iMaster NCE-FabricInsight Data Sheet

Huawei iMaster NCE-FabricInsight is a data center network analyzer that provides ubiquitous network and service assurance analysis, making network O&M more intelligent, faster, and comprehensive.

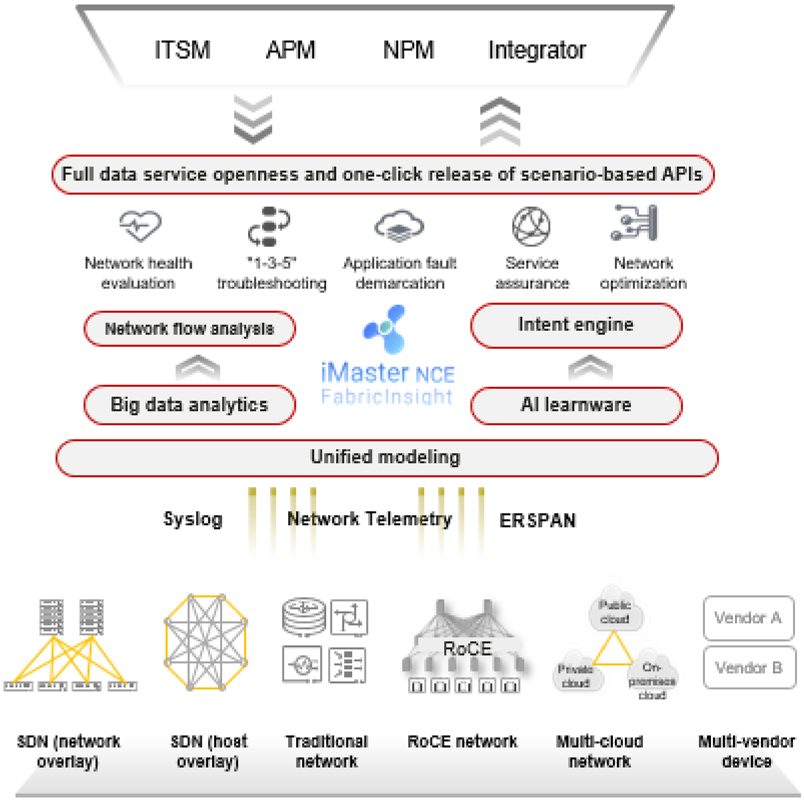
Product Description

As technologies such as cloud computing, big data, and artificial intelligence continue to develop and grow in popularity, enterprises are deepening their digital transformation, covering aspects such as office, production, and testing. Traditional data centers can no longer keep pace with development, and cloud-based transformation has become an inevitable trend. However, the current data center cloudification solutions currently available in the industry focus on virtualizing resources, improving resource utilization, automating deployment, and implementing cloud-based strategies, but overlook network management and service operations challenges brought by the growing scale and traffic of data centers. Traditional manual O&M cannot effectively deal with complex application migration policies, unstable service experience quality, difficult fault locating, and large-scale security policy management.

Huawei iMaster NCE-FabricInsight — a data center network analyzer — eschews the traditional resource status-based monitoring mode. Instead, it detects network health status in real time, helping customers promptly detect exceptions and locate root causes in minutes while also ensuring continuous and stable application running.

Key Components

iMaster NCE-FabricInsight (FabricInsight for short) supports multiple data center network architectures, such as the general-purpose computing network, intelligent computing network, and NoF storage network. It uses telemetry to collect network-wide metrics within seconds, analyzes and displays network data through big data and AI algorithms. It also provides northbound APIs such as Kafka, RESTful, SNMP, and WebSocket, implements full network data service openness, supports drag-and-drop orchestration, and quickly generates scenario-specific APIs to facilitate interconnection with upper-layer application systems.



Highlights

Network health evaluation

- Five-layer system: Modeling of 50+ network resources from five layers, ensuring comprehensive evaluation.
- Evaluation capability: Network dashboard + health report, building systematic health evaluation capability.

"1-3-5" fault locating

- Network fault: Analysis of 90+ typical faults and intelligent source tracing of massive logs.
- Risk evaluation: Intelligent evaluation of 40+ network risks, implementing proactive network O&M.

Application view

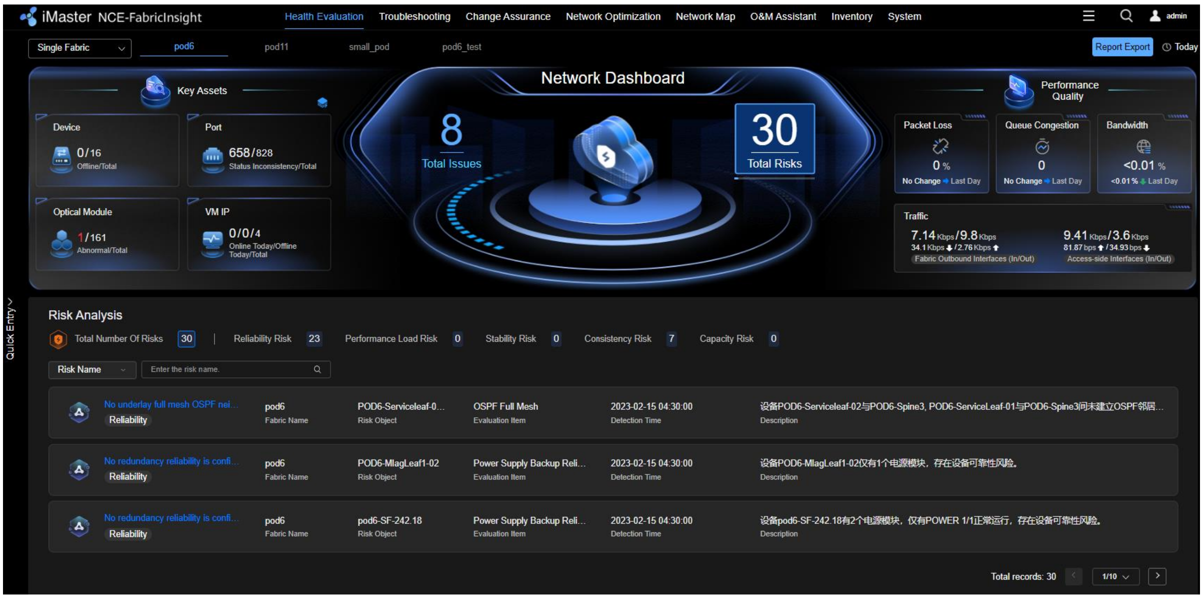
- Emergent diagnosis: Cross-cloud and cross-vendor network path analysis hop by hop, implementing application fault diagnosis in one click.
- Service assurance: Integrated analysis of services and networks, proactively assuring service experience.

Key Features

Comprehensive Network Health Evaluation

Network health check in traditional O&M is inefficient and cannot accurately reflect the network status in real time because it must be performed manually on devices one by one during off-peak hours. FabricInsight takes a different approach. It performs network-wide modeling based on the knowledge graph, displays the 24/7 network quality, visualizes network-wide resource status, and analyzes performance metrics such as traffic, bandwidth, and packet loss. In addition, it dynamically detects key metrics and proactively reports exceptions.

By providing network health evaluation reports in real time or periodically, FabricInsight helps network administrators gain insights into networks and improve O&M efficiency and service experience quality.



