimum time granularity matching the backtracking time is selected by default. Examples of graphical data are as follows:

11.2. Communication on data

For TCP/UDP sessions, XPM adopts the aggregation method for storage. That is to say, all TCP/UDP communications between client IP and the same server Port within every 10s are aggregated into a record and stored in the local database. Record contents include server IP:Port, client IP; Kpis and KQI for content such as 9.2.1; Such as:

172.26.201.1	80	172.26.25.11	19.06Kb	0	<1ms	<1ms	<1ms	<1ms	<1ms
172.26.201.3	80	155.1.120.2	14.46Kb	0	<1ms	<1ms	<1ms	<1ms	<1ms
172.26.201.3	80	155.1.120.4	38.70Kb	0	<1ms	<1ms	<1ms	<1ms	<1ms
172.26.201.1	80	172.25.13.131	16.54Kb	0	28.32ms	<1ms	<1ms	<1ms	<1ms
172.26.201.3	80	172.23.8.6	17.66Kb	0	2.02ms	2.02ms	63.83ms	<1ms	<1ms
172.26.201.1	80	172.24.4.26	116.50Kb	0	3.21ms	<1ms	<1ms	<1ms	<1ms
172.26.201.99	80	172.26.3.17	14.48Kb	0	<1ms	<1ms	<1ms	<1ms	<1ms

11.3. Application layer session

Every application layer session, the XPM system will store it into the local database, including session IP (server/client), port (server/client), application layer header content (for example, URL, SQL, etc.), application layer return code; Kpis and KQI for content such as 9.2.2; Such as:

Begin time	XPMserver name	ServerIP	Server port	ClientIP	URL	Bytes	HTTP return code	URL payload transfe
08-27 14:02:42	Local	192.168.1.12	80	192.168.1.121	192.168.1.12/ipmDb2Servlet	591034	200	2898.27ms
08-27 14:03:09	Local	192.168.1.12	80	192.168.1.121	192.168.1.12/alertStatistic	2461	200	<1ms
08-27 14:00:59	Local	192.168.1.12	80	192.168.1.106	192.168.1.12/netStatistic	1152	200	<1ms
08-27 13:59:13	Local	192.168.1.12	80	192.168.1.100	192.168.1.12/netStatistic	1315	200	<1ms
08-27 14:01:01	Local	192.168.1.12	80	192.168.1.106	192.168.1.12/ipmAlarmServlet	1548	200	<1ms
08-27 13:59:07	Local	192.168.1.12	80	192.168.1.100	192.168.1.12/alertStatistic	3219	200	5.01ms

11.4. Raw packet

When the network traffic storage function is enabled, XPM will Packet the network traffic in the Raw Packet format and store it in the local storage location. The user can extract the original packet through TCP/UDP communication, or application layer session, or specify the extraction time and quintuple form.

11.5. Relationships between four data formats

- The graphical data of a KPI/KQI is the average or cumulative value of the KPI/KQI of multiple communication pairs or application sessions;
- The threshold value of alarm is based on graphical data, and the trigger principle is that the real time value exceeds the set threshold value.
- The corresponding communication pair or session can be obtained by drilling the graphical data.
- If traffic tracing is enabled, the Raw Packet can be downloaded from a communication pair or session.

In short, all functions and usage scenarios of XPM are developed around these four kinds of data. Therefore, an accurate understanding of the logical and technical relationships of these four

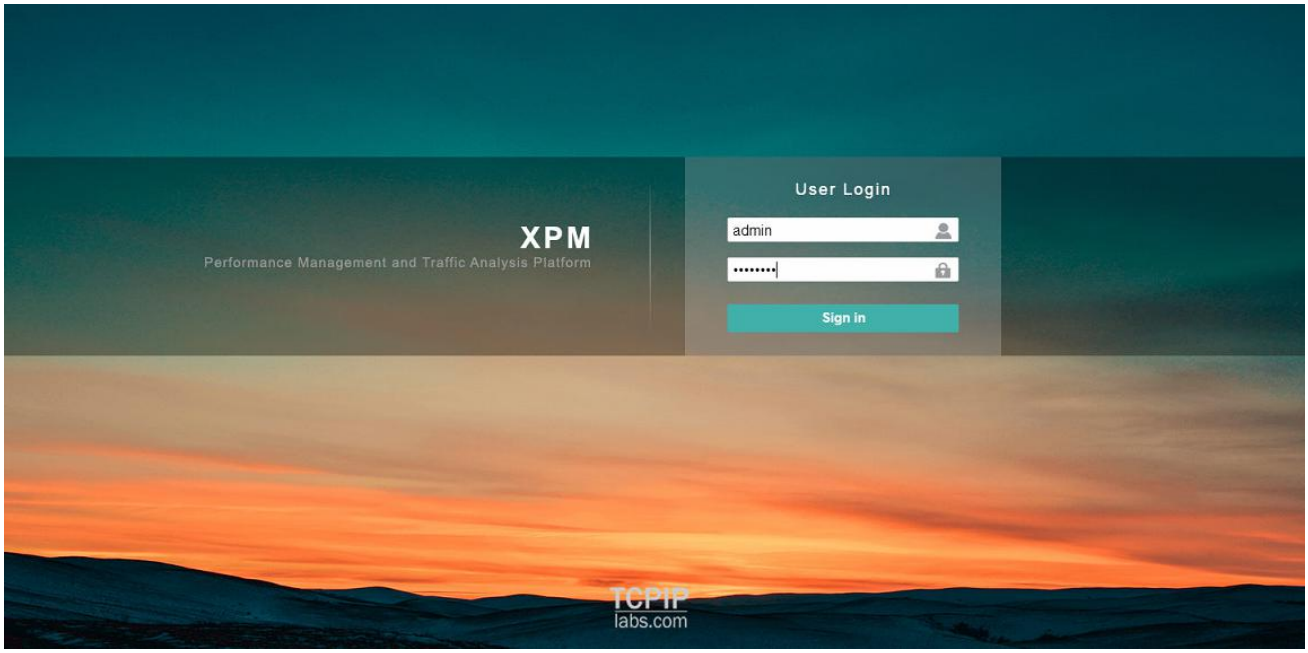
kinds of data is of fundamental significance for learning and using XPM.

12. Get authorization to use and activate XPM

12.1. Login System

12.1.1. First login XPM

- Visit XPM's management IP through browser to access and use XPM. The first normal login interface is as follows
- If the following page is not displayed, please check whether the management IP is configured correctly or whether the Ping Management IP is connected.
- If the display is not normal, the browser needs to be replaced. The browser support is shown in the following section.



12.1.2. Types of browsers supported by XPM

- Browsers of Chrome or Chrome Kernel, Firefox Browser and Microsoft Edge Browser in the past three years;
- Microsoft's IE browser only supports versions above IE10, which are lower than IE10, and may display or use abnormalities.

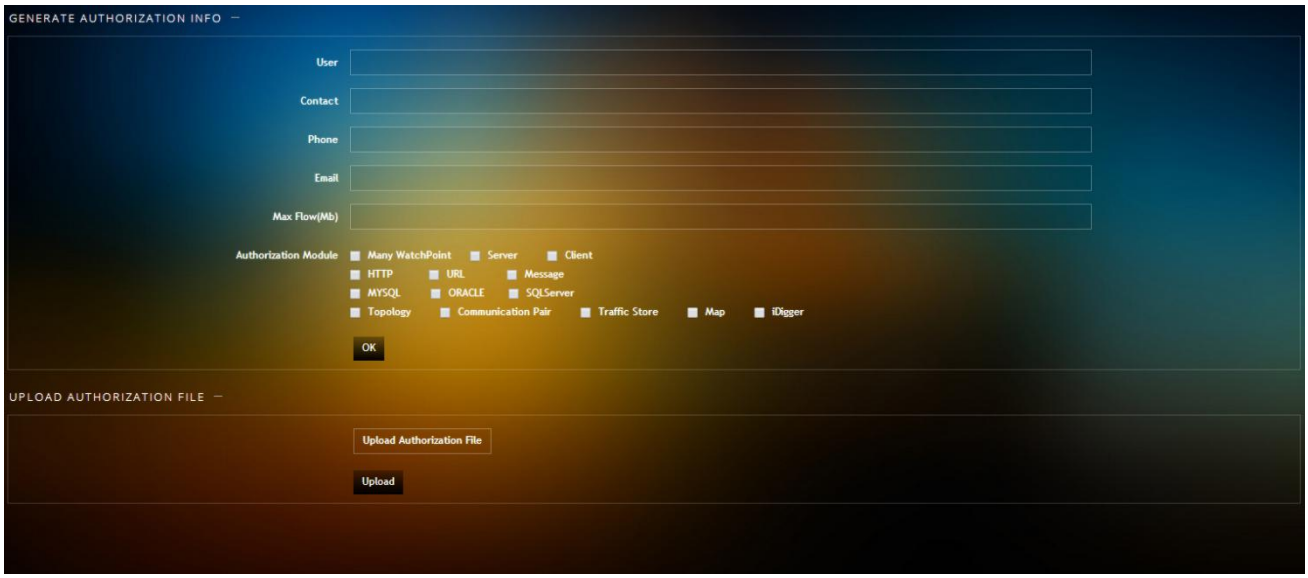
12.1.3. XPM's default account number and password are

- user：admin
- password：ptcs1608

Please change your password and add a new account as soon as possible after you log in.

12.2. Get authorization to use and activate XPM

- After the user enters the correct account number and password, the system will automatically jump to the authorization application and upload page whether it is a free version or a fee version.
- Users need to fill in the real user information carefully according to the content of the page, then generate an authorization application file and send it to tcpiplabs@outlook.com by mail to obtain authorization documents.
- Without authorization files, you will not be able to use XPM.
- Authorization application page is as follows:



12.3. Authorization function page usage instructions

- Maximum Analytical Traffic: It refers to the maximum peak traffic that users mirror to XPM. If users do not know the size of the traffic, they can estimate an upper limit. Please pay special attention to the fact that XPM automatically discards packets that exceed the upper

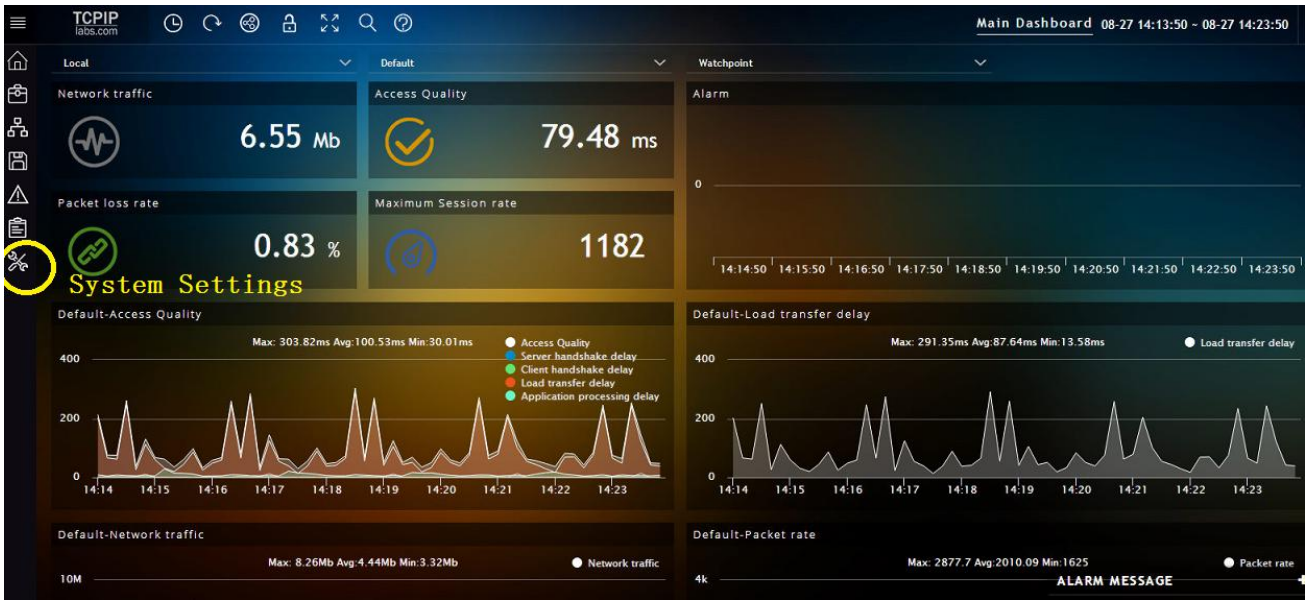
limit.

- For most users, the function of the authorization module is charged, so please consult service@protocolsoft.com or XPM online IM before checking the module to find out the price of each module.
- After correctly filling in the relevant content of this page, click on "OK", the system will automatically generate an encrypted file, send the encrypted file to service@protocolsoft.com , and wait for the authorization file.
- The process of activating XPM can be completed by clicking on the newly acquired authorization file under the function of uploading authorization file.

13. System settings

13.1. How to access the system setup function

On the default home page of the product, at the yellow circle position shown in the following figure, you can click on the system settings function.



