FabricInsight

AI Technology Simplifies Data Center Network O&M

[Product Overview]

FabricInsight is a data center network analyzer launched by Huawei. It provides ubiquitous network application analysis and visualization functions to streamline applications and networks.

Based on the big data analysis technology, FabricInsight collects massive real service packets through the Telemetry, provides correlation analysis between internal applications and networks of the data center, and displays the application map and network quality in real time, helping customers quickly identify fault and proactively identify risks before services are affected.

[Product Description]

With continuous development and commercial use of technologies such as cloud computing, big data, and artificial intelligence, enterprise are deepening their digital transformation, covering various business forms including office, production, and testing. Traditional data centers can no longer catch up with development, and cloud-based transformation has become an inevitable trend. However, the current data center cloudification solutions in the industry focus on "Resource virtualization and resource utilization improvement" and "Automatic deployment and cloud-based strategies", and on the other hand overlook network management difficulties and challenges brought by the data center scale and traffic surge. 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 data center network analyzer FabricInsight abandons the resource status-based traditional monitoring mode. It detects fabric and application status in real time, streamlines networks and applications, monitors networks from the perspective of applications, helps customers detect network and application problems in a timely manner, and ensures continuous and stable application running.

[Key Components]

FabricInsight provides second-level collection of real flow on the entire network in Telemetry mode, analyzes and displays network data based on the big data intelligent algorithms, and provides northbound APIs to interconnect with upper-layer application systems.





[Benefits]

Mutual visibility between applications and networks, facilitating second-level fault identification

- Second-level display of service flows and network-wide KPIs through Telemetry
- Analysis of correlation between services, network paths, and network devices, visualizing network health status

Training the knowledge inference engine using AI, achieving minute-level fault locating

- Training the knowledge inference engine using machine learning, supporting minute-level root cause diagnosis for 75 types of faults
- Millisecond-level detection of historical microbursts, and accurate fault playback

Predictive maintenance using AI

- Dynamic baseline construction based on ML/AI and identification of issues at the device, queue, and port levels
- Proactively predicting traffic or optical module faults, reducing the fault rate by up to 68%

[Key Features]

DashBoard: multi-dimensional data analysis and graphical display

FabricInsight provides multi-dimensional Top N statistical views for hosts, applications, sessions and fabrics to help users detect network quality through multi-dimensional analysis.



Management of mutual access relationship between applications (ADM) and visualization of network policies

FabricInsight provides an application view, which can intuitively display the actual interaction relationships between services based on the network-wide real service flows. When a new service goes online, the network administrator can sort out the service relationship and complete the policy configuration based on the network-wide application association



map. In addition, the network administrator can quickly detect non-compliant access and traffic and take related measures.



Mutual visibility between applications and networks for quick fault analysis and demarcation

FabricInsight provides the intra-application visibility function. In the application details view, you can view the nodes with abnormal interaction to locate performance problems and analyze specific bottlenecks through the association with networks. In addition, FabricInsight provides the function of collecting statistics on and filtering abnormal events for users to quickly focus on abnormal events and quickly identify the service network health in the application based on the interaction diagram and heatmap of clusters in the application.





FabricInsight provides the network view, performs intelligent analysis of TCP flow status and detects abnormal flows based on big data, displays network quality in real time through indicators such as delay and traffic, and quickly identifies and analyzes abnormal flows on the network.



In addition, FabricInsight supports network change visualization. By comparing device configuration changes using snapshots, FabricInsight can quickly identify network changes such as Up Route, BD, Static Route, Dynamic Route, Host Route, Gateway Route, MAC, ARP, VRF, and Running Config.

Ch	langed Devices													
	Device Name		Device IP		Device Type			evice Role		Latest Changed Time		Changed devices		
~														
						0 (0
	198	42	41	0	50	40		198	42	41	0	50	40	
	Up Route Index	BD Index 45 MAC Index	Static Route Index O ARP Index	Dynamic Route Index	Host Route Index	Gateway Route Index		Up Route Index 22 VRF Index	BD Index 59 MAC Index	Static Route Index	Dynamic Route Index	Host Route Index	Gateway Route Index	
2														
2														
Tot														1 0

Network exception detection based on dynamic baselines and intelligent identification of service changes

FabricInsight collects statistics on metrics of devices, boards, queues, and interfaces in real time based on the GRPC, displays the top ranking of metrics in the area distribution chart, and displays the trend chart of top 5 metrics in real time.