Network Dashboard

Key Assets

Device 0/16 Offline/Total

Port 658/828 Status Inconsistency/Total

Optical Module 1/161 Abnormal/Total

VM IP 0/0/4 Online Today/Offline Today/Total

8 Total Issues

30 Total Risks

Performance Quality

Packet Loss 0 % No Change → Last Day

Queue Congestion 0 No Change → Last Day

Bandwidth <0.01 % <0.01 % Last Day

Traffic

7.14 Kbps/9.8 Kbps 34.1 Kbps /2.76 Kbps Fabric Outbound Interfaces (In/Out)

9.41 Kbps/3.6 Kbps 81.87 bps /34.93 bps Access-side Interfaces (In/Out)

Risk Analysis

Total Number Of Risks 30 | Reliability Risk 23 Performance Load Risk 0 Stability Risk 0 Consistency Risk 7 Capacity Risk 0

Risk Name: Enter the risk name.

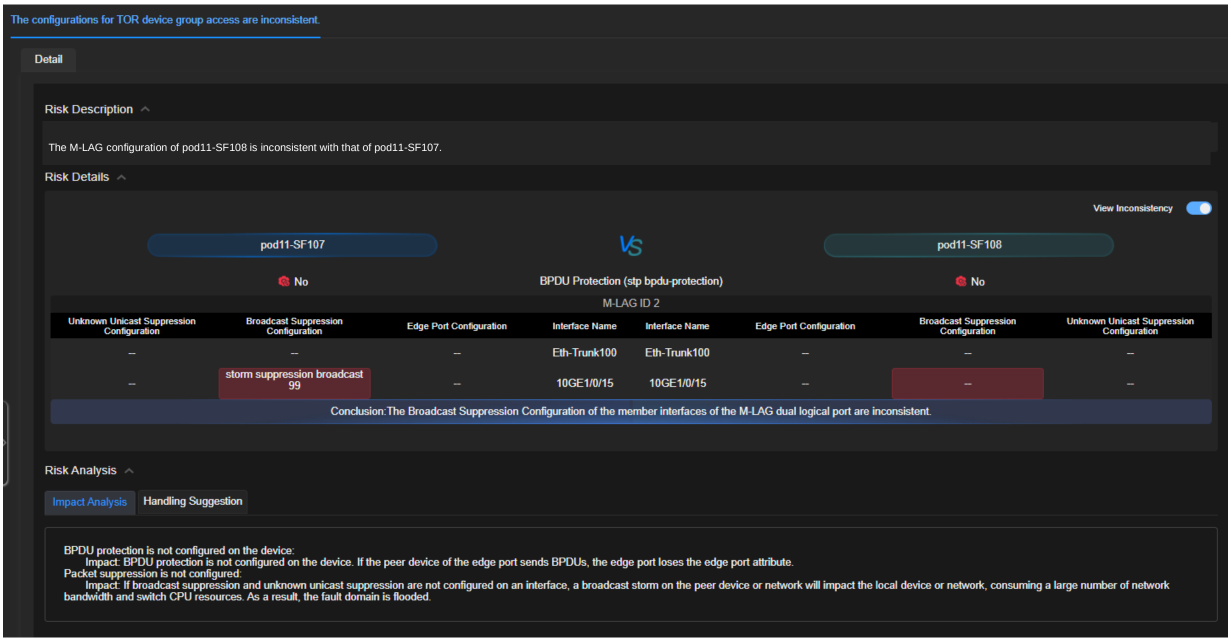
Risk Name	Fabric Name	Risk Object	Evaluation Item	Detection Time	Description
No underlay full mesh OSPF nei... Reliability	pod6	POD6-Serviceleaf-0...	OSPF Full Mesh	2023-02-15 04:30:00	设备POD6-Serviceleaf-02与POD6-Spine3, POD6-ServiceLeaf-01与POD6-Spine3间未建立OSPF邻居...
No redundancy reliability is confi... Reliability	pod6	POD6-MlagLeaf1-02	Power Supply Backup Reli...	2023-02-15 04:30:00	设备POD6-MlagLeaf1-02仅有1个电源模块，存在设备可靠性风险。
No redundancy reliability is confi... Reliability	pod6	pod6-SF-242.18	Power Supply Backup Reli...	2023-02-15 04:30:00	设备pod6-SF-242.18有2个电源模块，仅有POWER 1/1正常运行，存在设备可靠性风险。

Total records: 30 1/10

Risk Evaluation

With continuous service rollout and development, service risks may occur due to uncertainties. We need to check whether the network bearing changes, whether the network-wide health status changes, and whether sub-health deterioration risks exist, and even whether actions can be performed in advance to ensure application and operations.

Based on systematic network modeling, FabricInsight performs inference and analysis on data center networks from multiple dimensions, such as reliability, consistency, performance load, capacity, and stability, and provides systematic network risk evaluation and predictive maintenance suggestions. When performing network health inspection, O&M personnel can use the risk evaluation function to identify network risks in advance and handle risks before services are affected, ensuring network service quality.



The configurations for TOR device group access are inconsistent.

Detail

Risk Description

The M-LAG configuration of pod11-SF108 is inconsistent with that of pod11-SF107.

Risk Details

View Inconsistency

pod11-SF107 VS pod11-SF108

BPDU Protection (stp bpdu-protection): No | No

M-LAG ID 2

Unknown Unicast Suppression Configuration	Broadcast Suppression Configuration	Edge Port Configuration	Interface Name	Interface Name	Edge Port Configuration	Broadcast Suppression Configuration	Unknown Unicast Suppression Configuration
--	--	--	Eth-Trunk100	Eth-Trunk100	--	--	--
--	storm suppression broadcast 99	--	10GE1/0/15	10GE1/0/15	--	--	--

Conclusion:The Broadcast Suppression Configuration of the member interfaces of the M-LAG dual logical port are inconsistent.

Risk Analysis

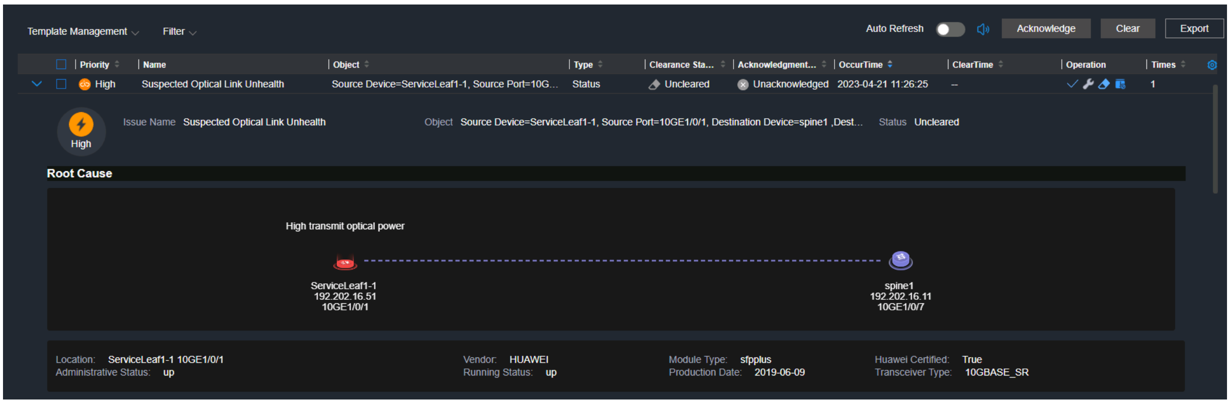
Impact Analysis | Handling Suggestion

BPDU protection is not configured on the device:
Impact: BPDU protection is not configured on the device. If the peer device of the edge port sends BPDUs, the edge port loses the edge port attribute.
Packet suppression is not configured:
Impact: If broadcast suppression and unknown unicast suppression are not configured on an interface, a broadcast storm on the peer device or network will impact the local device or network, consuming a large number of network bandwidth and switch CPU resources. As a result, the fault domain is flooded.