The main interface of the system settings after entering is shown in the following figure:

There are five main functional groups in the system settings, from top to bottom, respectively:

A. System setup and management

B. Product renewal and authorization

C. Account management

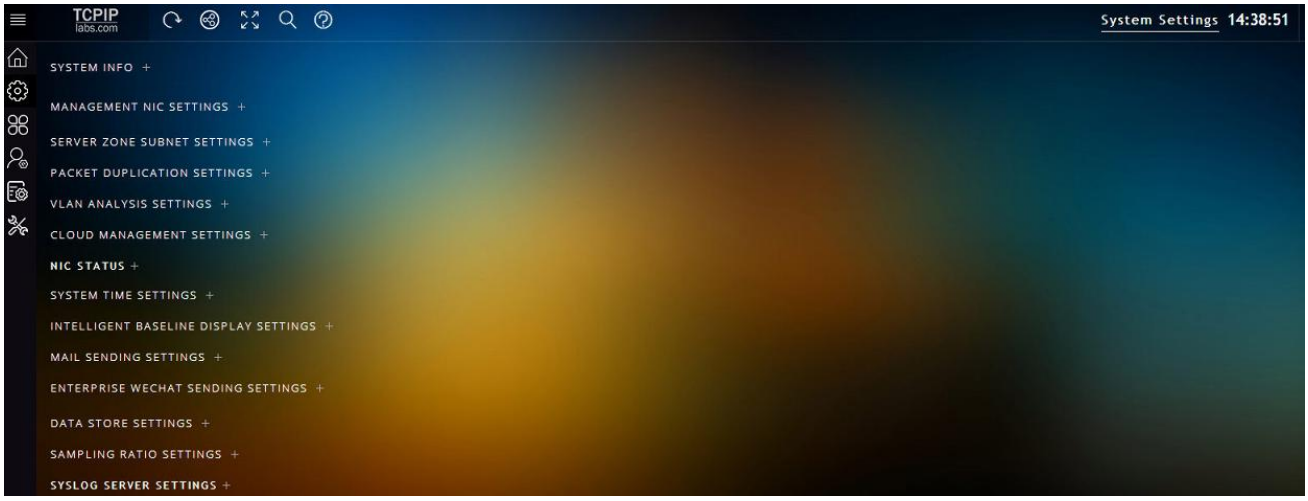
D. System log

E. System tools

Now, each functional group will be introduced in detail one by one.

13.2. System Setup and Management

Click on the [-] next to the system information as shown in the figure above to retrieve the function of the system information. The system setup and management interface after collection are as follows:



Each sub-function of system setup and management is described below:

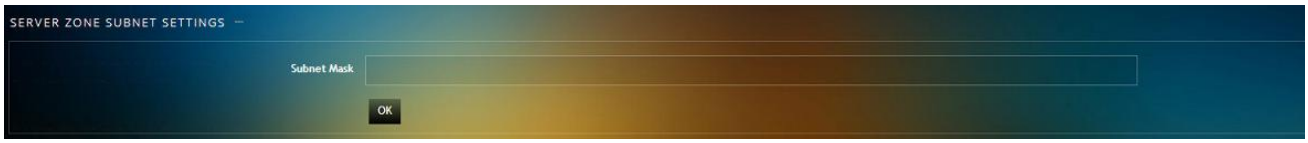
13.2.1. System Information

The information displayed by this function is the relevant content filled in when the user applies for authorization. The user needs to confirm again whether it is consistent with the authorization information applied for. This function cannot be edited and operated.

13.2.2. Manage network port settings

- XPM is a product of B/S architecture. When installing hardware or virtual machine of XPM, users must configure at least two network ports, one is the work port (without IP), and the other is the management network port (need to configure IP). Through the IP of the management network port, users can access and use XPM by browser.
- When browsers access XPM management IP, the default is HTTP protocol, using 80 ports;
- Although the management ports have been set up during the installation of XPM mirrors, users can adjust the management ports in this location if they want to change.

13.2.3. Intranet segment settings



- Intranet segment refers to the IP located in the server area of the back end (internal test) of the XPM deployment location.
- Correct input and complete network segment in server area are the most important settings for XPM to output correct downlink and downlink traffic and related KPIs.
- Please pay special attention to: do not set the IP of the public network, or the client IP accessing the server area to this location!
- The default input method is the standard subnet input method.

13.2.4. Packet de-duplication

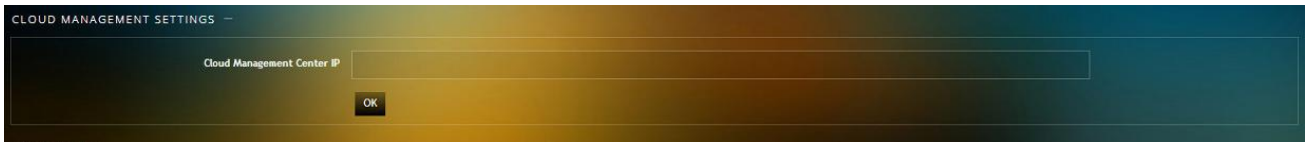
- The default state is off

- This function is used to filter the repetitive flow that may occur during the mirror image process. This situation is more common, especially when it is necessary to mirror both the north-south flow and the East-West flow.
- After the system is installed, the packet de-duplication function of XPM is turned off by default, because the traffic received by XPM needs to be checked with the traffic of SNMP network management to confirm the correct access.
- Please pay special attention to the fact that once the access traffic is confirmed to be the same as that of SNMP network management, the packet de-duplication function needs to be activated immediately. Otherwise, many KPI accounting errors occur.

13.2.5. VLAN analysis settings

- The default state is on
- This function is used to identify traffic labeled with VLAN through Traffic Gathering Device (TAP), which is usually used to identify mirror traffic from different switches; Namely, if TAP device is used to label VLAN for different image traffic, this function must be turned on.
- Note that the VLAN recognition here is different from the VLAN used for partitioning network access, but all are in the same byte location as the IP packet, except that the bit location is different.

13.2.6. Cloud management settings

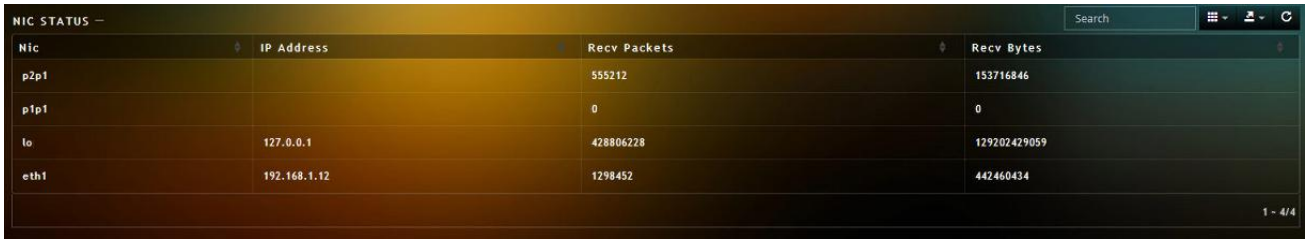


- XPM provides cloud monitoring services to help users perform watchkeeping and monitoring; the service is a fee-based service.
- The user enters the correct service center IP, that is to say, the user agrees to the XPM

service center located in the cloud and receives the important basic indicators of the user's local XPM.

- Local XPM systems only upload graphical data, other types of data are not uploaded, including but not limited to communication pairs, application sessions, raw data packets, or other configuration information.
- Users can get the IP of XPM cloud service center through mail service@protocolsoft.com or XPM online IM.
- Engineers in XPM service centers will contact users through email, IM or other methods to avoid serious accidents when they find abnormal XPM monitoring indicators uploaded locally by users.

13.2.7. Network Card Status



- This function has no editing function; it can only be used to display the relevant information of the network card.
- The most important purpose of this function is to help users determine which network port is the workport and which is idle by judging the number of data packets and bytes when there are more network ports.
- When the network card name of the workport is confirmed, the watch point function can be set correctly.

13.2.8. System Time Settings

- The default system time of XPM is the time of installing the hardware server or virtual machine

of XPM.

- If the time is not accurate, you can also set up a time synchronization server at this function. After setting up, XPM will use the time of the time synchronization server as the time of XPM system.
- Please pay special attention to: if the time used to access the XPM user's personal computer is quite different from the time spent on the XPM server, it will cause abnormal data and display!

13.2.9. Intelligent Baseline Display Settings

- This function is aimed at the alarm function, the KPI which opens the intelligent baseline alarm is effective; the alarm function will be described in detail in the next page.
- This function is turned off by default; when turned on, the intelligent baseline will appear in the KPI graphics with the intelligent baseline alarm set up.
- But please pay special attention: after setting up the intelligent baseline function, it takes at least 7 days to see the baseline in the relevant KPI graphics.

13.2.10. Mail Sending Settings

- This function is used as a mailbox for sending reports.
- SMTP service mailbox needs to be able to communicate with XPM.

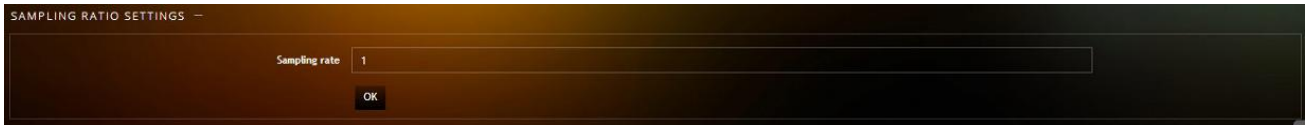
13.2.11. Enterprise Wechat Sending Settings

- Users can configure this function to send the alert information of XPM to the enterprise Wechat client of relevant users through enterprise Wechat.

13.2.12. Data storage settings

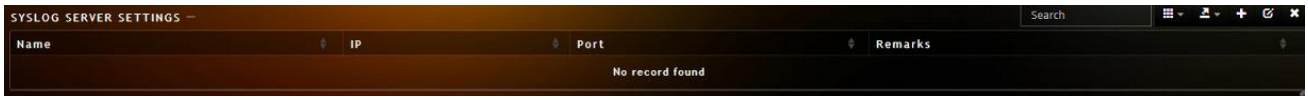
- This function is mainly aimed at traffic storage and backtracking function.
- File size refers to the size of each file that stores the original traffic. It is recommended to use 500MB when the traffic is less than 5Gbps, and 1GB when the traffic is greater than 5Gbps.
- This function is not inconsistent with the partition of disk space in XPM installation. The utilization of disk here refers to the percentage of the partitioned disk space in system installation, which is a protection measure for some special cases.
- Whether it is traffic storage, local (storage of communication pairs or application sessions) database, or graphical data storage, the system adopts FIFO strategy. The specific coverage period is determined by the actual network and business situation of users.

13.2.13. Sampling Proportion Setting



- This function can be used when the user's real-time network traffic is large and may exceed the processing power of the XPM server.
- The default value of this function is 1, which means no sampling; fill in the number 2, which means that TCP/UDP of all network traffic is sampled according to 1/2; fill in the number 3, which means 1/3 sampling;
- The higher the sampling rate, the greater the distortion of the system. At the same time, due to sampling reasons, the corresponding proportion of TCP/UDP or application-level sessions will be lost; therefore, in most cases, it is not recommended to turn on the function, but only retain the default number "1", which means no sampling.

13.2.14. SYSLOG server setting

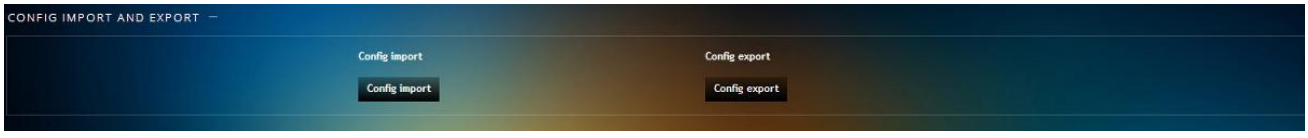


- By properly configuring this function, users can send XPM's SYSLOG and alarm information to other monitoring platforms or large data platforms through SYSLOG mechanism.
- To add the SYSLOG receiving server, please select the [+] in the upper right corner of the list and delete it as [x].

13.3. Product Renewal and Authorization

The main page of product update and authorization is as follows:

13.3.1. Configuration import and export

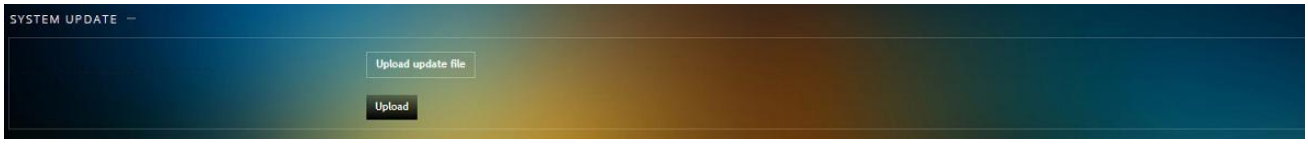


- This function is used for system upgrade, machine migration, and other special cases.
- Since all kinds of information will be related to settings or configurations after users use it for a period of time, if only export configurations, many functions and data may be abnormal. Therefore, unless there is an official XPM statement, it is necessary to upgrade the configuration backup. We do not recommend users to use this function on their own.

13.3.2. Application Configuration EXCEL Import

- This function is mainly aimed at the server and client monitoring functions of XPM.
- This function can be used when there are many clients and servers that users need to set up.
- Users need to click on the template to download, and then import the server and client information that needs to complete the settings one-time according to the format and content of the EXCEL document downloaded to the local site.
- After filling in, click on the EXCEL file and import it into the XPM system, which can complete the settings of several servers and clients at one time.
- It is not recommended to use this function when the number of servers and clients that users need to set is less than 20.

13.3.3. System upgrade



There are two ways to upgrade XPM systems:

- First, through online upgrade, XPM service center will automatically upgrade the XPM server which can communicate remotely.
- Secondly, the upgrade file is sent to the user through the mail message registered by the user. After the user receives the upgrade file on the local computer, the upgrade file is uploaded to the XPM server in this functional location.