									Last 1 Hour
FabricInsight									
	Device	Board	Interface	Queue	Optical Module				
	Indicator: CPU Usage 🔹								
<u>III</u> Network	Device CPU Usage Dis	tribution							
								All	Abnormal
Application									
Event		Normal 2(33.33%)	-						
(++) Telemetry		6						Leaf2	Leaf1
0	AbnormalTot 4(66.67%)	al Devices							
•C: Inventory									
Ø									
	Device CPU Usage Tre	nd							
	08:41					09:13 09:17			
	Device: Spine2								
						Spin	e2: 73%		
	0 Device: Leaf3								ti
						09:1	7		
						Leat	5 , 1574		
	Device: Spine1								ជា
() About									
						09:1 Snir	7 w1: 14%		

Based on machine learning algorithms, FabricInsight displays the dynamic baseline range of each metric to quickly locate the time point when the baseline exception occurs and proactively identify faults before service interruption. In addition, FabricInsight automatically associates exception points with the affected service flows. You can view data such as connection setup failure flow behavior on the device at the exception time point.

								🗲 Undo Ċ Redo	Last 24 Hours		
FabricInsight											
Dashboard	Indicator: CPU Usage 🔻										
	Device CPU Usage Distribut	ion									
								All	Abnormal		
Application	Abnormal										
	1(16.67%)										
Event											
((+)) Telemetry	6										
Q	Total De	wices									
		Normal S/82 239(1)									
		5(65.55 %)									
© System	Device CPU Usage Trends										
	7 07-29 16:00 07-29										
	Device: Leat3 1/13 < >										
		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~				MANAMA MA	M Mmmar	mmmm/	N.D.M		
	Connection setun failures o	n the device. Query time:20	18-07-29 15-14-00-2018-07-29	15:16:00							
	Connec		Pac								
	×🗆 18			8	1	0	$\forall$	5			
	Connection Setup Failure Fl	ow List, Total:18									
					Provider APP	Retransmitted Events	Connection Setup Failures	Connection Setup Failu	re Rate 🧿		
() Help	> 15:14:00~15:16:00		192.168.2.65		Undefined App						
					Undefined App						

### Predictive maintenance using machine learning, effectively reducing the network fault rate

FabricInsight provides the capability to predict faults of optical modules. Based on the Big Data and machine learning algorithms, FabricInsight can detect optical module faults and predict the optical module faulty probability to identify abnormal optical modules before services are affected. In addition, FabricInsight displays basic attributes of optical



modules on the entire network and the trend of optical module metrics in the last 14 days. Users can evaluate the deterioration of optical modules based on the data to better troubleshoot faults.

In addition, FabricInsight supports traffic forecast based on the RX and TX bandwidth utilization of interfaces, and displays the traffic prediction results for the next 12 weeks.

			Interface	Queue	Optical Module				
FabricInsight								📒 High Risk Of Fault 📒 St	bhealth 🔲 Normal
BD Dashboard									
-Ö-									
<u>III</u> Network	0	2018-10-12 2018-10	-13 2018-10-14	2018-10-15 2018-10	-16 2018-10-17 2018-1	0-18 2018-10-19	2018-10-20 2018-10-21	2018-10-22 2018-10-23	2018-10-24
	Fault Rate and Distribu	ution							
	ruun note und cristino.								
-Ara Execut		_	Contraction 10 Leaf4	Leaf3 10GE1/0/2	Spine2 2 10GE1/0/4	Spine1 10GE1/0/2	Spine1 10GE1/0/4	Leaf6 25GE1/0/3	
((-))	<pre>/</pre>								
Telemetry	(	21	Leat4 10GE1/0/17	Spine2 10GE1/0/	Spine1 10GE1/0/1	Spine1 10GE1/0/23	Leaf5 25GE1/0/1		
8		Total							
		$\smile$	10GE1/0/2	5pine2 10GE1/0/	2 10GE1/0/10	10GE1/0/3	25GE1/0/3		
	High Ri	sk Of Fault 1 (4.76%)	Leaf2	Spino 2	Suine1	Series	Lesf6		
	Subhea	Ith 0 (0%)	10GE1/0/1	10GE1/0/:	3 10GE1/0/19	10GE1/0/33	25GE1/0/1		
Alarm	- Norman								pe: 21 • 1/1 •
	Optical Module Attrib	ute		Optical Module Top			ault Probability Prediction Curve	e	
	1 == 14			Eault Drobabiliter 87%					
	10GE1/0/1	HUAWEI	gbic	Laser error	Fault	Probability: 0%			
				L					
			2017 07 21	<u> </u>			1/7:		
	Administrative Status	Running Status	Production Date	192.168.113.2 10GE1/0/1		92.168.10.1			
							2018-10-13 2018-10-15	2018-10-17 2018-10-19 2018-10	21
	Online the state	- D-1-							
	Optical Module Metric	Data							
	E 10-12 00.00								ŧ
() Help	-3								
	Sanding Downer (dPm)								