"1-3-5" Troubleshooting

Data centers are not only service support centers, but also value creation centers. For 98% of enterprises, they will lose more than US$100,000 per hour if their services are interrupted, which is why customers have zero tolerance for network interruptions. Traditional network O&M is mainly performed manually, making it difficult and time-consuming to locate network faults, and severely affecting service continuity.

Leveraging telemetry, FabricInsight collects data on the management, forwarding, and data planes of the entire network in all scenarios, detecting 90+ typical issues and user-defined syslog-converted issues in minutes. In addition, FabricInsight uses the knowledge graph to automatically identify the root causes of faults and potential risks and provide effective rectification suggestions. Furthermore, FabricInsight collaborates with Huawei iMaster NCE-Fabric to recommend fault handling plans, enabling typical faults to be quickly rectified.



□	Priority	Name	Object	Type	Clearance Sta...	Acknowledgment...	OccurTime	ClearTime	Operation	Times
□	High	Suspected Optical Link Unhealth	Source Device=ServiceLeaf1-1, Source Port=10G...	Status	Uncleared	Unacknowledged	2023-04-21 11:26:25	--		1

High

Issue Name Suspected Optical Link Unhealth

Object Source Device=ServiceLeaf1-1, Source Port=10GE1/0/1, Destination Device=spine1 ,Dest...

Status Uncleared

Root Cause

Location: ServiceLeaf1-1 10GE1/0/1
Administrative Status: up

Vendor: HUAWEI
Running Status: up

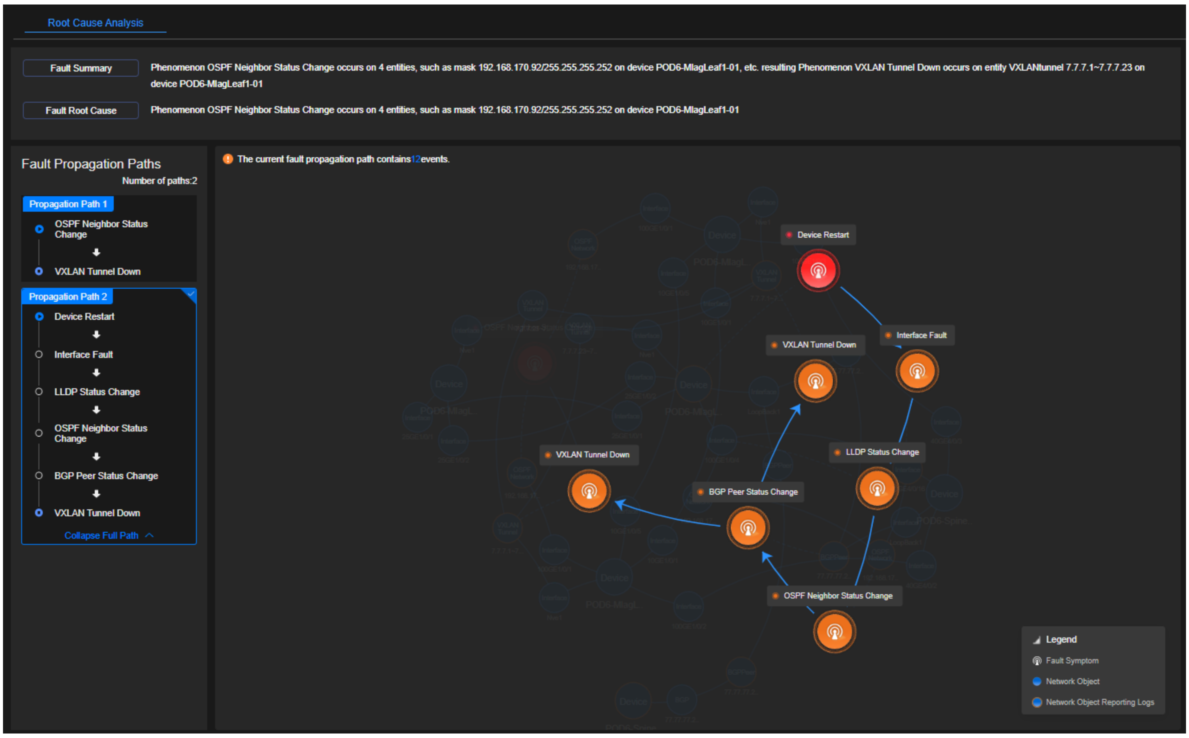
Module Type: sfpplus
Production Date: 2019-06-09

Huawei Certified: True
Transceiver Type: 10GBASE_SR

Intelligent Source Tracing for Massive Logs

After a network fault occurs, a large number of logs are generated. Traditional O&M relies on expert experience to locate the fault one by one, which is time-consuming and difficult to locate the root cause.

FabricInsight provides inference and clustering capabilities for logs, quickly identifies root causes based on knowledge graph and AI algorithms, displays fault propagation paths, and identifies impact scopes. It has little dependence on expert experience, improving analysis efficiency by 90%.



Fault Summary: Phenomenon OSPF Neighbor Status Change occurs on 4 entities, such as mask 192.168.170.92/255.255.255.252 on device POD6-MlagLeaf1-01, etc. resulting Phenomenon VXLAN Tunnel Down occurs on entity VXLANtunnel 7.7.7.1~7.7.7.23 on device POD6-MlagLeaf1-01

Fault Root Cause: Phenomenon OSPF Neighbor Status Change occurs on 4 entities, such as mask 192.168.170.92/255.255.255.252 on device POD6-MlagLeaf1-01

Fault Propagation Paths

Number of paths:2

Propagation Path 1

- OSPF Neighbor Status Change
- VXLAN Tunnel Down

Propagation Path 2

- Device Restart
- Interface Fault
- LLDP Status Change
- OSPF Neighbor Status Change
- BGP Peer Status Change
- VXLAN Tunnel Down

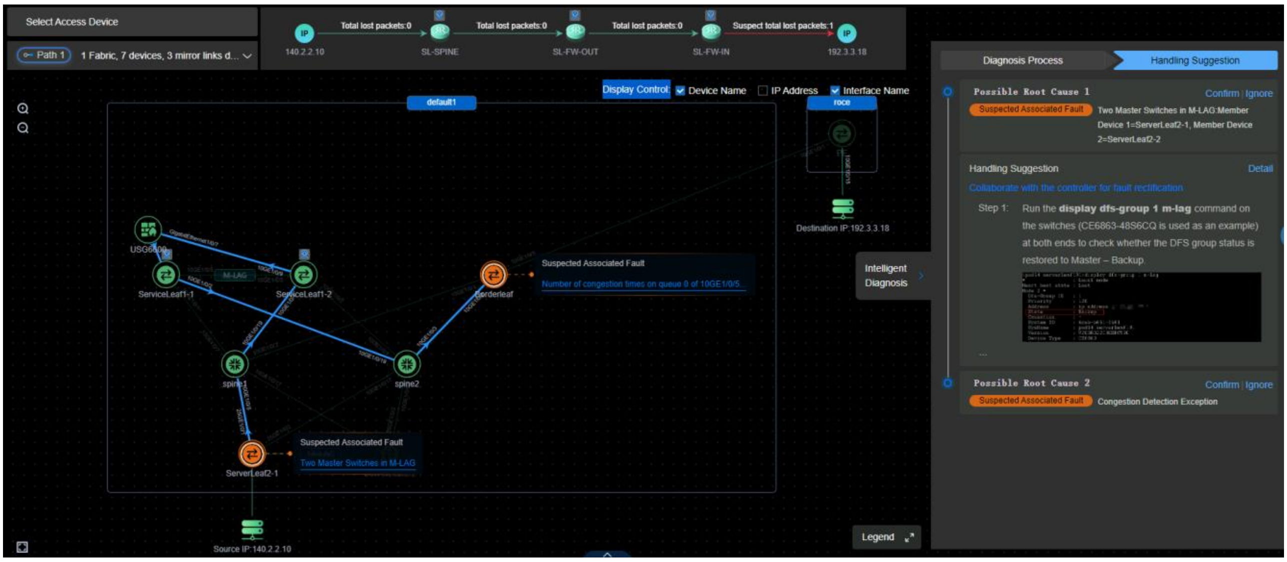
Collapse Full Path

The current fault propagation path contains 12 events.