13.3.4. Generate authorization information and upload authorization files

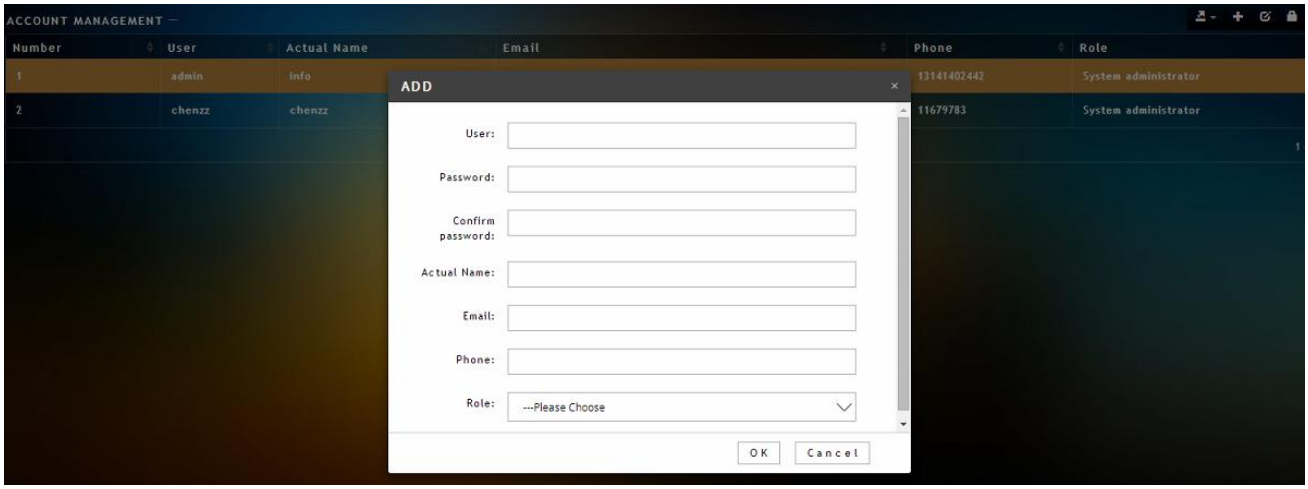
These two functions have been introduced in previous chapters, and will not be covered here.

13.4. Account management

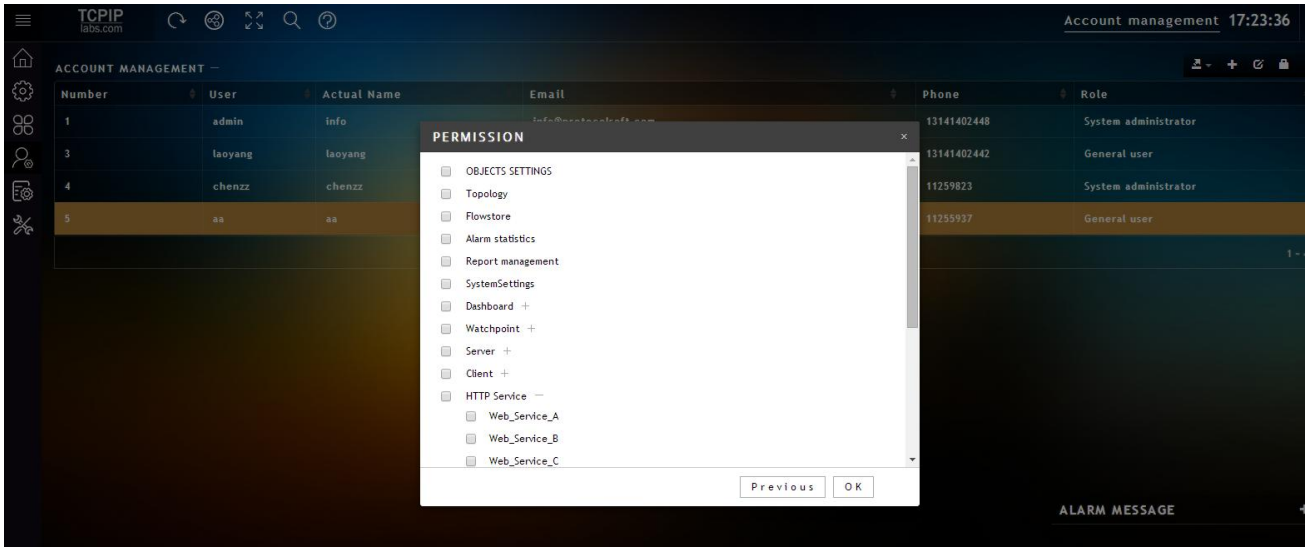
The main interface of the 【Account Management】 function is as follows:

13.4.1. Adding Accounts

- Click on the [+] at the top right corner of the list to pop up the following account window:



- According to the contents of the input box, fill in the relevant contents one by one.
- Please pay special attention to: When the last [role] option is selected, the [confirmation] at the bottom of the window will automatically change to [next step], click [next step], and the system will automatically jump to the following window content. Administrator users can create different permissions for each ordinary user according to the content of the window.



- XPM account management function is very powerful. It can not only authorize the use of functions, but also authorize each monitoring object separately. Without authorized monitoring object, ordinary users can not see its content.

13.4.2. Editing, deleting and modifying passwords in account management

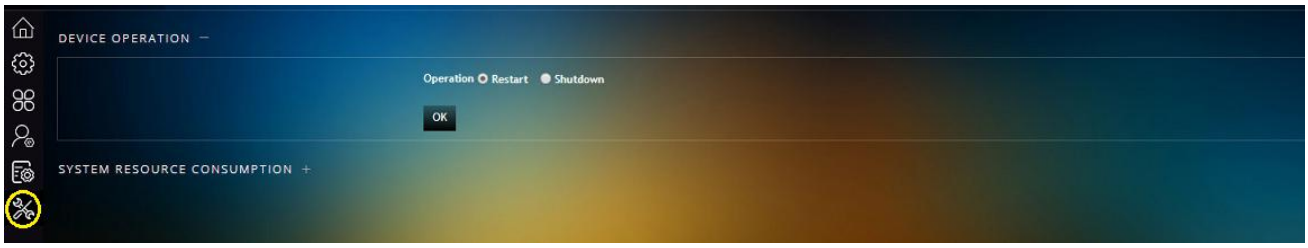
- The three functions are in the upper right corner of the account management list. Users can perform relevant operations according to the pop-up window content of the three functions.

13.5. System log

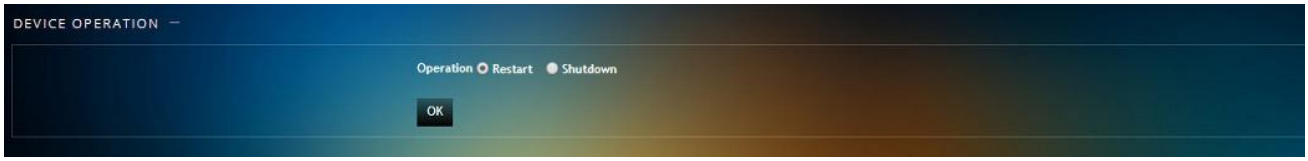
- XPM records each user's actions on XPM's main login, creation, modification, deletion, etc.
- Users cannot edit or delete the recorded operations.
- If you need to export these system logs, you can choose the Export Data function in the upper right corner of the list and the format of the exported file.

13.6. System tools

System tools are an important function of XPM for self-monitoring. In most cases, users do not need to use this function. The main interface of the system tool is shown in the following figure:



13.6.1. Equipment operation



13.6.2. System resource consumption

- Select the time period, and after the start and end time, XPM will open a web page separately, as shown below. Users can view the use of CPU and memory by XPM programs through this web page.
- Users can adjust the content of the page through the [+] at the bottom of the page
- If the system response is slow for a long time in the process of using XPM, it is recommended to use this function to check whether the system load is too high for a long time. If the payload value is higher than 70% for a long time, it means that the system is always in a

busy processing state. In this case, we suggest that the hardware configuration of the system, such as CPU, memory, or the performance of disk array should be increased as soon as possible.

14. Monitoring Object Settings

14.1. Types of monitored objects

Number	Monitoring object	Scope of application
1	Watch Point	Suitable for monitoring network links, operator dedicated lines, network serial devices
2	Server	One or a group of IP or NAT devices that provide services to the outside world; analysis granularity is TCP/UDP connection
3	Client	Client, subnet, branch; analysis granularity is TCP/UDP connection
4	HTTP Service	Network services using HTTP protocol; Web, middleware, etc. Analysis granularity is HTTP session.
5	Oracle Service	Oracle database; analysis granularity is Oracle SQL statement
6	MySQL Service	MySQL database; analysis granularity is MySQL SQL statement
7	SQLserver Service	SQL server database; analysis granularity is SQL server SQL statement
8	URL Service	Web services defined by business using URLs; analysis granularity is HTTP session
9	Message transaction	Use JSON, XML, HTML for business defined services; Analysis granularity is HTTP session
10	Application Availability	IP: Port, which provides services to the outside world; dial-up form, which only monitors the survival status

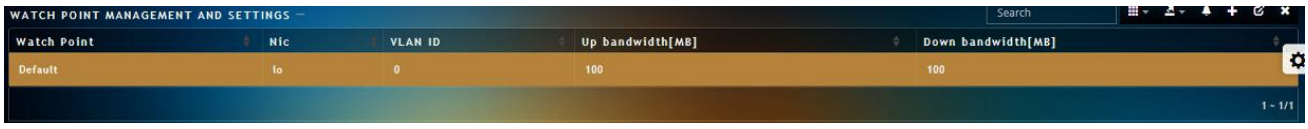
14.2. Enter monitoring object settings

Default home page, left main function bar, the second function is [monitoring object settings]

When you click on it, you can see the following:

14.3. Management and setup of watch points

- Watch points refer to the traffic mirror points of switches, and also support VXLAN, MPLS tunnel protocols as a kind of mirror traffic, usually more than one watch point;
- Watch points are usually used as monitoring network links, serial network equipment, operator dedicated lines.

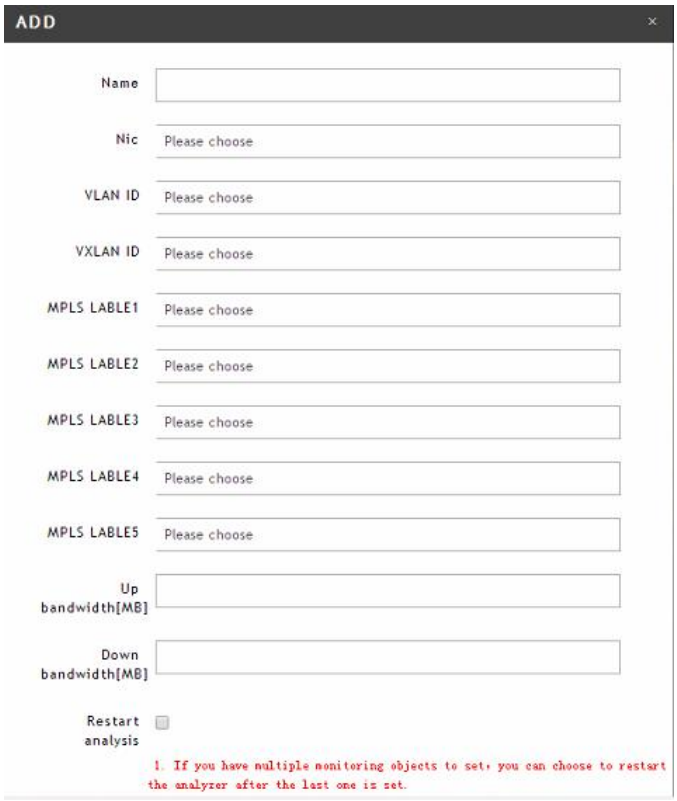


14.3.1. Add, edit, delete watch points

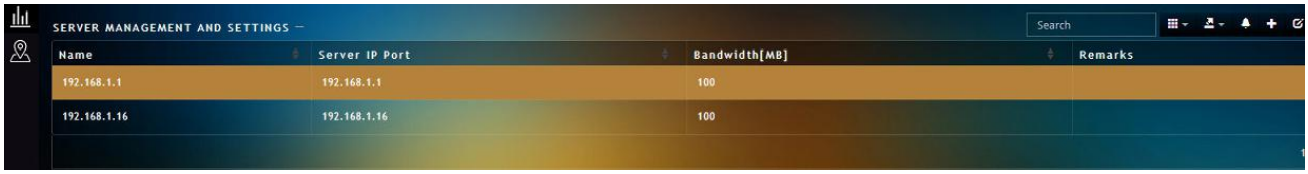
In the upper right corner of the list of watch points, the functions are as follows: column selection, data export, alarm settings, additions, modifications, deletions; these functions can be completed

by pop-up window prompts. Points to be noted include:

- XPM supports aggregating multiple network ports (VXLAN/MPLS) into one watch point
- The upstream and downstream bandwidth must be set, which is related to bandwidth utilization; for full-duplex ethernet, both are bidirectional at the same rate

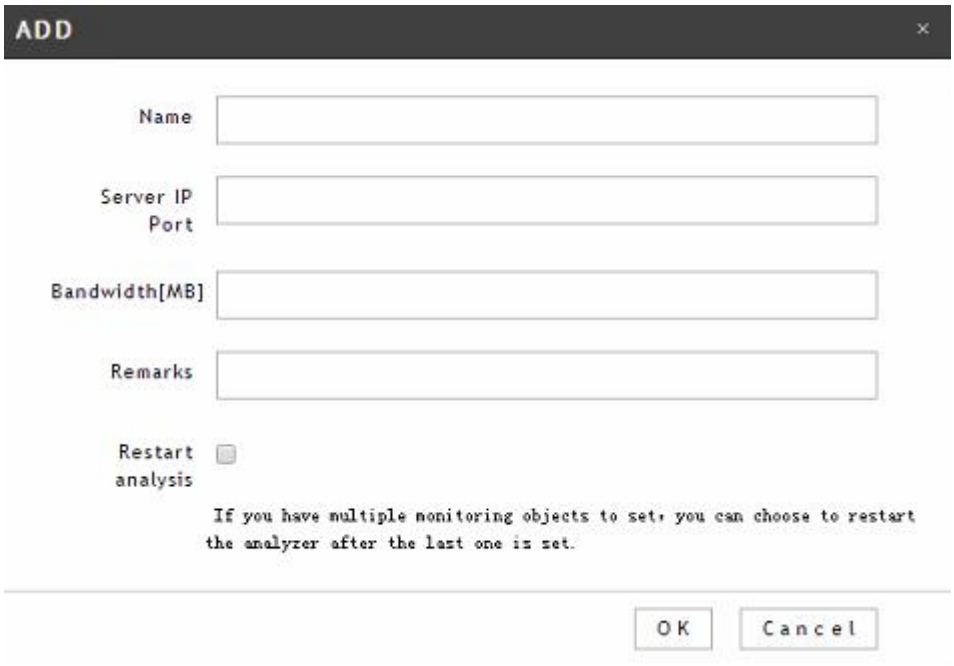


14.4. Server management and setup



In the upper right corner of the server list, the functions are as follows: column selection, export data, alarm settings, add, modify, delete; these functions can be completed by pop-up window prompt. Points to be noted include:

- The expression of server input must be matched strictly according to the prompt of pop-up window.
- When adding, modifying or deleting server settings, the relevant analysis program needs to be restarted, so breakpoints may occur on the graphics.