# Training the knowledge inference engine using AI, achieving minute-level locating for 75 types of faults

FabricInsight continuously conducts fault drills in Huawei, sorts out 75 types of faults (7 categories in total) based on Huawei's 30+ O M experience and network fault scenarios of 7800+ data center customers, and builds the knowledge inference engine using AI automatic learning and training results to improve the system immunity.

From the service aspects, FabricInsight summarizes faults as typical application quality, network service, and security compliance issues for intelligent recognition and analysis of service faults, helping O&M personnel analyze the impact and quickly rectify faults.

• Application quality issues

FabricInsight can intelligently detect and analyze the following issues: continuous service interruption, intermittent service interruption, and host ports not listened. Based on the IP triplet, FabricInsight can identify services with abnormal TCP connection setup on the network, enabling users to quickly view active and historical issues and affected sessions, hosts, and applications. In addition, FabricInsight can analyze the abnormal event trend and network-wide connection setup information, helping users quickly collect and analyze issues.



										0	unction Strict	Today
FabricInsight												Search
08												
Dashboard	62	Continuous Service Interruption	Intermittent Service In	erruption	Host Port Not Listened On							
Ö	•	Active Issue Count Baseline Exception Count 1	Active Issue Count 2 Baseline Exception Co	unt 1	Active 2485 Historical 47540							
Issue Analy	$\odot$	Affected Hosts 2		0	Affected Session 2615	Ê						
Network					Affected Hosts 11 Affected Apps 2							
e,	G											
Application												
-A- Event	8	tatistics Issue List Original Abnor										
(1.1)		Original Abnormal Event Trend Analysis										
Telemetry												
8												
Edge Intelli		Baseline Exception Count: 1/1(Current/Total)	< >						Number of Original Statement of Original	inal Anomalies	Dvnamic Bas	eline
AJ												
												Intelligent
Alarm												Agent
•(: Inventory												
Ø												
System	Baseline Exception Time Range 2019-08-06 09 42 00-2019-08-06 10 59:00, New Original Abnormal Event Count 1232, Exception Time 2019-08-06 09 42 00, Original Abnormal Event Count 316422, Issue Count 1.											
O Ares Guard		Decommended Other Analysis										
		Consumer IP	onginal Abnormal Event Ci	Provider								
		Total After Deduplication: 120 Duplication Rate: 90		r Deduplication:2 Duplic		Total After De						
		172.1.2.80	1.62% 192	168.2.3	50.08%	172.1.2.80->	1	0.97%				
		172.1.2.12	1.54%			172.1.2.67->	1	0.89%				
		172.1.2.60 1.3%					1	0.81%				
		172.1.2.75 1.3%					1	0.81%				
		172.1.2.10 1.22%					>	0.81%				
		172.1.2.100 1.22%				172.1.2.6->1	9	0.73%				
		172.1.2.54 1.22%				172.1.2.58->	1	0.73%				
		172.1.2.81		168.2.2	49.92%	172.1.2.60->.	1	0.73%				
L⇒ admin					-3.3LN							
Help												

For abnormal events, FabricInsight collects data such as service flow paths, device configurations, entries, and abnormal logs, generates network snapshots, and rectifies faults based on knowledge inference, helping locate root causes in minutes.