Application Fault Diagnosis

Once a service fault is reported, the network department needs to collaborate with the service department to demarcate and locate the fault. Depending on manual analysis of nodes one by one, traditional O&M cannot identify network forwarding paths and quickly locate faults.

By mirroring full flow at key network nodes and ERSPAN flows at all nodes, FabricInsight can search for the forwarding path of real service flows in the DC in one-click mode based on source and destination IP addresses and identify the status of devices, interfaces, and links along the path, implementing correlation analysis of applications and networks and one-click diagnosis of connectivity and poor-QoE faults. In addition, it provides network path state and real packets of application interaction as evidence, ensuring trusted and traceable data.



Suspected Associated Fault
Number of congestion times on queue 0 of 10GE1/0/5.

Suspected Associated Fault
Two Master Switches in M-LAG

Possible Root Cause 1 — Confirm | Ignore
Suspected Associated Fault — Two Master Switches in M-LAG:Member Device 1=ServerLeaf2-1, Member Device 2=ServerLeaf2-2

Handling Suggestion — Detail
Collaborate with the controller for fault rectification

Step 1: Run the **display dfs-group 1 m-lag** command on the switches (CE6863-48S6CQ is used as an example) at both ends to check whether the DFS group status is restored to Master – Backup.

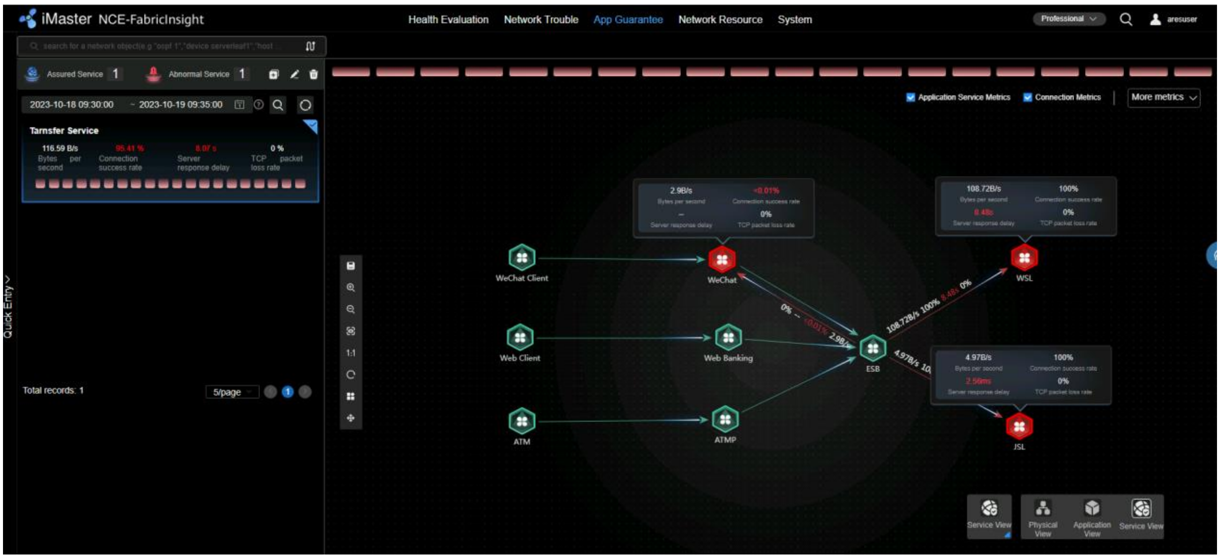
...

Possible Root Cause 2 — Confirm | Ignore
Suspected Associated Fault — Congestion Detection Exception

Application Quality Assurance

With the development of digital transformation, as well as the explosive growth of data, application and network systems are separated. Once a service fault occurs, multiple departments need to collaborate and communicate with each other to locate the fault, which is inefficient and cannot meet the requirements of service innovation and development. To address this problem, FabricInsight introduces xFlow intelligent full-flow analysis.

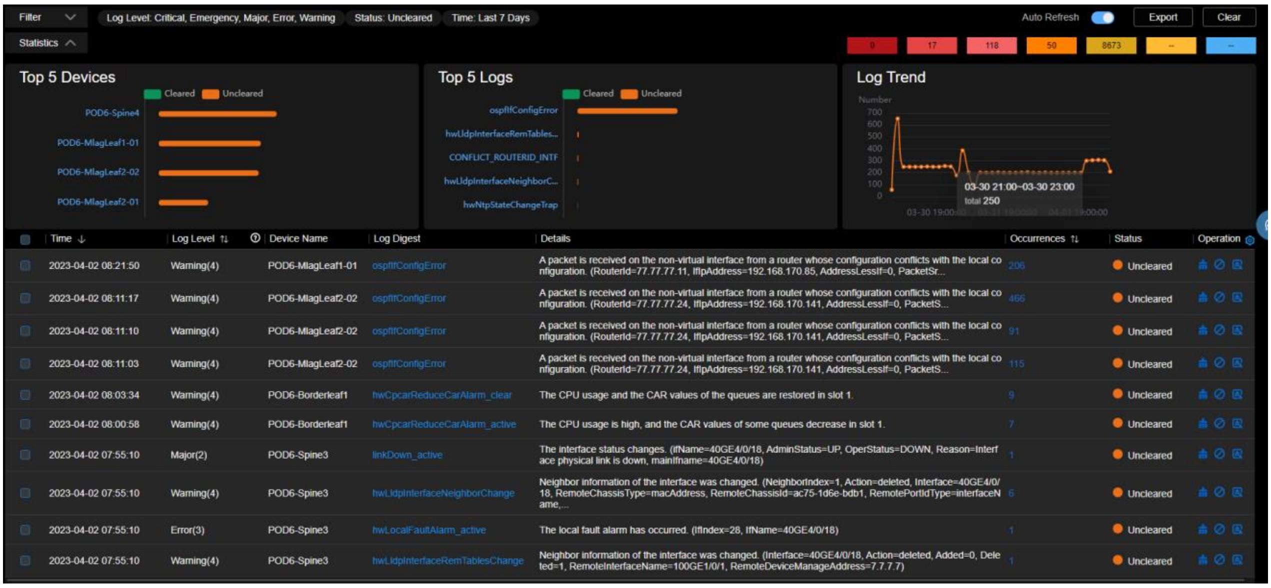
Based on xFlow intelligent full-flow analysis, FabricInsight implements integrated monitoring of applications and networks. It monitors more than 140 performance metrics in real time, enabling the system to proactively evaluate application experience and network quality. It also pre-defines key service views for key services to specify call chains during service interaction, implementing real-time service quality monitoring from applications to networks in an E2E manner. For key applications, FabricInsight automatically discovers applications and their interactions based on LB configurations and xFlow intelligent full-flow analysis, proactively detects application exceptions, associates with network paths in one-click mode, and locate the failure points.