14.5. Client Management and Settings

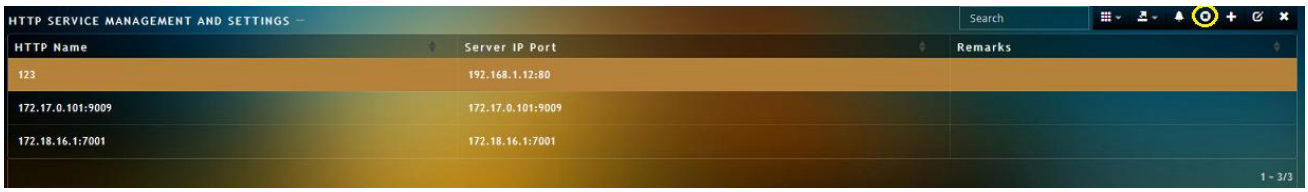
The content is similar to that of the server, please refer to the previous section "Server Setup and Management".

14.6. HTTP Service Management and Settings

HTTP service management and settings, the main content is similar to the server side, please refer to the previous section "Service side settings and management". But there are two main points to pay special attention to:

14.6.1. Parse and store HTTP load segment message content and retrieve keywords

- The fourth function of the Quick Function Bar in the upper right corner of the HTTP Service List (Open Load Storage) is a unique feature of HTTP.

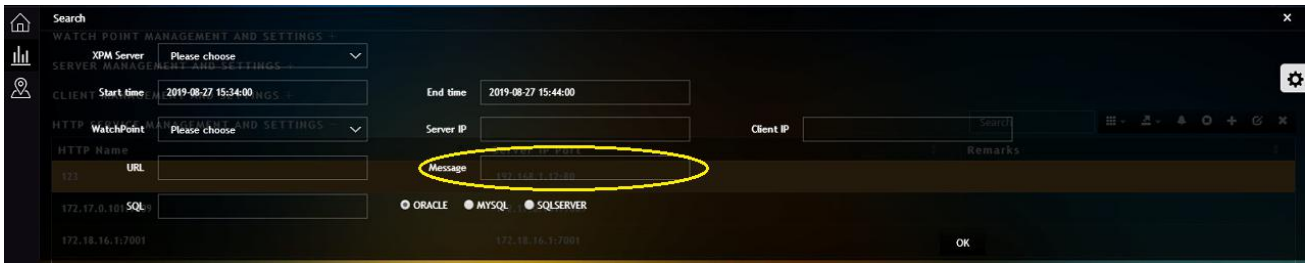


- This function can parse the JSON, XML and HTML contents of the load segment and write them

to the local database.

- The main application scenarios for this feature are applicable to queries and audits of various business data, such as forms.
- Query function is located in the top of the product page in the Quick Toolbar, the fourth function [Search Query], as follows:

Click on the search query function to pop up the following window:



Select the XPM server one by one, time, and input the characteristic text of the load segment that needs to be queried in the [message] input box. XPM can output the content of the text and the corresponding HTTP session.

14.7. Oracle/MySQL/SQLserver Service Management and Settings

In addition to the IP and Port expressions of the monitoring objects are different from those of the server side, the functions of adding, modifying and deleting the monitoring objects in these three databases are basically the same as those of the server side. Please refer to the section on management and setup of the server side.

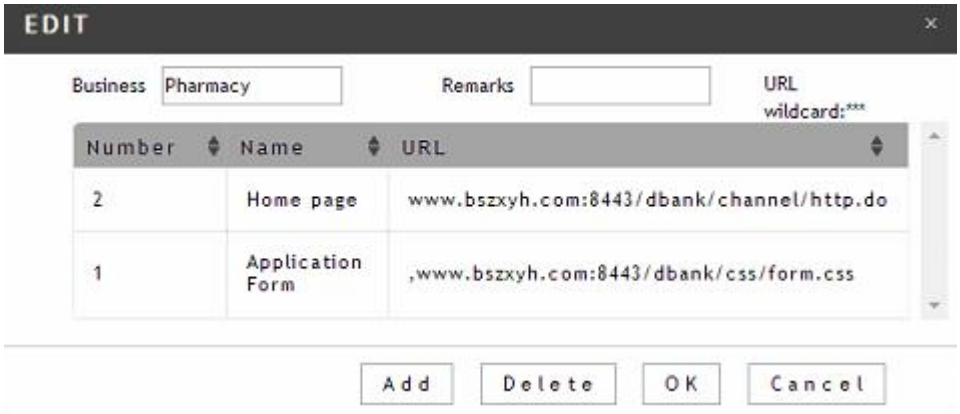
14.8. URL Service Management and Settings

- URL transaction monitoring is one of the features of XPM, and it is also a very practical business-level monitoring function!
- We know that most B/S architecture businesses have many URLs on their front pages. Only part of these URLs perform specific business operations. The rest, such as static picture URLs and style URLs, are not business-level interactions. Obviously, all URLs are monitored and output based on these URLs. The relevant indicators are obviously inaccurate or even wrong.

Therefore, independent monitoring and analysis of URLs carrying business interaction content is the functional understanding that meets business needs. XPM's URL service performance monitoring is a functional group designed specifically for this application scenario.

14.8.1. How to monitor a multi-step URL service?

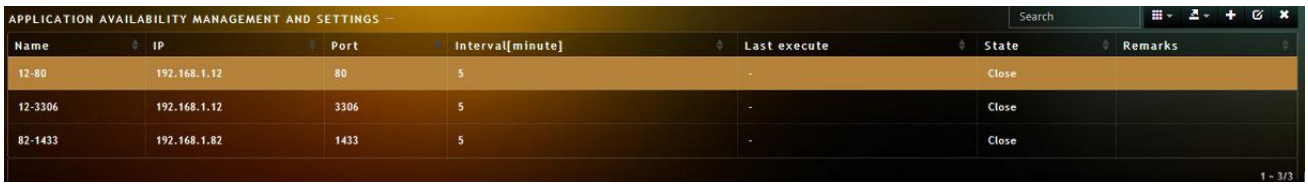
URL transactions are composed of several operations, each operation is a URL that interacts with the day after tomorrow. Therefore, these URLs can be combined into a monitoring object to complete the monitoring and analysis of this business. Click on the URL service management and settings list in the upper right corner of the new function [+], or modify [✎], you can pop up the following window:



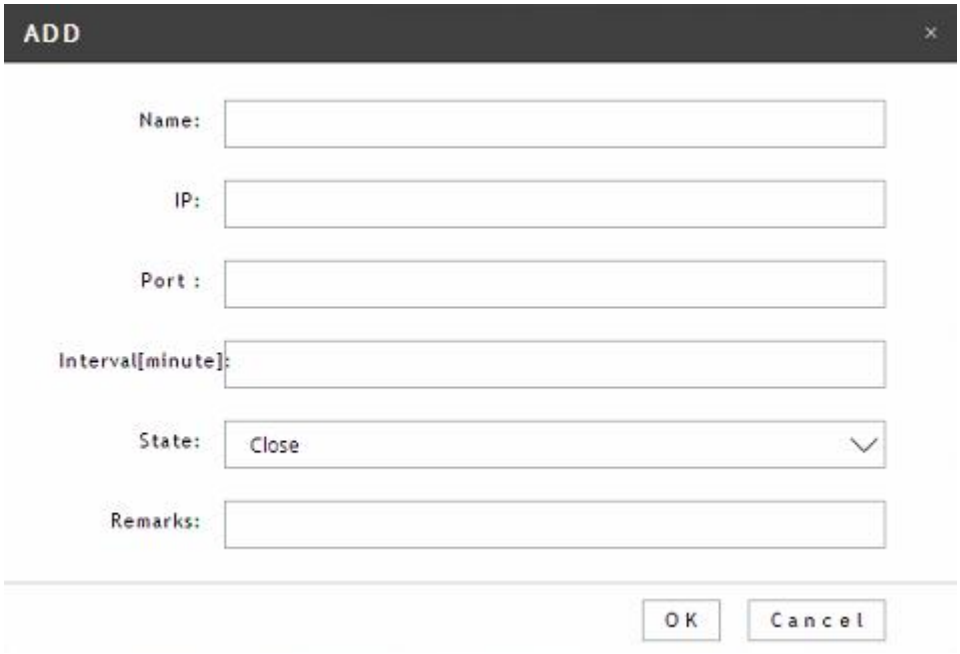
According to the function hints in the window, you can add or modify a business consisting of multiple URLs.

14.9. Application Availability Management and Settings

Usability management is to use dial-up method to detect the port of the server to confirm whether the service is normal or downtime. This function is often used in basic monitoring.



Click on the Apply Availability Management and Settings list in the upper right corner to add a new function [+], or modify [✎], you can pop up the following window:



The user can complete each setting according to the prompt of the pop-up window.

15. Warning-related functions

15.1. Essentials of Alarm Algorithms Must Be Knowledged

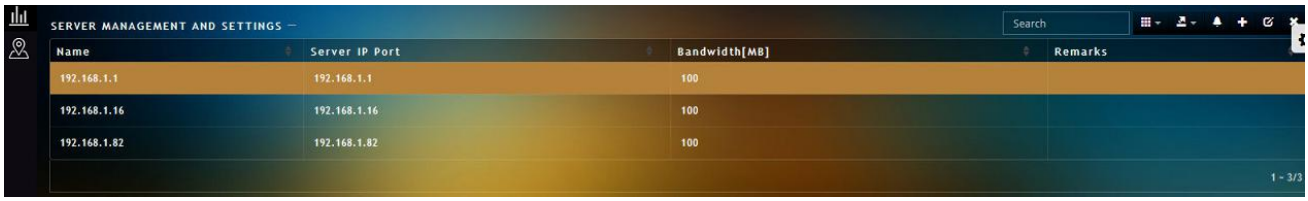
For XPM alert algorithm, the following points need to be specifically explained:

- XPM can be divided into manual threshold and intelligent alarm for all monitoring objects.
- Both alarm algorithms are triggered by the average value of an index of the monitored object, which is the average value of the index of all TCP/UDP or application sessions in the current period.
- For performance indicators, we recommend artificial threshold, and for status indicators, we recommend intelligent alarm algorithm.
- Artificial threshold and intelligent alarm can set high threshold and low threshold and send out alarm.
- There are three levels of artificial thresholds: ordinary, important and urgent.
- Intelligent alert has only one level, which is determined by the percentage of the current KPI value exceeding the baseline.
- XPM adopts a more reasonable baseline algorithm, which effectively avoids the effect of multiple extremes on baseline deviation.
- In order to reduce false alarm and false alarm ratio, XPM adopts reasonable alarm suppression algorithm, which can effectively avoid the impact of occasional short peaks or troughs on alarm.

15.2. Alarm threshold setting

15.2.1. Functional Entry of Alarm Threshold Setting

- The alarm settings for all monitored objects are completed in the second main function of the left toolbar, which is the alarm settings. The specific function locates in the upper right corner of each monitored object list, which is indicated by. The following figure shows the alarm settings.



- After clicking the alarm settings function [🔔], the page will automatically move down to the KPI/KQI list of the monitored object, as follows:

- Select the KPI/KQI that needs to be set with the mouse and click on the modification function in the upper right corner of the list, which will pop up the alert setting window of the KPI/KQI, as shown below.

The setting of this window is very important. Be sure to understand the following:

1) Ordinary alarm, important alarm and emergency alarm are all effective to artificial

threshold algorithm.

2) Four input boxes on the left are valid for low thresholds; four input boxes on the right are valid for high thresholds.

3) When the threshold value is input, whether the alarm function for KPI/KQI is turned on or not depends on whether the selection boxes of low threshold and high threshold are checked after threshold opening.

4) For performance indicators, we recommend artificial threshold; for status indicators, we recommend intelligent alarm algorithm.

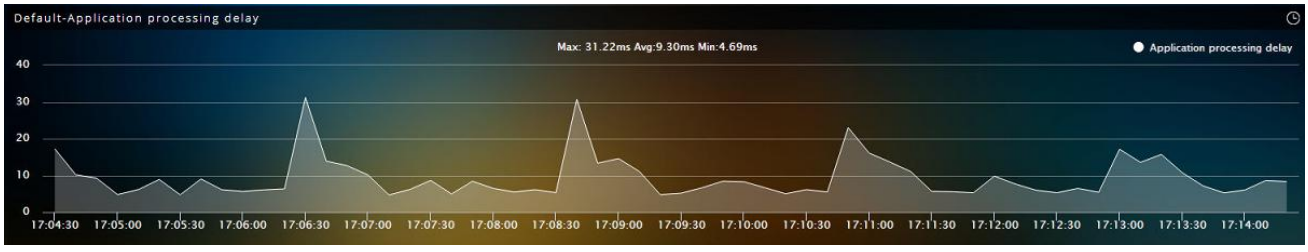
5) Intelligent alarm settings need to run for at least 7 days before it can take effect.

6) If multiple monitored objects of the same type need to set the same KPI/KQI threshold, check Global Settings to reduce settings repeatability and workload.

15.2.2. How to Reasonably Set the Warning Threshold of Performance Index KQI

As mentioned earlier, we strongly recommend that artificial thresholds be used for KQI (time-based, error-based, unresponsive-based) because these indicators are related to business quality and user perception and have a relatively reasonable and fixed range. So, how to determine the reasonable threshold range of KQI?

We suggest that if there is no accident or complaint in the past few days, the peak or valley value of these days can be used as the artificial threshold, the high and low threshold of ordinary alarm, the important alarm will float up 50%, and the emergency alarm will float up 100%. For example:



For this legend, we propose a warning threshold of 1000ms for general notice, 1500ms for important warning and 2000 ms for emergency warning.