Troubleshooting Procedure									
Fabric: POD6-collector Network Type: Hardware-distributed gateway network Forward Type: Three-Layer Forwarded 🥒									
Network Logic Topology			Q Q 1:1 € x 0.105-> 0.100						
Spotogy Abhormal Flow Path 🕐 Path1: 04-15 20:10:56,518 (SYN) 📀	Including 1 events								
VM VM 10.105 10.136.242.165 Normal Flow Path O Path1: 04-10 09:30:00,30 (FIN ACK) O	Including 2 events								
VM VM VM 0.105 0.100 10.136.242.165									
Asset Troubleshooting Possible faults: 1			Vev						
Possible Cause F	ault Point	Additional Information	Discovery Time						
✓ The VXLAN tunnel status is Down.	POD6-MiagLeaf2-2								
No data.									

• Network service issues

FabricInsight can proactively check whether the entry resource usage of the network device forwarding plane on the fabric is abnormal. The issues include the following: TCAM resource insufficiency, insufficiency or abrupt changes of FIB, ARP, and MAC address entry resources. FabricInsight can locate such an issue to the specific board, chip, and resource type.



		O Last 24 Hours
FabricInsight		
Dashboard	Insufficient TCAM Resources     Insufficient y CAM Resources     Insufficient y or Sharp Change of Fitile     Insufficient y or Sharp Change of ARP       Imposed Denses 0     Imposed Denses 0     Imposed Denses 0     Imposed Denses 0       Imposed Denses 0     Imposed Denses 0     Imposed Denses 0       Imposed Denses 0     Imposed Denses 0     Imposed Denses 0	
E Application		
-4- Europe	hues	
((+))	Insufficient TCAM Resource Issue Distribution	
Telemetry	Meters Insufficient Resource Distribution Ingress   Pre-Ingress   Egress   Ingress   Egress   Eg	
Edge Intelli	Slick hulffidett Resources 1 Lade(SciUd)/ofgress 5	reshold:80%
@ AL Jobs	Spin-2/dat/ChyDrogens 63	
	Lash/ShUC/Shp0ingers 52	
Alarm	Commer monitorin who to see 1	
Inventory	Rules Insufficient Resources 0	78% 84% 90% 96%
© System	Issues	
	1	
	Active Historical	
		Use Percentage of Used
	Resource Usage Trend Exception Contract   Last How / Last J Days   Last 7 Days	Threshold Setting ded Threshold Exceeded
Et open		
for all the	1807 1809 1811 1811 1815 1817 1819 1821 1823 1827 1829 1831 1833 1833 1837 1839 1841 1843 1845 1847 1849 1840 1845	18:59 19:01 19:03
Chalkense		
O About		
(7) Help		

• Security compliance issues

FabricInsight can quickly detect security compliance issues and proactively identify potential non-compliant traffic interactions, suspicious SYN flood attacks, and suspicious port scanning attacks. FabricInsight comprehensively analyzes related data to identify the location of the suspicious attack source, analyzes the attack impact on the target host, and helps users audit non-compliant traffic.



Associating software and hardware with edge intelligence and comprehensively analyzing specified flows



Based on the intelligent switch chip, FabricInsight provides edge intelligence and can comprehensively analyze UDP/TCP flows as required. The intelligent chip obtains and analyzes all the flows passing through the VM passes through in real time, including flow characteristics, packet loss, RTT delay, and traffic, and reports the analysis result to FabricInsight. Compared with reporting raw data, reporting analyzed data reduces the data volume by 99%, greatly reducing the impact on the analysis server. In addition, FabricInsight correlates and analyzes the data of the application network, network paths and network devices, compares the path delay hop by hop, and locates the packet loss point in minutes.

						C Last 1 Hour
FabricInsight						Search
Dashboard Ö Health Ö Issue Analy Network	156.7.7.024>157.7.7.6000     Protocot TCP     Number of Packet Loss     Kinth Session Count 7     Number of Packet Loss     Owner Source Configuration     Service Configuration	156 7.7 0/24>157.7.7.7 5001 Protocol UDP Total Session Count 6 Number of Packet Loss Enable Measuring Point 66 Latency Threshold (or) 5 Device Configuration	+			
e.						
Application	Basic Information					
Event	2/6 Number of Packet Loss Sessions	1,284/92 Number of Lost Pack	0 iets/Total N	1.73MB/1.24MB Lost Traffic/Total Traffic	570.03ms/2.89s Average Latency/Maximum Latenc	
((+)) Telemetry						
2	Analysis Conclusion					
Edge Intelli	A Packet loss occurs during netwo	rk forwarding. The percentage of packet loss sessions is eeds threshold(5us) and reaches 570.03ms.	33.33%, and the percentage of lost packets is 1009	₩. ►		
AI	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,					
Alarm						
-e						
inventory	Event List					
System						
0						
Ares Guard						