Intelligent Analysis of Network-Wide Logs

After a network fault occurs, a large number of logs are generated and 95% of them are invalid logs. In traditional O&M, the manual check of logs one by one is time-consuming and inefficient.

FabricInsight visualizes network-wide log events, including the multi-dimensional trends, distribution statistics, and details from Layer 0 to Layer 6. In addition, more than 200 default rules are preset in the system or user-defined rules can be customized to aggregate and clear abnormal logs, improving log analysis efficiency. FabricInsight also supports user-defined syslog-converted issues for fault locating in minutes.



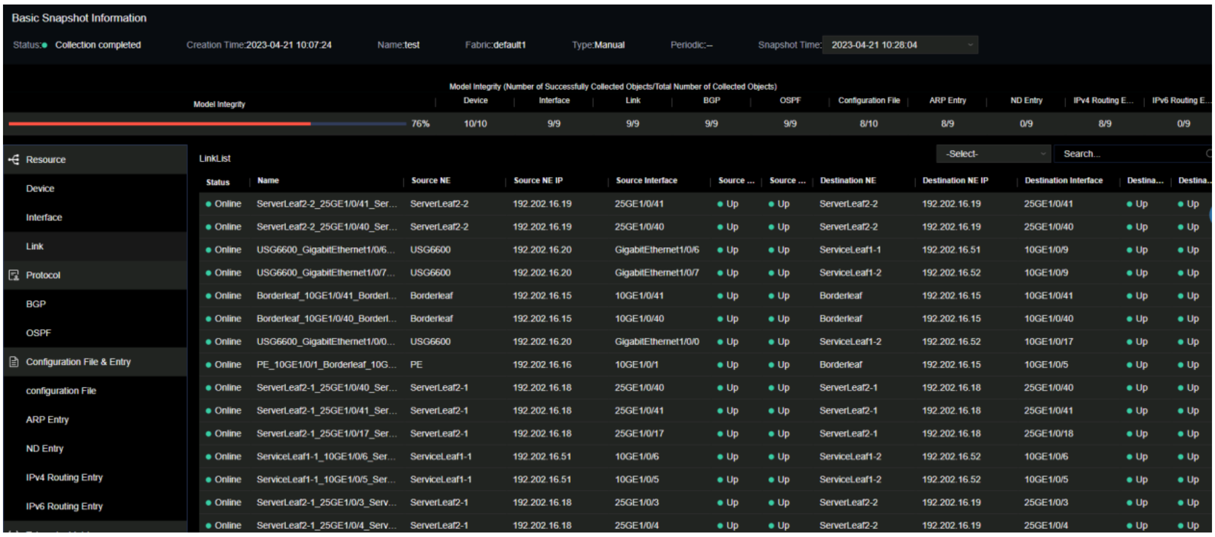
Log Level: Critical, Emergency, Major, Error, Warning | Status: Uncleared | Time: Last 7 Days

Time	Log Level	Device Name	Log Digest	Details	Occurrences	Status	Operation
2023-04-02 08:21:50	Warning(4)	POD6-MlagLeaf1-01	ospfIfConfigError	A packet is received on the non-virtual interface from a router whose configuration conflicts with the local configuration. (RouterId=77.77.77.11, IfIpAddress=192.168.170.85, AddressLessIf=0, PacketSr...	206	Uncleared	
2023-04-02 08:11:17	Warning(4)	POD6-MlagLeaf2-02	ospfIfConfigError	A packet is received on the non-virtual interface from a router whose configuration conflicts with the local configuration. (RouterId=77.77.77.24, IfIpAddress=192.168.170.141, AddressLessIf=0, PacketS...	466	Uncleared	
2023-04-02 08:11:10	Warning(4)	POD6-MlagLeaf2-02	ospfIfConfigError	A packet is received on the non-virtual interface from a router whose configuration conflicts with the local configuration. (RouterId=77.77.77.24, IfIpAddress=192.168.170.141, AddressLessIf=0, PacketS...	91	Uncleared	
2023-04-02 08:11:03	Warning(4)	POD6-MlagLeaf2-02	ospfIfConfigError	A packet is received on the non-virtual interface from a router whose configuration conflicts with the local configuration. (RouterId=77.77.77.24, IfIpAddress=192.168.170.141, AddressLessIf=0, PacketS...	115	Uncleared	
2023-04-02 08:03:34	Warning(4)	POD6-Borderleaf1	hwCpcarReduceCarAlarm_clear	The CPU usage and the CAR values of the queues are restored in slot 1.	9	Uncleared	
2023-04-02 08:00:58	Warning(4)	POD6-Borderleaf1	hwCpcarReduceCarAlarm_active	The CPU usage is high, and the CAR values of some queues decrease in slot 1.	7	Uncleared	
2023-04-02 07:55:10	Major(2)	POD6-Spine3	linkDown_active	The interface status changes. (ifName=40GE4/0/18, AdminStatus=UP, OperStatus=DOWN, Reason=Interface physical link is down, mainIfname=40GE4/0/18)	1	Uncleared	
2023-04-02 07:55:10	Warning(4)	POD6-Spine3	hwLldpInterfaceNeighborChange	Neighbor information of the interface was changed. (NeighborIndex=1, Action=deleted, Interface=40GE4/0/18, RemoteChassisType=macAddress, RemoteChassisId=ac75-1d6e-bdb1, RemotePortIdType=interfaceName,...	6	Uncleared	
2023-04-02 07:55:10	Error(3)	POD6-Spine3	hwLocalFaultAlarm_active	The local fault alarm has occurred. (IfIndex=28, IfName=40GE4/0/18)	1	Uncleared	
2023-04-02 07:55:10	Warning(4)	POD6-Spine3	hwLldpInterfaceRemTablesChange	Neighbor information of the interface was changed. (Interface=40GE4/0/18, Action=deleted, Added=0, Deleted=1, RemoteInterfaceName=100GE1/0/1, RemoteDeviceManageAddress=7.7.7.7)	1	Uncleared	

Network Change Visibility

As data center networks are subject to frequent network changes, traditional manual O&M faces pressing challenges in terms of detecting thousands of device configuration changes and learning tens of thousands of entries per device.

With network snapshot management, FabricInsight supports automatic and manual synchronization of network snapshots from 17 items, such as device configuration, entry, topology, capacity, and performance. In addition, it automatically analyzes differences before and after changes, and clearly displays the detection results.