15.2.3. How to Set the Warning Threshold of State Indicator KPI Reasonably

Because the state index KPI has no absolute reasonable range, such as network traffic, session volume, packet rate, etc., but mutation represents a risk or anomaly, it is more appropriate to use intelligent alarm algorithm.

In order to reduce the probability of false alarm and false alarm, we suggest that the threshold of intelligent alarm should not be less than 100% for most business or network environments without stable operation rules. That is, when the current value of a KPI exceeds 100% of the baseline value of the past seven days, an alarm is issued.

15.3. Acquisition and drilling of alarm information

15.3.1. Acquisition of alarm information

XPM warning alert has three places: warning information floating window, default dashboard warning bar chart, business chain dashboard small list of health.

- [Warning Information]Floating window, in the lower right part of the page; as shown below, click on the [+] on the right side of the floating window to expand the alarm content.

- Alarm histogram of default dashboard

- Health of business chain dashboard list

15.3.2. The drilling of alarm information

- Click [Alarm Information]-> Jump to [Alarm Graphics]-> Drag the Peak or Valley of the Alarm Graphics -> to get the [Communication Pair or Session] that causes the alarm to occur.

Starting time	ServerIP	ClientIP	Network traffic	Attempt connection	Round trip time
08-27 17:24:00 ~ 08-27 17:26:20	172.17.0.102	117.136.41.127	2.11Mb	8	338.85ms
08-27 17:24:30 ~ 08-27 17:26:50	172.26.201.99	172.26.28.75	49.86Kb	4	220.05ms
08-27 17:24:30 ~ 08-27 17:26:40	172.26.201.1	172.26.8.11	134.11Kb	4	204.56ms
08-27 17:24:30 ~ 08-27 17:26:50	172.26.201.1	172.24.9.20	463.65Kb	0	169.56ms
08-27 17:24:30 ~ 08-27 17:26:50	172.26.201.3	172.26.3.28	543.58Kb	0	154.86ms
08-27 17:24:30 ~ 08-27 17:26:50	172.26.201.99	172.26.16.5	736.08Kb	0	154.19ms
08-27 17:24:30 ~ 08-27 17:26:50	172.26.201.1	172.23.11.8	235.20Kb	0	145.78ms
08-27 17:24:30 ~ 08-27 17:26:40	172.26.201.3	172.21.4.99	200.19Kb	0	137.52ms
08-27 17:23:50 ~ 08-27 17:26:00	172.17.0.102	124.113.19.32	1.74Mb	20	134.36ms
08-27 17:24:30 ~ 08-27 17:26:50	172.26.201.3	172.26.6.47	1.99Mb	0	129.51ms
08-27 17:24:30 ~ 08-27 17:26:50	172.26.201.99	172.22.222.13	406.48Kb	0	121.16ms
08-27 17:24:30 ~ 08-27 17:26:50	172.26.201.3	172.28.10.3	335.50Kb	4	114.28ms
08-27 17:24:40 ~ 08-27 17:26:50	172.26.201.3	172.25.9.52	26.02Kb	4	114.15ms

- If the XPM-H version is available and the traffic storage and traceback function is enabled, click again on any of the communication pairs in the screenshot above, and the page will automatically move down to the 10s clock-size list of communication pairs, as shown below:

DETAIL LIST

Search

Starting time	ServerIP	ClientIP	Network traffic	Attempt connection	Round trip time
08-27 17:24:00	172.17.0.102	117.136.41.127	1.05Mb	4	198.78ms
08-27 17:26:10	172.17.0.102	117.136.41.127	990.86Kb	4	58.77ms
08-27 17:26:20	172.17.0.102	117.136.41.127	64.57Kb	0	759.01ms

ALARM MESSAGE

- Click on the download function in the upper right corner of the list again. According to the prompt, the original traffic of the communication can be downloaded to the local area in PCAP file format. Users can open and do further analysis with the package parsing tools such as Wireshark.

15.4. Statistical analysis function of alarm

15.4.1. Entrance of alarm statistical analysis function

The fifth function of the main function bar on the left, and the lower left corner of the alarm information floating window, have the entrance of this function. As shown in the yellow circle below:

After clicking on the entry, the alarm statistics page is shown as follows:

15.4.2. The field of alarm information

The fields of alarm information include but are not limited to: time, monitoring object, alarm level, alarm type, response status, responder, response time, possible cause, contact, telephone, email;

15.4.3. Dimension of alarm statistical analysis

XPM's alarm statistical analysis function is very powerful. It can make detailed statistical analysis of each alarm information according to the following dimensions.

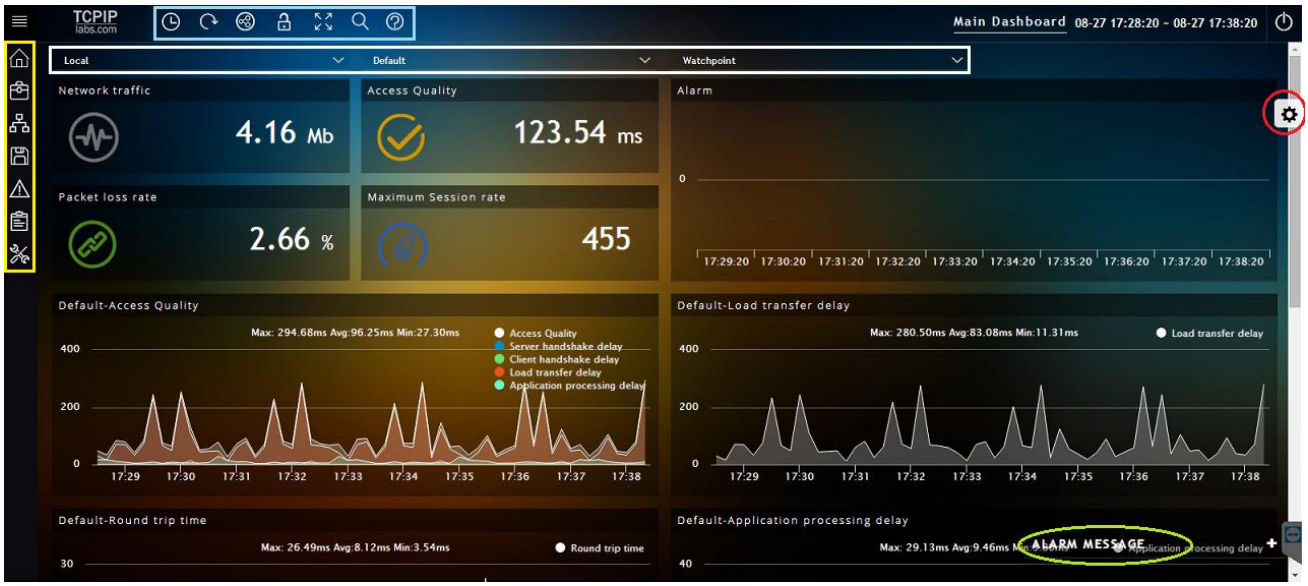
- Time Dimension
- Monitoring Object Dimension
- KPI/KQI Dimension
- Alarm Level Dimension
- Corresponding State Dimensions

Each alarm message after statistical analysis can also be drilled into a communication pair or application session (if it is not covered by new data) by double-clicking.

15.4.4. Exporting alarm information

After statistical analysis, if the alarm information of statistical analysis needs to be output, it can be exported after the file format is selected by the second function in the upper right corner of the alarm information list.

16. Page Operation



16.1. Quick Access Toolbar

Functions in the blue box shown above.

From left to right, the functions are time retrospective, real-time refresh, topology query, dashboard lock, full screen, search query, help.

16.1.1. time retrospective

This function can be the current page, all graphics, figures, a full amount of time back statistics. Different backtracking time periods correspond to different time granularity. The corresponding relationship between backtracking time period and granularity is:

A. backtrack 4 hour, granularity is 10 second

B. backtrack 1 day, granularity is 1 minute

C. backtrack 1 week, granularity is 10 minute

D. backtrack 1 year, granularity is 1 hour

The above time granularity is obtained through full investigation and practice. However, in some cases, when the time interval is longer and the time granularity is larger, the data from backtracking may be different from the actual feeling. However, this is a normal situation, and

the reason is that the time granularity is larger.

16.1.2. Real-time Refresh

This function is mainly aimed at the refresh operation of the current page, not the frequency of real-time calculation. There are four options. From left to right: refresh immediately, 10s, 30s, 60s. Each choice represents the frequency at which the current page updates its data each time.

Please pay special attention to: refresh function is only browser function, not background data calculation frequency; real-time calculation and output frequency of XPM is 10s, which is the fastest for similar products in the industry.

16.1.3. Topology Query

This function is one of the key functions of XPM and is part of the Topology Chart function, which will be described in detail on the next page.

16.1.4. Dashboard Locking

This function is used to lock the dashboard which has been set up at present. After locking, it can not be edited again. It is suitable for multiple users to use the same dashboard.

16.1.5. Full Screen

Click on this function, the user browser will enter the full screen mode and press ESC when it exits. When this function comes into effect, other browser functions that are not related to the display content will be hidden, which is suitable for monitoring the use of large screen.

16.1.6. Search Query

This function is one of the most commonly used general functions in the process of users using XPM. Search and query function, can query and output all monitoring object's inbound information, suitable for user barrier removal, or handling customer complaints.

A. TCP/UDP communication pair. The query condition is server IP or client IP.

B. HTTP/URL services. The query condition is the key words in the URL or the URL.

C. Oracle/MySQL/SQLserver。The query condition is keywords in SQL

D. For users who have opened HTTP load warehousing or message transaction monitoring, queries can be made by searching the keywords of the load segment.

16.1.7. Help

For some of the main pages, we will prompt the operation of the page help, we strongly recommend that users should be proficient in grasping the basic operation of these commonly used pages.

At the bottom of the pop-up window, there are also links to this User Manual.

16.2. Main Function Bar

In the yellow box above.

From top to bottom the functions are: home page, monitoring object settings, topology, traffic storage, alarm statistics, report management, system settings.

- Home page. The default home page of the system is the dashboard of the monitored object.
- Monitor object settings. It has been introduced on the previous page. See related content.
- Topology diagram. It will be introduced in separate chapters on the next page
- Flow storage. This feature is only valid for XPM-H, which will be described in a separate section on the next page; XPM-S and XPM-V will not load the function.
- Warning statistics. It has been introduced on the previous page. See related content.
- Report management. It will be introduced in separate chapters on the next page.
- System settings. It has been introduced on the previous page, please refer to the relevant content.

16.3. Online IM Help

In the purple circle in the lower left corner of the page.

This function is only valid for the Chinese version of XPM, and only for the users who have purchased

online services, but not for the English version.

On the premise that XPM can communicate with the Internet, clicking on this function can show the following picture. Users can communicate online with experts of XPM, and help users solve some problems of product use and application scenarios efficiently.

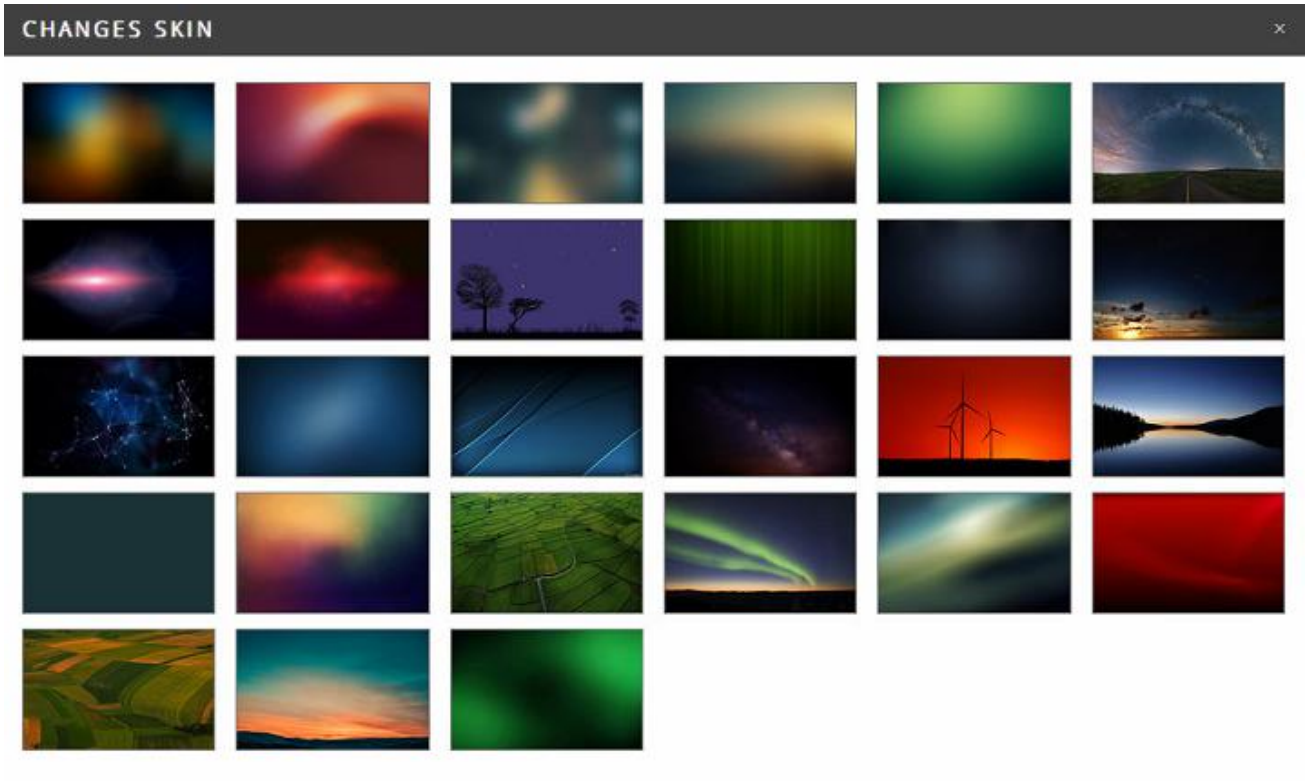
16.4. Warning information floating window

In the green circle in the lower right corner of the page. Relevant content of alarm floating window has been introduced on the previous page, please see the relevant chapters.