### Comprehensive RoCE flow analysis and AI-based Fabric visualization

For distributed storage, HPC, and AI networking scenarios in data centers, FabricInsight supports RoCE flow analysis and collects session statistics based on the source IP address, source QP, destination IP address, and destination QP. In this manner, users can view KPI details such as the number of packet loss events, RTT, read throughput, and write throughput of a single session in the source and destination directions and the multi-dimensional trend.



# [Product Components]

FabricInsight consists of the basic package and value-added package based on functions and features. The following table describes the Telemetry network analysis functions of the basic package.



Feature	Description
Network status visualization	<ul> <li>Supports visualized and multi-dimensional top N statistics of Fabric data.</li> <li>Displays the Fabric network topology.</li> <li>Supports visualization of network configuration changes.</li> <li>Displays device abnormality logs and trends.</li> <li>Enables users to view detailed information about packet loss events.</li> </ul>
Network abnormality detection	<ul> <li>Displays the key performance indicators (KPIs) of devices, boards, chips, interfaces, queues, and optical links in a trend chart.</li> <li>Displays dynamic baselines and detects abnormalities of KPIs of devices, boards, and interfaces.</li> <li>Supports millisecond-level queue congestion and packet loss detection.</li> </ul>
Predictive maintenance	<ul> <li>Supports optical link health status prediction.</li> <li>Displays the forecast results of the RX and TX bandwidth utilization of interfaces in the next 12 weeks.</li> </ul>
Network service issue detection and analysis	<ul> <li>Supports detection and analysis of TCAM resource insufficiency, and insufficiency or abrupt changes of FIB entry resources, ARP entry resources, and MAC entry resources.</li> </ul>

The following table describes the service flow analysis functions provided by the value-added package of intelligent flow analysis.

Feature	Description
TCP service flow analysis	<ul> <li>Supports visualized top N statistics and analysis of hosts, applications, and sessions.</li> <li>Allows users to view the number of SYN events, abnormal TCP events, traffic, and delay in a specified period.</li> <li>Enables users to view details about packet loss events.</li> <li>Combines packets for analysis in the 1:1 NAT mapping scenario.</li> <li>Supports abnormal flow fault reasoning and one-click troubleshooting.</li> </ul>
Application and network association analysis	<ul> <li>Analyzes application health status.</li> <li>Analyzes interaction between applications and displays application interaction relationships in the topology.</li> <li>Supports intra-application interaction analysis and mutual visibility between applications and networks.</li> </ul>
Intelligent analysis of application quality or security compliance issues	<ul> <li>Supports detection and analysis of application quality issues, including continuous or intermittent services interruption, and host ports not listened.</li> <li>Supports detection and analysis of security compliance issues, including non-compliant traffic interaction, suspected SYN flood attacks, and suspected port scanning attacks.</li> </ul>



Feature	Description
Visualization of all RoCE flows	<ul> <li>Supports visualized network topology views.</li> <li>Collects statistics on the trends of RoCE network read throughput, write throughput, RTT,</li> </ul>
	<ul> <li>and packet loss.</li> <li>Supports RoCE flow analysis and abnormal session trend statistics.</li> </ul>
Edge intelligence analysis	<ul> <li>Support intelligent traffic analysis based on the triplet rules of the specified TCP source IP address, destination IP address, and destination port. The system can display information such as the number of sessions with packet loss, total number of sessions, number of lost packets/total number of packets/traffic in the request direction, number of lost packets/total number of packets/traffic in the response direction, and application interactions based on the specified rule.</li> </ul>
	• Support intelligent traffic analysis based on the triplet rules of the specified UDP source IP address, destination IP address, and destination port. The system can display information such as the number of sessions with packet loss, total number of sessions, number of lost packets, total number of packets, discarded traffic, total traffic, average latency, maximum latency, and application interactions based on the specified rule.