Status: ● Collection completed   Creation Time:2023-04-21 10:07:24   Name:test   Fabric:default1   Type:Manual   Periodic:--   Snapshot Time: 2023-04-21 10:28:04

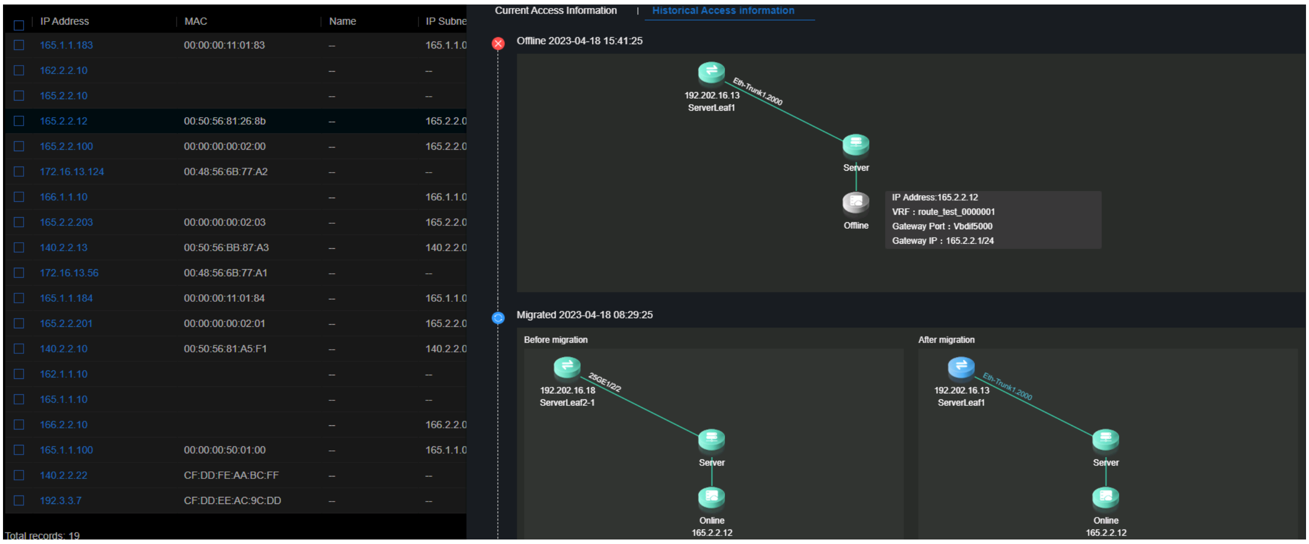
	Model Integrity (Number of Successfully Collected Objects/Total Number of Collected Objects)									
Model Integrity	Device	Interface	Link	BGP	OSPF	Configuration File	ARP Entry	ND Entry	IPv4 Routing E...	IPv6 Routing E...
76%	10/10	9/9	9/9	9/9	9/9	8/10	8/9	0/9	8/9	0/9

Status	Name	Source NE	Source NE IP	Source Interface	Source ...	Source ...	Destination NE	Destination NE IP	Destination Interface	Destina...	Destina...
● Online	ServerLeaf2-2_25GE1/0/41_Ser...	ServerLeaf2-2	192.202.16.19	25GE1/0/41	● Up	● Up	ServerLeaf2-2	192.202.16.19	25GE1/0/41	● Up	● Up
● Online	ServerLeaf2-2_25GE1/0/40_Ser...	ServerLeaf2-2	192.202.16.19	25GE1/0/40	● Up	● Up	ServerLeaf2-2	192.202.16.19	25GE1/0/40	● Up	● Up
● Online	USG6600_GigabitEthernet1/0/6...	USG6600	192.202.16.20	GigabitEthernet1/0/6	● Up	● Up	ServiceLeaf1-1	192.202.16.51	10GE1/0/9	● Up	● Up
● Online	USG6600_GigabitEthernet1/0/7...	USG6600	192.202.16.20	GigabitEthernet1/0/7	● Up	● Up	ServiceLeaf1-2	192.202.16.52	10GE1/0/9	● Up	● Up
● Online	Borderleaf_10GE1/0/41_Borderl...	Borderleaf	192.202.16.15	10GE1/0/41	● Up	● Up	Borderleaf	192.202.16.15	10GE1/0/41	● Up	● Up
● Online	Borderleaf_10GE1/0/40_Borderl...	Borderleaf	192.202.16.15	10GE1/0/40	● Up	● Up	Borderleaf	192.202.16.15	10GE1/0/40	● Up	● Up
● Online	USG6600_GigabitEthernet1/0/0...	USG6600	192.202.16.20	GigabitEthernet1/0/0	● Up	● Up	ServiceLeaf1-2	192.202.16.52	10GE1/0/17	● Up	● Up
● Online	PE_10GE1/0/1_Borderleaf_10G...	PE	192.202.16.16	10GE1/0/1	● Up	● Up	Borderleaf	192.202.16.15	10GE1/0/5	● Up	● Up
● Online	ServerLeaf2-1_25GE1/0/40_Ser...	ServerLeaf2-1	192.202.16.18	25GE1/0/40	● Up	● Up	ServerLeaf2-1	192.202.16.18	25GE1/0/40	● Up	● Up
● Online	ServerLeaf2-1_25GE1/0/41_Ser...	ServerLeaf2-1	192.202.16.18	25GE1/0/41	● Up	● Up	ServerLeaf2-1	192.202.16.18	25GE1/0/41	● Up	● Up
● Online	ServerLeaf2-1_25GE1/0/17_Ser...	ServerLeaf2-1	192.202.16.18	25GE1/0/17	● Up	● Up	ServerLeaf2-1	192.202.16.18	25GE1/0/18	● Up	● Up
● Online	ServiceLeaf1-1_10GE1/0/6_Ser...	ServiceLeaf1-1	192.202.16.51	10GE1/0/6	● Up	● Up	ServiceLeaf1-2	192.202.16.52	10GE1/0/6	● Up	● Up
● Online	ServiceLeaf1-1_10GE1/0/5_Ser...	ServiceLeaf1-1	192.202.16.51	10GE1/0/5	● Up	● Up	ServiceLeaf1-2	192.202.16.52	10GE1/0/5	● Up	● Up
● Online	ServerLeaf2-1_25GE1/0/3_Serv...	ServerLeaf2-1	192.202.16.18	25GE1/0/3	● Up	● Up	ServerLeaf2-2	192.202.16.19	25GE1/0/3	● Up	● Up
● Online	ServerLeaf2-1_25GE1/0/4_Serv...	ServerLeaf2-1	192.202.16.18	25GE1/0/4	● Up	● Up	ServerLeaf2-2	192.202.16.19	25GE1/0/4	● Up	● Up

IP Analyzer

When production systems are migrated to the cloud, the VMM automatically completes VM deployment and migration. However, information such as VM node location, VM migration or offline time, and VM distribution cannot be quickly found, meaning that only passive O&M can be performed on the network side.

FabricInsight provides 360-degree IP address analysis to quickly learn the number of online VMs and the distribution of top N switches connected to VMs, helping network administrators effectively plan resources in advance. FabricInsight supports full lifecycle management of VMs on the entire network, displays VM logout, migration, and login records in real time, and provides network-wide IP snapshot analysis. It also compares all IP address changes before and after network changes, and checks whether exceptions such as VM logout occur.