16.5. Skin Settings

On the top right side of the page, next to the scrollbar, in a red circle.

XPM Web pages adopt translucent design style, so the page background can also be replaced by skin setting function, which is very beautiful and gorgeous. The background of the default load is shown in the following figure :


CHANGES SKIN

17. Three Functions and operation of dashboard

XPM has excellent ease of use. Taking the dashboard for daily monitoring purposes as an example, XPM provides three scenarios, which can be adapted to three application scenarios:

Name of dashboard	用途与应用场景
Monitoring object dashboard	The default home page of the system landing can monitor every monitoring object comprehensively.
Statistical analysis of dashboard	All monitoring objects of a certain type of monitoring can be analyzed and compared horizontally.
Business Chain Dashboard	The fully customized dashboard can be used to monitor the vertical business chain shape of different types of monitoring objects, and can be used as the upper screen interface of monitoring large screen.

17.1. Monitoring object dashboard

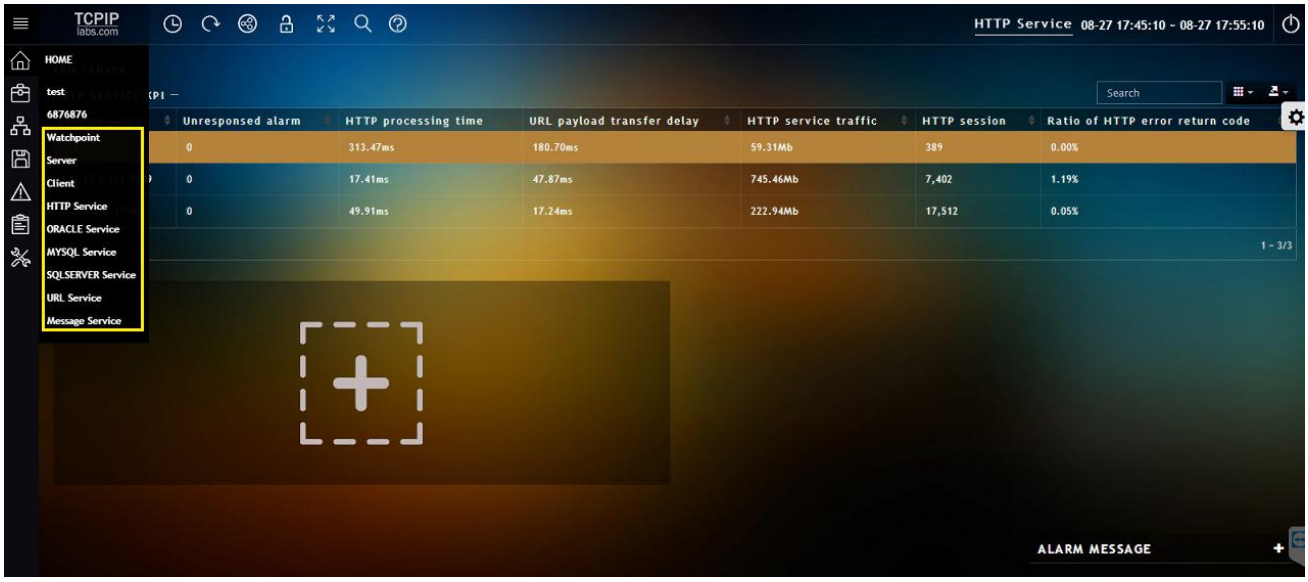
The default home page after the system logs in; after each user logs in, the system records the content of the default home page and presents it the next time he logs in.

- By choosing the drop-down menu of the yellow box in the picture, the monitoring object of the dashboard can be changed.

- The monitoring indicator KPI/KQI corresponding to the four digits in the upper right corner and the alarm bar chart on the right side cannot be changed.
- Other graphics can be added and modified by the 【+】 at the end.
- All data and graphics of the dashboard can be traced back through the quick toolbar at the top of the page.
- All the numbers and graphics on the page (including bar chart, line chart, pie chart, etc.) can be drilled into TCP/UDP communication pairs or application sessions.

17.2. Statistical analysis of dashboard

Statistical analysis of the dashboard can be used to compare different monitoring objects of the same type horizontally, especially when combined with the function of "time traceback" of the shortcut toolbar, which services are the worst and which are the most active can be quickly found.



- Click on the column name of the list to sort the KPI/KQI values of the column.
- In the first column, select any monitored object, and the graph below the list will change to the content of the monitored object.
- All the numbers in the list, as well as the graphics below, can be further drilled into TCP/UDP communication pairs or application sessions.
- The contents of the list can be exported to a specific format file through the data export function in the upper right corner of the list.

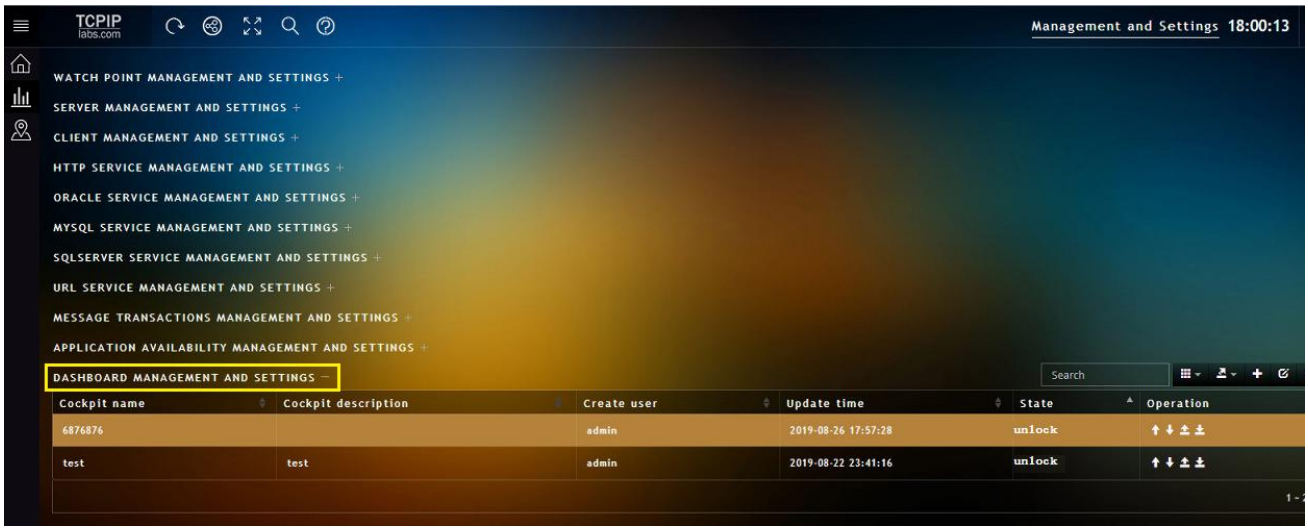
17.3. Business Chain Dashboard

Business chain dashboard is an important tool for daily monitoring of XPM users, and its function is very powerful; The main manifestations are as follows:

- Full drawing board dashboard, users can customize to build, change its content.
- There are also text, links, rounded boxes, icon examples and other auxiliary annotation and beautification functions.
- An XPM system that can create multiple business chain dashboards and grant privileges to different users.
- Business chain dashboard has a small list of monitored objects and health function, which is very suitable for screen display.
- Inside the dashboard, you can add small lists, graphics and other elements.
- The complete drilling function can be realized by adding numbers and graphics to the dashboard.

17.3.1. How to create a new business chain dashboard?

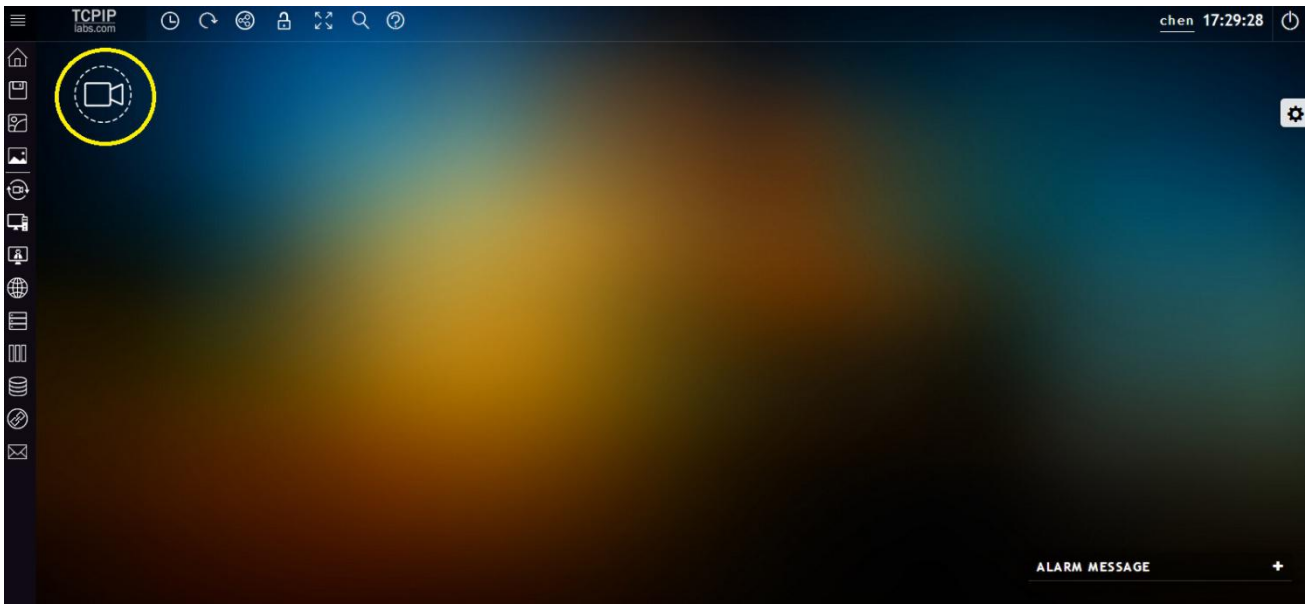
This function is the last function of [Monitoring Object Settings], [Dashboard Management and Settings]. Like the following figure:



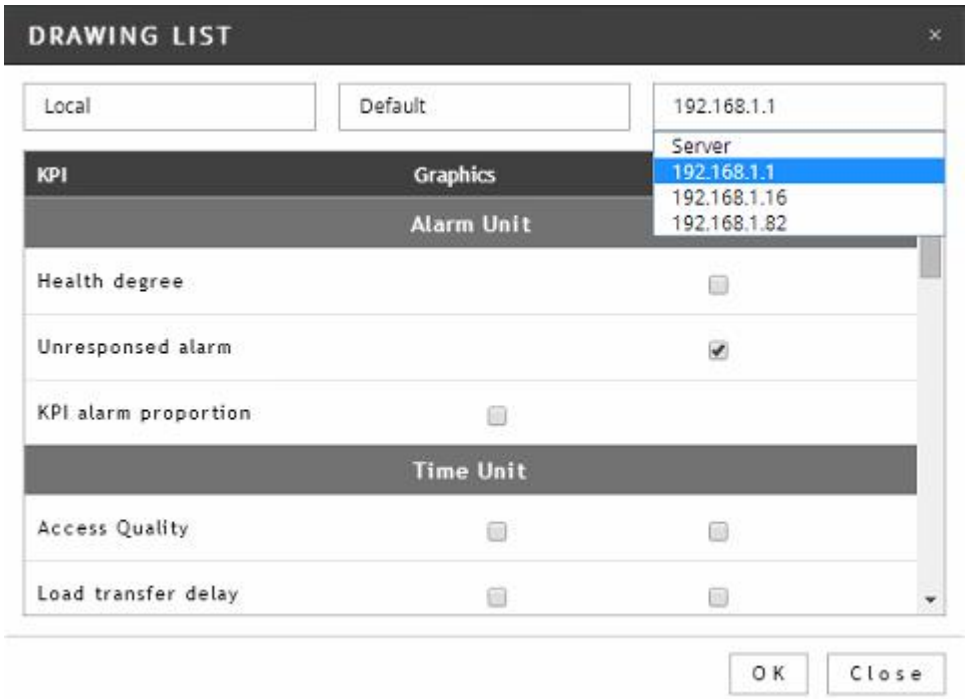
Click on the 【+】 in the upper right corner of the dashboard list to complete the creation, modification and deletion of the business chain dashboard according to the prompt of the pop-up window.

17.3.2. How to add, modify and delete the contents of business chain dashboard?

- After creating the business chain dashboard, users need to refresh the browser page once, that is, they will find the newly created dashboard in the menu that pops up on the first icon of the main function bar on the right. Click on the new dashboard to enter the dashboard page, as shown below:
- Starting from the fourth icon on the left, the content of the monitoring object can be added. After adding the icon of the monitoring object, double-clicking the icon will pop up the drawing list of the monitoring object. According to the contents of the list, the setting of adding, modifying and deleting can be completed.



- After double-clicking the monitor object icon, the drawing list window pops up as follows. Selection of digital form will be displayed in the form of a small list, graphic form will be displayed in the form of line, pie chart, etc.



- How to add a connection to a small list of different monitored objects? Put the mouse in the middle of the four edges of each small list, that is, a small black dot will appear. Hold the left mouse button on the small black dot, and drag to the edge of another small list of monitored objects to complete the wiring operation.
- Repeat the above operations to complete the business chain building process. The final

completed style can be seen in the following figure:

- If you want to delete the added content? You can place the mouse in the upper right corner of the content, which will result in the deletion function 【x】.

17.3.3. Tips for building business chain dashboard

- Every time you set up a monitoring object content, you must click on the "save" function!
- XPM users in different departments and positions suggest to build dashboards that meet their application scenarios, and use authorization separately in authority management.
- Please strictly follow the logic of the business chain to build, only in this way can we find the problem node in the event of an exception. For example, a small list of monitored objects from left to right can be firewall -> Load Balancing -> Web Services -> Application Services -> middleware -> Database -> third-party applications.
- KPI/KQI content recommendations for each small list are: health, delay class KQI, error class KQI, unresponsive class KQI, number of sessions.
- The function of the quick toolbar at the top of the page is also effective for the business chain dashboard. Through this function, the abnormal nodes in the business chain can be found efficiently.