□	IP Address	MAC	Name	IP Subne
□	165.1.1.183	00:00:00:11:01:83	--	165.1.1.0
□	162.2.2.10		--	--
□	165.2.2.10		--	--
□	165.2.2.12	00:50:56:81:26:8b	--	165.2.2.0
□	165.2.2.100	00:00:00:00:02:00	--	165.2.2.0
□	172.16.13.124	00:48:56:6B:77:A2	--	--
□	166.1.1.10		--	166.1.1.0
□	165.2.2.203	00:00:00:00:02:03	--	165.2.2.0
□	140.2.2.13	00:50:56:BB:87:A3	--	140.2.2.0
□	172.16.13.56	00:48:56:6B:77:A1	--	--
□	165.1.1.184	00:00:00:11:01:84	--	165.1.1.0
□	165.2.2.201	00:00:00:00:02:01	--	165.2.2.0
□	140.2.2.10	00:50:56:81:A5:F1	--	140.2.2.0
□	162.1.1.10		--	--
□	165.1.1.10		--	--
□	166.2.2.10		--	166.2.2.0
□	165.1.1.100	00:00:00:50:01:00	--	165.1.1.0
□	140.2.2.22	CF:DD:FE:AA:BC:FF	--	--
□	192.3.3.7	CF:DD:EE:AC:9C:DD	--	--

Total records: 19

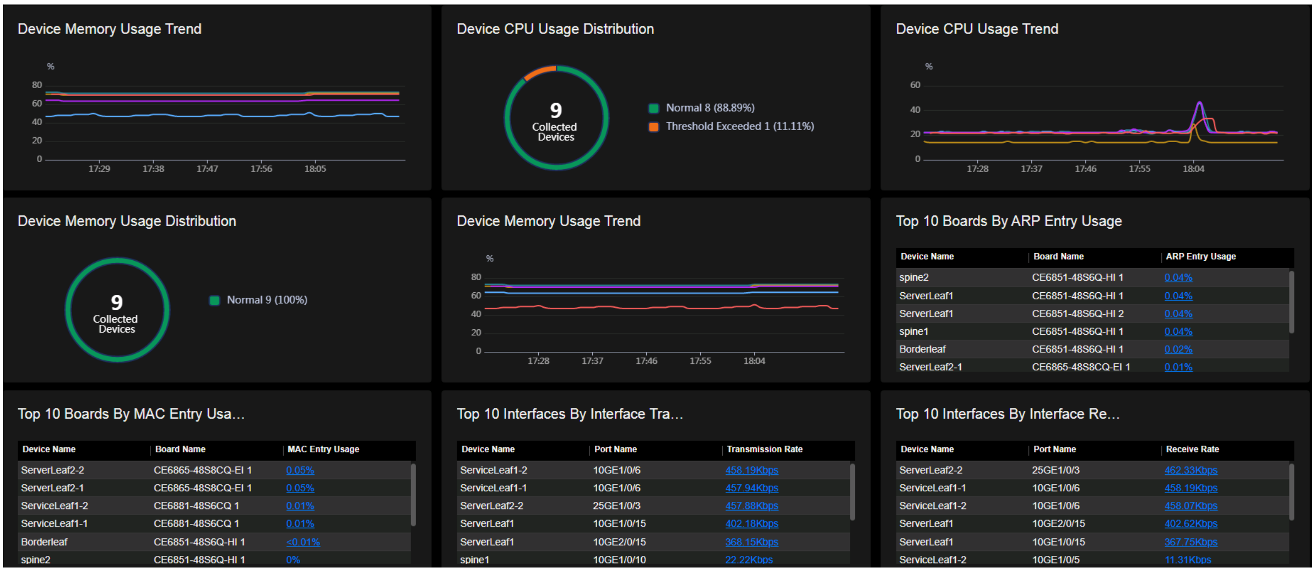
Offline 2023-04-18 15:41:25

IP Address:165.2.2.12
VRF : route_test_0000001
Gateway Port : Vbdif5000
Gateway IP : 165.2.2.1/24

Migrated 2023-04-18 08:29:25

Telemetry-Powered Network Visibility in All Scenarios

FabricInsight collects statistics on metrics such as devices, boards, queues, interfaces, and entries through Google Remote Procedure Call (gRPC) and displays the dynamic baseline range of each metric using machine learning algorithms. This enables FabricInsight to quickly detect the time point when a baseline exception occurs and proactively identify issues before they interrupt services. In addition, it automatically associates each abnormal time point with the affected service flows, allowing users to view the flow behavior data that passes through the device at the time point when an exception, such as a connection setup failure, occurs.



Top 10 Boards By ARP Entry Usage

Device Name	Board Name	ARP Entry Usage
spine2	CE6851-48S6Q-HI 1	0.04%
ServerLeaf1	CE6851-48S6Q-HI 1	0.04%
ServerLeaf1	CE6851-48S6Q-HI 2	0.04%
spine1	CE6851-48S6Q-HI 1	0.04%
Borderleaf	CE6851-48S6Q-HI 1	0.02%
ServerLeaf2-1	CE6865-48S8CQ-EI 1	0.01%

Top 10 Boards By MAC Entry Usa...

Device Name	Board Name	MAC Entry Usage
ServerLeaf2-2	CE6865-48S8CQ-EI 1	0.05%
ServerLeaf2-1	CE6865-48S8CQ-EI 1	0.05%
ServiceLeaf1-2	CE6881-48S6CQ 1	0.01%
ServiceLeaf1-1	CE6881-48S6CQ 1	0.01%
Borderleaf	CE6851-48S6Q-HI 1	<0.01%
spine2	CE6851-48S6Q-HI 1	0%

Top 10 Interfaces By Interface Tra...

Device Name	Port Name	Transmission Rate
ServiceLeaf1-2	10GE1/0/6	458.19Kbps
ServiceLeaf1-1	10GE1/0/6	457.94Kbps
ServerLeaf2-2	25GE1/0/3	457.88Kbps
ServerLeaf1	10GE1/0/15	402.18Kbps
ServerLeaf1	10GE2/0/15	368.15Kbps
spine1	10GE1/0/10	22.22Kbps

Top 10 Interfaces By Interface Re...

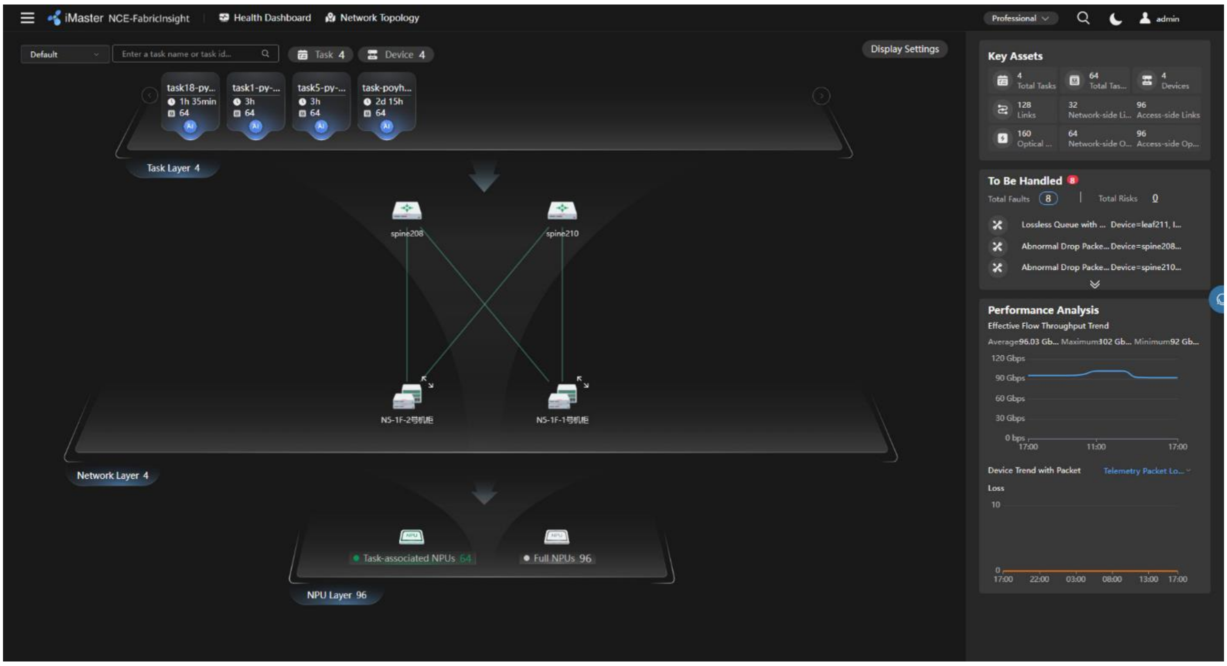
Device Name	Port Name	Receive Rate
ServerLeaf2-2	25GE1/0/3	462.33Kbps
ServiceLeaf1-1	10GE1/0/6	458.19Kbps
ServiceLeaf1-2	10GE1/0/6	458.07Kbps
ServerLeaf1	10GE2/0/15	402.62Kbps
ServerLeaf1	10GE1/0/15	367.75Kbps
ServiceLeaf1-2	10GE1/0/5	11.31Kbps