18. Communication Topology Discovery and Carding

Communication topology discovery and combing is one of the most powerful, practical and commonly used functions of XPM. Its application scenarios include

- Help users verify that business chain logic is correct
- Help users discover active hosts or potentially risky hosts in the network
- Help users intuitively determine the size of each KPI/KQI between different hosts, and drill into communication pairs or sessions.

18.1. Basic operation of topological functions

18.1.1. Two Entrances to Topological Functions

- The function of the main function bar on the right side of the page is topology discovery.
- Topology Search is a quick toolbar on the top of the page, which combs the topology.

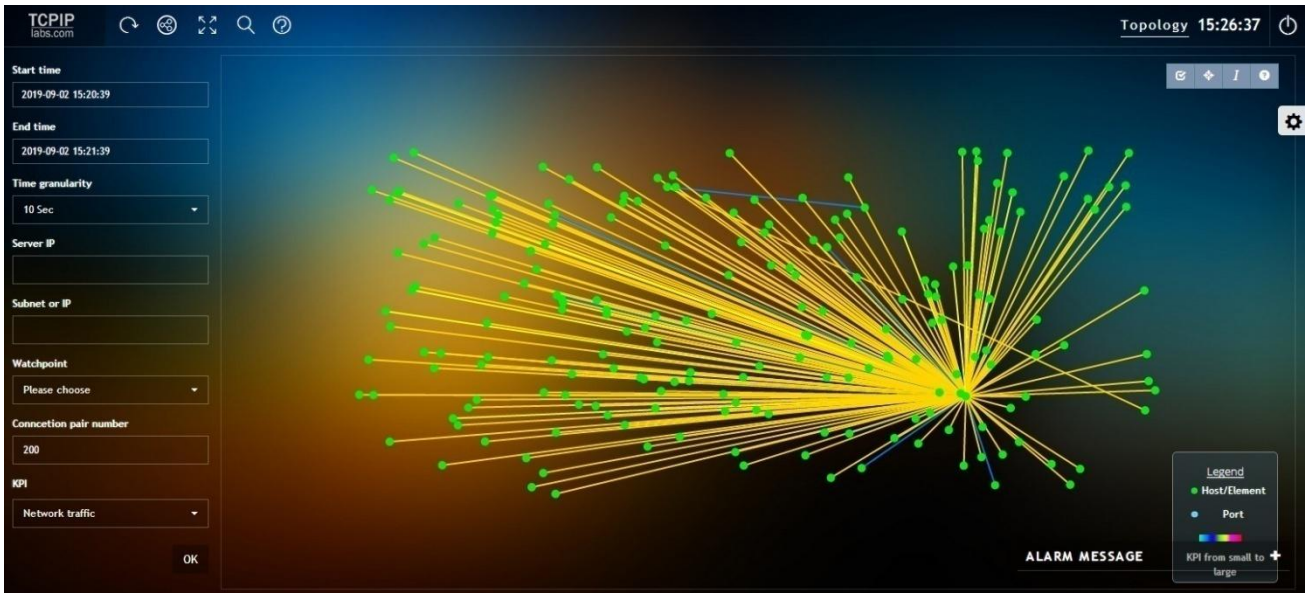
18.1.2. Basic operation of topological functions

- Green dots in the topology represent IP; blue dots represent Port.
- Double-click on the green dot (IP) to drill into Port; double-click on Port again to drill further into the IP with which it communicates; this operation is used to sort out the path of the business chain.
- The color of the connection represents the value size of KPI/KQI, and its legend is in the lower right corner of the page.
- Double-click the connection between two IP dots to drill down the communication pair between the two IP dots.
- Rolling the wheel of the mouse can zoom in or out of the topology map; it helps better visualization.
- Hold down the left mouse button in the blank area where there is no content to drag the topology map as a whole.

- Place the mouse cursor on the IP or Port dot and click the right mouse button to pop up three functions: Copy the current IP, Delete the Object and Hide the Toolbar.
- Topology features come with a shortcut toolbar in the top right corner of the topology map. Shortcut functions include: box selection, center display, save status, display/cancel display IP, help, request save.

18.2. How to use the topology discovery function

After entering the function of topology discovery from the right side of the home page, the communication topology of the whole network will be presented in the current minute. As shown in the following figure.



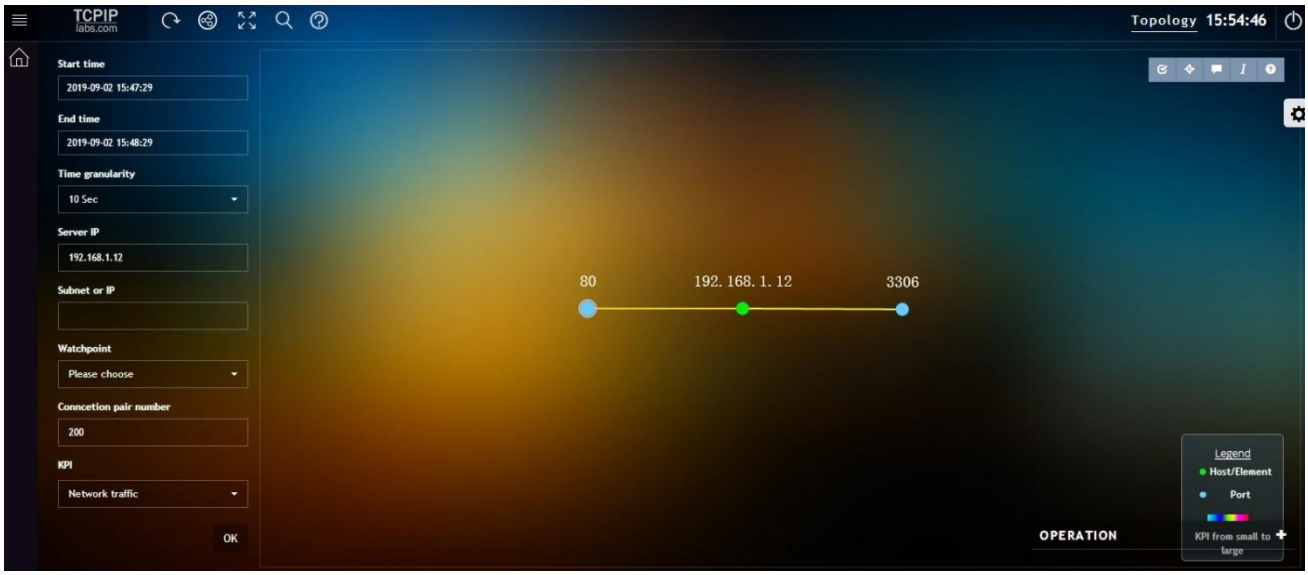
- Users can select functions according to the conditions on the left side and customize the communication topology on the right side.
- The default output of communication topology is 200 IP, users can increase the number of display, but the more the display, the longer the output time of the topology.
- According to the basic operation of the topology function in the previous section, the topology diagram can be operated in accordance with the application scenario.

18.3. How to Use Topology Carding Function

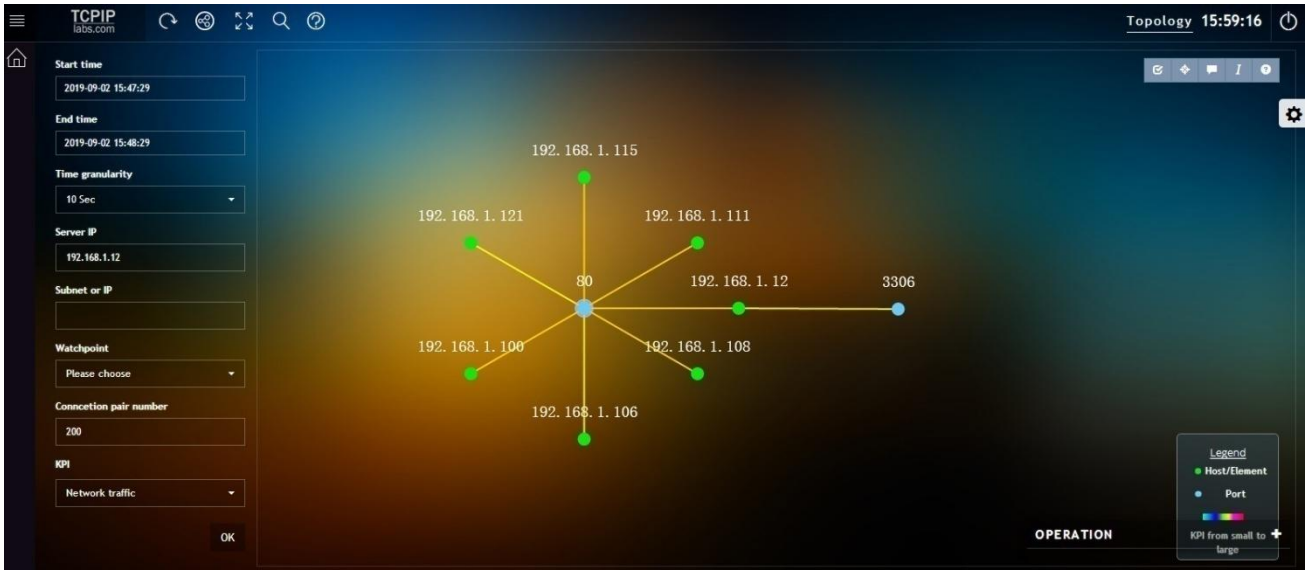
- Again, it is emphasized that the communication topology carding function can be used to verify

whether the business chain relationship is correct and accurate, and it is one of the most important functions of XPM.

- Click on the third function of the quick toolbar at the top of the page, [Topology query] function, you can enter the topology combing function.
- After entering, in the left conditional selection function, input the host IP that needs to be combed, and select the time and KPI type one by one. After clicking on the confirmation, you can output the first qualified communication relationship, as follows:



- Continue to double-click port 7001 (blue dot) in communication, and repeat this double-click operation, you can sort out a complete communication relationship business chain; based on this communication relationship, you can create a business chain dashboard, you can also verify whether the configuration provided by the business department is correct;



- Double-click on the connection to obtain the communication pairs of related communications.

19. Traffic Storage and Backtracking

Traffic traceback and analysis (hereinafter referred to as TSE) is one of the important functions of XPM-H. XPM-S and XPM-V do not provide this function.

The principle of TSE is to store network traffic in local disk arrays with high performance and non-destructive technology, and extract the original traffic of the accident through TCP/UDP five-tuple after a difficult security or maintenance accident. The original traffic of the accident is opened and analyzed in detail by using local packet parsing tools (such as Wireshark).

Because TSE stores complete and unprocessed network traffic, TSE is also the most effective and reliable method of data recovery and forensics, in many cases, even the only technical means. In the theory of safety and operation and maintenance, TSE is the last technical guarantee measure of safety and operation and maintenance system, and also the last important link of forming closed-loop of safety and operation and maintenance architecture.

19.1. Characteristics of XPM Traffic Storage and Backtracking Function

- For the XPM-H version, XPM-H can provide up to 16Gbps lossless zero-loss storage capability on the premise of meeting the hardware recommendation standard.
- By drilling alarms or graphics into the list of communication pairs or sessions, and the most accurate and streamlined data packets, the off-line analysis workload can be effectively reduced.
- After specifying the five-tuple condition, the qualified original data packet can be extracted from the TB-level original traffic at second-rate.
- Provide advanced storage scheme to save user storage resources effectively.

19.2. Functional Entry to Traffic Storage

There is only one entry for traffic storage, that is, the fourth function of the main function bar on the left side of the page. After clicking on it, the function page looks like the following:

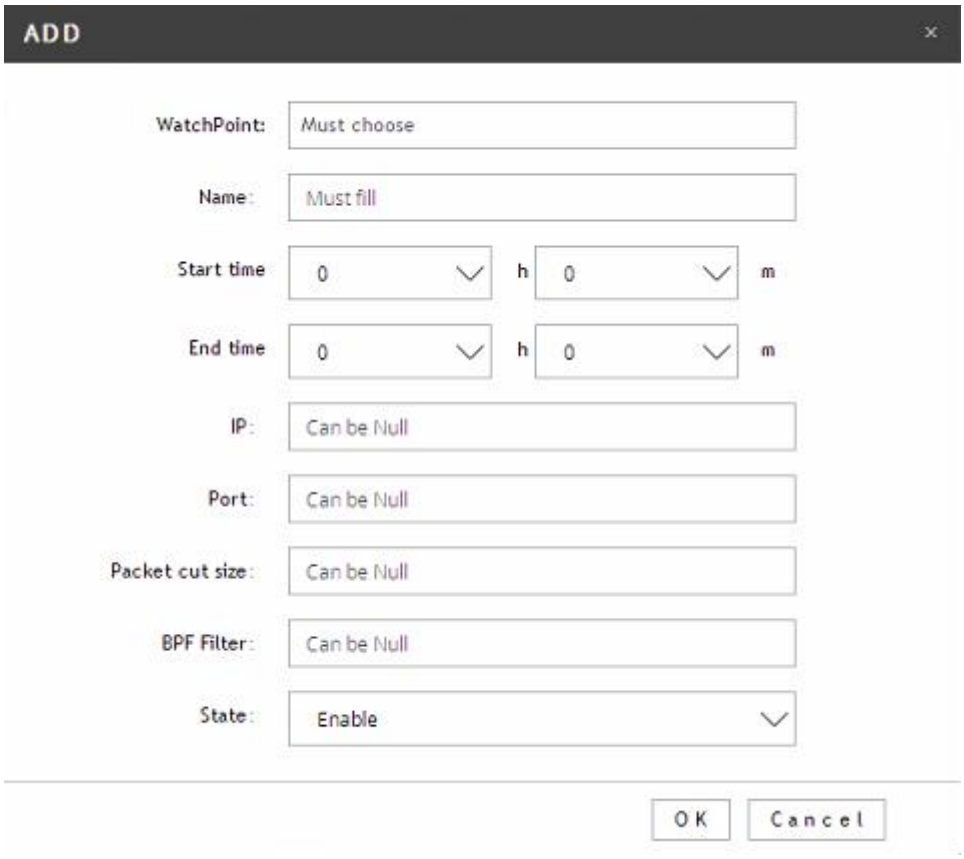
19.3. Standard storage scheme

Provides storage solutions for watch points, or IP, or ports, while supporting BPF filtering conditions.

19.4. Advanced Storage Scheme

Click on the third function on the left side of the traffic storage function [Advanced Storage Scheme], and you can enter the function page:

Create a new advanced storage strategy, add a new function to the third function in the upper right corner of the list; click on [+], and the following window will pop up:



According to the various functional options in the window, users can customize storage conditions, including the effective time of the scheme, the size of the intercept, and the conditions in other standard storage schemes.

19.5. Historical Data Extraction (Traffic Backtracking)

There are two functional portals for traffic backtracking

- One is the fourth function of the left function bar in the screenshot above [Historical Traffic Extraction]
- Another is the download function in the upper right corner of each communication pair or session list. After clicking on this function, the user can download the original traffic of the communication in PCAP file format to the local area, and open it with Wireshark and other data package parsing tools for further analysis.

19.6. Data extraction list

- For the extracted original data packet, XPM stores a backup in the local storage unit, which

can be used if the user needs to retrieve it again.

20. Main functions and application scenarios

20.1. Alert and locate abnormal service/application/network performance

The performance early warning of service/application/network is to set a reasonable threshold for the performance index KQI related to service/application/network and trigger an alarm when the threshold is reached:

A. These performance indicators KQI see in detail: what is XPM KPI and KQI?
B. The setting method of alarm is detailed: Functional entrance of alarm threshold setting
C. Detailed methods for setting alarms: Functional entrance of alarm threshold setting
D. The range of thresholds can be seen in detail: How to set the alarm threshold of performance index KQI reasonably.
E. How to get the alarm information in time and drill into the communication pair or session, please see details: Acquisition and drilling of alarm information

20.2. Visual monitoring of performance (on-screen monitoring)

XPM's UI design has fully considered the needs of screen monitoring, so there are special designs in the aesthetics and flexibility of the interface. Specifically, it can be achieved through the business chain dashboard, please see details: Business chain dashboard

20.3. Statistical analysis of business/application/network operation and correlation

- How to find the worst performance monitoring objects among the same types of monitoring objects?

  Through statistical analysis of the list function of dashboard and retrospective analysis of the time period required for statistical analysis, users can compare and analyze different

groups of the same type of monitoring objects to find the Web service with the worst performance, or the DB service with the most SQL return codes, or the branch with the worst quality of access, or the link time consumption. Most watch points.

- How to grasp the relationship between session volume and service performance?

  In statistical analysis dashboard, by choosing different monitoring objects in the first column of the list, we can change the graphical content under the list. Combining with time traceback, we can find the relationship between business, application and KQI of the network, for example:

  A. What is the handshake delay when TCP traffic peaks?

  B. When HTTP session volume peaks, what is the processing performance of the Web?

  C. When DB has the highest processing latency, which SQL is TOP10 with processing latency?

20.4. How to locate the delay of network serial devices

Network serial devices include switches, firewalls, load balancing and various kinds of security devices. The performance consumption of these devices to network quality is a common problem that is difficult to locate and check in network operation and maintenance.

In XPM, it is relatively simple to locate the network bottleneck with such delay or error. It only needs to retrospect the time in the built dashboard of business chain. By comparing the difference of the same performance index between different monitoring objects, we can find which monitoring object or which segment has performance degradation.

20.5. How to define the fault area of user complaints

If the HTTP module is loaded and HTTP traffic can be seen at each watch point, HTTP sessions of all complaint periods of the client IP can be found by searching for the complaint's Client IP and the business's included URLs. Then, by comparing the KQI delay of the same HTTP session, the time between different watch points can be found. Loss can locate the fault area. As follows:

Begin time	End time	XPMserver name	ServerIP	ClientIP	URL	CommandType	HTTP return code
08-27 18:26:22	08-27 18:26:22	Local	172.18.16.1	172.17.0.101	www.bszxyh.com:8443/dbank/channel/http.do	POST	200
08-27 18:26:41	08-27 18:26:42	Local	172.18.16.1	172.17.0.101	www.bszxyh.com:8443/dbank/channel/http.do	POST	200
08-27 18:26:37	08-27 18:26:37	Local	172.18.16.1	172.17.0.102	www.bszxyh.com:8443/dbank/channel/http.do	POST	200
08-27 18:26:39	08-27 18:26:39	Local	172.18.16.1	172.17.0.101	www.bszxyh.com:8443/dbank/channel/http.do	POST	200
08-27 18:26:22	08-27 18:26:22	Local	172.18.16.1	172.17.0.101	www.bszxyh.com:8443/dbank/channel/http.do	POST	200
08-27 18:26:20	08-27 18:26:20	Local	172.18.16.1	172.17.0.101	www.bszxyh.com:8443/dbank/channel/http.do	POST	200
08-27 18:26:37	08-27 18:26:37	Local	172.18.16.1	172.17.0.102	www.bszxyh.com:8443/dbank/channel/http.do	POST	200
08-27 18:26:15	08-27 18:26:15	Local	172.18.16.1	172.17.0.101	www.bszxyh.com:8443/dbank/channel/http.do	POST	200
08-27 18:26:21	08-27 18:26:21	Local	172.18.16.1	172.17.0.101	www.bszxyh.com:8443/dbank/channel/http.do	POST	200
08-27 18:26:36	08-27 18:26:36	Local	172.18.16.1	172.17.0.102	www.bszxyh.com:8443/dbank/channel/http.do	POST	200
08-27 18:26:37	08-27 18:26:37	Local	172.18.16.1	172.17.0.102	www.bszxyh.com:8443/dbank/channel/http.do	POST	200
08-27 18:26:42	08-27 18:26:42	Local	172.18.16.1	172.17.0.101	www.bszxyh.com:8443/dbank/channel/http.do	POST	200
08-27 18:26:21	08-27 18:26:21	Local	172.18.16.1	172.17.0.101	www.bszxyh.com:8443/dbank/channel/http.do	POST	200
08-27 18:26:33	08-27 18:26:34	Local	172.18.16.1	172.17.0.102	www.bszxyh.com:8443/dbank/channel/http.do	ALARM MESSAGE	200

20.6. Early warning and analysis of traffic anomalies

Early warning and analysis of abnormal traffic is one of the difficulties of network operation and security departments. In XPM, we can operate as follows:

Set reasonable threshold range for intelligent early warning. See details: How to Set the Warning Threshold of State Indicator KPI Reasonably.

After obtaining the alarm information, the alarm graphics are drilled first, and then abnormal peaks or troughs are formed by dragging and dragging, so that the communication or conversations leading to the peaks or troughs can be drilled. See for details: Acquisition and drilling of alarm information.

20.7. How to Multidimensional Analysis of Network Traffic

Through the aggregation analysis function of XPM, users can realize the aggregation or average statistical analysis of various dimensions, arbitrary time and arbitrary KPI.

Operating Path: [KPI/KQI Line Diagram for Analysis] -> Enter the line diagram page, default on the left is [Aggregated Analysis Dimension] -> After filling in the input box, click OK -> to get the graph, and then according to the time axis, drag and drop, you can get the statistical analysis value of each dimension of the analysis object in that period.

Aggregation analysis is very powerful! It not only provides a rich statistical analysis dimension,

but also creates the concept of "aggregation", and all statistical analysis content can be obtained in a few seconds, even for several days of statistical needs.

20.8. How to give targeted optimization suggestions

Operations and Maintenance Departments can help Operations and Maintenance Departments to put forward targeted optimization proposals to R&D Departments through the analysis functions of HTTP module and DB module of XPM. For example:

- The slowest URL, the URL with the most error return codes.
- The slowest SQL, the SQL with the most return codes. The following figure:


Default-SQLserver_DB_A-Ranking of Nonzero return code of SQLstatements(17:45-17:55)
insert into chen_testaa values(1, 'chen', 'fengtai', CURRENT TIMESTAMP)
update chen_testaa set name='zhao' where id=2
delete from chen_testaa where id=1
select * from chen_testaa
0 2 4 6 8 10 12 14 16 18 20 22 24
Start time:
2019-09-02 17:45:40
End time:
2019-09-02 17:55:40
XPM Server
Local
Watchpoint:
Default
Business:
SQLserver_DB_A
SESSION LIST
Search
Begin time
End time
ServerIP
ClientIP
SQLstatements
Return code
SQL processing time
Network delay at client
Network de
09-02 17:55:24
09-02 17:55:24
192.168.1.82
192.168.1.129
insert into chen_testaa values(1, 'chen', 'fengtai', CURRENT TIMESTAMP)
156
<1ms
<1ms
<1ms
ALARM MESSAGE
1.17ms

Enclosure 1 : Indicator Algorithm Description

XPM Full Stack Performance Management and Traffic Analysis Platform

Indicator Algorithm Description

Ver4.0

2019-8

1. Watch Point/Server/Client

KPI	Describe	Unit
Access quality	Handshake Delay + Application Processing Delay + Load Transfer Delay	ms
Server Communication Delay	Time difference between sending data to server and receiving [ACK]	ms
Client Communication Delay	Time difference between sending data to client and receiving client [ACK]	ms
Link Delay RTT	Server Communication Delay + Client Communication Delay	ms
Client Handshake Delay	Time difference between sending [SYN] to receiving [SYN, ACK] at the server	ms
Client Handshake Delay	The time difference between sending [SYN, ACK] to receiving [ACK] from the client	ms
Application Processing Delay	Time difference between the first request packet and the first response packet	ms
Load transmission delay	Time difference between the first response package and the last one	ms
Server retransmit delay	The time difference between the last retransmitted packet sent to the server and the sending packet	ms
Client Retransmit Delay	The time difference between the last retransmitted packet sent to the client and the sending packet	ms
Network flow	Statistical Data Frame Traffic Size (Layer 2 Traffic)	bps
TCP traffic	Traffic of data frames with layer 3 protocol field TCP	bps
UDP traffic	Traffic of data frames with layer 3 protocol field UDP	bps
Downstream flow	All traffic of destination IP in Intranet segment settings	bps
Upstream traffic	All traffic of source IP in Intranet segment settings	bps
Undefined server traffic	Traffic whose source or destination address is not within the defined server scope	bps
Undefined client traffic	Traffic whose source or destination address is not within the defined client scope	bps
Maximum number of sessions	Maximum number of active TCP/UDP connections over a period of time	number
Connection Initiation Number	Number of single SYN packets	number
TCP connection reset	Number of packages with RST	number
Number of connection responses	Number of packages with SYN/ACK	number

Connection closure number	Number of packages with FIN	number
Number of active shutdown connections	Number of first FIN packets in four-way interrupts	number
Connection unresponsiveness	Number of packages with SYN and without SYN/ACK	number
Number of passively closed connections	Number of second FIN packets in four-way interrupts	number
Packet Rate	Statistical Layer 2 Packet Rate	pps
Network Packet Loss Rate	Number of retransmitted packets/total TCP packets	%
Packet Loss Rate at Server	The number of retransmitted packets received by the server/the total number of TCP packets received by the server	%
Client Packet Loss Rate	The number of retransmitted packets received by the client/the total number of TCP packets received by the client	%
Tiny Packet Rate	Packet Rate with Packet Length Less than 64	pps
Tiny Packet Ratio	Number of tiny packages/total packages	%
Average package length	Total bytes/total packages	
Number of Zero Window Packets	Zero Window Packet Number for Source or Destination	number
Uplink bandwidth occupancy	Uplink Network Traffic/Uplink Bandwidth	%
Downlink bandwidth occupancy	Downlink network traffic/downlink bandwidth	%
ARP traffic	Statistical traffic of ARP	bps
ARP Packet Rate	ARP Packet Rate	pps
Connection reset rate	RST Packet Number/Session Number	
Number of sessions	Number of active TCP/UDP connections	number

2. HTTP Service

KPI	Describe	Unit
Server Communication Delay	For each HTTP session, the client sends the last packet of application layer data, and the server confirms the time difference of the packet.	ms
Client Communication Delay	For each HTTP session, the server sends the last packet of application layer data, and the time difference for the client to confirm the packet	ms
Link Delay RTT	Server communication delay + Client communication delay	ms
Service response latency	For each http session, the time difference between requesting the first packet and the corresponding first packet	ms
URL Load Delay	For each http session, the time difference between requesting the first packet and the corresponding last packet	ms
Network flow	For defined ip: port traffic, including source and destination.	bps
Number of HTTP application sessions	Number of HTTP Application Sessions	number
HTTP Error Return Code Ratio	Number of HTTP error return codes / Number of HTTP application sessions	%
HTTP unresponsive ratio	Number of unresponsive HTTP / Number of HTTP application sessions	%
Network Packet Loss Rate	Number of retransmitted packets/total packets for defined ip: port	%

3. Oracle/MySQL/SQLserver

KPI	描述	单位
Server Communication Delay	For each SQL session, the client sends the last packet of application layer data, and the server confirms the time difference of the packet.	ms
Client Communication Delay	For each SQL session, the server sends the last packet of application layer data, and the time difference for the client to confirm the packet	ms
Link Delay RTT	Server communication delay + Client communication delay	ms
SQL processing delay	For each SQL session, the time difference between requesting the first packet and the corresponding first packet	ms
SQL Service Flow	For defined ip: port traffic, including source and destination.	bps
Number of SQL application sessions	Number of SQL Application Sessions	number
Number of SQL error return codes	Number of sessions with a return code of 0	number
SQL Error Return Code Ratio	Number of SQL error return codes / Number of SQL application sessions	%
Number of unresponsive SQL	Number of unresponsive SQL application sessions over 60 seconds	个
SQL unresponsive ratio	Number of unresponsive SQL / Number of SQL application sessions	%
Network Packet Loss Rate	Number of retransmitted packets/total packets for defined ip: port	%