Communication Assurance for AI Computing Networks

With the explosion of AI large models, the AI industry is reaching a tipping point in its evolution and accelerating applications. The operation cost of large model training is high. However, the current computing network, as an important resource for AI training, lacks unified network performance monitoring and quick fault locating methods. As a result, it is difficult to ensure that monthly training is not interrupted.

FabricInsight implements integrated O&M for the computing network before and during training.

- Before training: FabricInsight displays the health of task, network, and NPU layers in a visualized manner, as well as detects metrics such as the effective throughput of RDMA transmission and packet loss rate of tasks in real time to quickly identify tasks with performance deterioration. In addition, the system proactively evaluates network faults and risks and identifies more than 100 types of exceptions, such as subhealthy, dirty, and loose optical links, to ensure stable running of training tasks.
- During training: When detecting an exception in a training task, FabricInsight restores the network path between NPUs and performs correlation analysis based on the packet loss and throughput information to quickly diagnose and demarcate the exception.



Lossless Queue with ... Device=leaf211, I...

Abnormal Drop Packe... Device=spine208...

Abnormal Drop Packe... Device=spine210...

Composition

The following table describes the basic package of intelligent network analysis and value-added packages of different services for FabricInsight.

Scenario	Feature	Description
Basic package of intelligent network analysis	System monitoring	Supports system monitoring, license management, and multi-vendor resource management.
	Telemetry-powered network visibility	Monitors metrics such as device, board, chip, interface, queue, optical link, and RoCE within seconds and performs anomaly analysis.
	Network snapshot analysis	Compares and analyzes network changes from multiple dimensions, including device configurations, ND entries, ARP entries, and FIB entries.
	Syslog analysis	• Visualizes network-wide log events and intelligently identifies log changes and occasional exceptions. • Automatically clears or aggregates logs based on preset or user-defined rules.
	IP Analyzer	Supports analysis on VM distribution, switch IP address distribution, historical access relationships, and snapshot comparison.
Value-added package of network health	Network health evaluation	• Analyzes the health status of key network resources, network-wide resource usage, and hot resources. • Exports evaluation reports in real time or periodically. • Supports risk evaluation of 40+ potential risks, such as reliability, capacity, performance, and reliability risks.
	"1-3-5" troubleshooting	• Detects more than 90 types of typical faults in minutes, automatically locates their root causes, and provides rectification suggestions. • Supports intelligent source tracing for massive logs, root cause inference, and fault propagation path analysis.
Value-added package of xFlow specified flow analysis	ERSPAN flow analysis	• Displays statistics on abnormal TCP/ICMP events, traffic, as well as the topology path through which the traffic passes. • Supports fault reasoning for abnormal flows and one-click root cause locating. • Searches for network paths based on source and destination IP addresses to quickly demarcate and locate faults.
	Network traffic analysis	• Provides network traffic analysis based on NetStream. • Analyzing network service traffic from multiple dimensions, such as interface, interface group, device, session, host, application, protocol, IP group, DSCP, and VNI. • Support collecting information on the flows circulating through the device, including Source/destination IP, IP header protocol type parameter, QoS marking, Source/destination TCP/UDP ports, incoming traffic interface.

Scenario	Feature	Description
	Multicast flow analysis	Supports network quality analysis of multicast services, including packet loss and delay measurement, and performs quick fault locating.
Value-added package of xFlow intelligent full-flow analysis	Intelligent full-flow analysis	• Supports full flow collection and cross-firewall session combination, implementing minute-level network path analysis and automatic fault diagnosis. • Automatically identifies applications and their interactions, visualizes application quality, proactively detecting application exceptions. • Supports service assurance and proactively identifies exceptions to ensure service experience. • Supports traffic analysis of mirrored links, real-time monitoring of TCP/UDP packet metrics, and multi-dimensional traffic statistics analysis by session, DSCP, VNI, application, port, and service port.
AI DC network intelligent O&M scenario package	Communication exception diagnosis of AI computing networks	• Restores the network path and performs hop-by-hop network path analysis, proactively detecting faults. • Analyzes network failure points based on the hop-by-hop diagnosis of NPU IP addresses. • Measures the metrics of task-level RDMA flows, and demarcates faults upon task interruption, packet loss or congestion in minutes.

Ordering Information

Module		Type	Description
Software subscription	**Software Package**		
	Basic package of intelligent network analysis	Mandatory	This item is purchased based on the number of CloudEngine switches in a data center.
	Value-added package of network health	Optional	This item is purchased based on the number of CloudEngine switches in a data center.
	Value-added package of xFlow specified flow analysis	Optional	This item is purchased based on the number of VM IP addresses in a data center.
	Value-added package of xFlow intelligent full-flow analysis	Optional	This item is purchased based on the traffic volume on the node where full-flow mirroring needs to be deployed.
	AI DC network intelligent O&M scenario package	Optional	This item is purchased based on the number of CloudEngine switches in a data center.
	SnS		
	Basic package of intelligent network analysis - SnS	Mandatory	This item corresponds to the basic package of network intelligent analysis. The quantity is the same as that of the basic package of network intelligent analysis.

Module		Type	Description
	Value-added package of network health - SnS	Optional	This item corresponds to the value-added package of network health. The quantity is the same as that of the value-added package of network health.
	Value-added package of xFlow specified flow analysis - SnS	Optional	This item corresponds to the value-added package of xFlow specified flow analysis. The quantity is the same as that of the value-added package of network traffic analysis.
	Value-added package of xFlow intelligent full-flow analysis - SnS	Optional	This item corresponds to the value-added package of xFlow intelligent full-flow analysis. The quantity is the same as that of the value-added package of xFlow intelligent full-flow analysis.
	AI DC network intelligent O&M scenario package - SnS	Optional	This item corresponds to the AI DC network intelligent O&M scenario package. The quantity is the same as that of the AI DC network intelligent O&M scenario package.
Hardware subscription	Analysis server	Optional	This item indicates the number of servers required by the FabricInsight analyzer.
	Collection server	Optional	This item indicates the number of servers required by the FabricInsight collector. If reliability is required, configure two servers for each fabric.
	Probe server	Optional	The quantity is the same as that of the value-added package of xFlow intelligent full-flow analysis.

iMaster NCE-FabricInsight provides a 180-day trial license. To apply for the trial license, visit the ESDP at http://app.huawei.com/isdp/.

More Information

For more information about Huawei iMaster NCE-FabricInsight, visit the following link: http://e.huawei.com

Copyright © Huawei Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.
Address: Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China
Website:e.huawei.com