# [Operating Environment]

FabricInsight supports hardware configurations of physical servers and VMs. To avoid unexpected problems, configure the system according to the following software and hardware configuration requirements.

Management Scale	Recommended Huawei Server Configuration	System Configuration
Physical cluster server with 128 GB memory: If only basic packages are purchased,no collector is required. The initial three analyzer and one collector nodes manage 3000 flows per second. One analyzer node needs	Analyzer: TaiShan 200 (Model 2280) Server CPU: 2*48Core/2.6GHz Memory: 128 GB Hard disk: 6*1800GB-SAS 2.5inch Network port: 4*GE+1*4GE	OS: Huawei-developed EulerOS Database: Huawei Gauss100 OLTP
to be added each time when 1000 flows are increased per second. The RoCE flow analysis function must be configured with the 256G physical server.	Collector: TaiShan 200 (Model 2280) Server CPU: 2*48Core/2.6GHz Memory: 64 GB Hard disk: 2*1200GB SAS HDD Network port: 2*4 GE Elec-port	OS: Huawei-developed EulerOS
Physical cluster server with 256 GB memory: If only basic packages are	Analyzer: TaiShan 200 (Model 2280) Server CPU: 2*48Core/2.6GHz	OS: Huawei-developed EulerOS Database: Huawei



Datasheet

Management Scale	Recommended Huawei Server Configuration	System Configuration
purchased, no collector is required.	Memory: 256 GB	Gauss100 OLTP
The initial three analyzer and one collector nodes manage 8000	Hard disk: 12*1800GB-SAS 2.5inch	
	Network port: 4*GE+2*10GE	
flows/seconds. One analyzer node	Collector:	OS: Huawei-developed
in 5000 flows/second.	TaiShan 200 (Model 2280) Server	EulerOS
The RoCE flow analysis function must	CPU: 2*48Core/2.6GHz	
be configured with the 256G physical	Memorv: 64 GB	
server.	Hard disk: 2*1200GB SAS HDD	
	Network port: 2*4 GE Elec-port	
Customer-provided VM:	Analyzer VM types: FusionSphere(KVM)6.5	OS: Huawei-developed
If only basic packages are	VM resource configuration (exclusive use of	EulerOS
purchased, no collector is required.	memory and CPU resources):	Database: Huawei Gauss100 OLTP
The initial three analyzer and one	CPU: 32vCPU	Gaussion OFIL
per second. One analyzer node needs	Memory: 128 GB	
to be added each time when 1000	System disk: 900 GB	
flows are increased per second.	Data disk: 7T	
The RoCE flow analysis function must	The random read and write speed of the hard disk	
be configured with the 256G physical	is greater than or equal to 100 MB/s.	
server.	Network port: At least one network port is required	
	and two are recommended. The network port	
	bandwidth is 1 Gbit/s.	
	Collector VM type: FusionSphere(KVM)6.5	OS: Huawei-developed
	CPU: 32 vCPU	EulerOS
	Memory: 64 GB	
	Hard disk: 600 GB	
	Network port: At least two GE network ports are	
	required.	
	Note:	
	The random read and write speed of the hard disk	
	is greater than or equal to 100 MB/s.	

# [Deployment Scenarios]

The supported networks are as follows:

- Hardware-centralized gateway networking
- Hardware-distributed gateway networking



### • Pure IP networking (Host Overlay)

Network Overlay	Centralized gateway	Distributed gateway
The VXLAN tunnel ends are physical switches.	Edge Edge	Spine Spine
Physical Physical	Spine Spine Leaf Leaf FW VSwitch BM VM VM	Leaf Leaf FW VSwitch Edge
Underlay: IP forwarding	Leaf: VXLAN L2 Bridge     Spine or Edge: VXLAN L3 Routing	Leaf: VXLAN L3 Routing     Spine: IP Forwarding
	• opine of Edge. VAL in ES Routing	
IP Fabric	IP forwa	arding
Virtual Virtual Underlay: IP forwarding	Edge Spine Leaf Leaf	Edge Spine f

#### Remarks:

- (1) The underlay network is based on IP forwarding.
- (2) SVF networking is not supported.
- (3) IP address overlapping scenarios (for example, multi-tenant and VPC scenarios) are not supported.
- (4) Other networking modes such as traditional layer-2 networking (including the VLAN and STP), TRILL networking, and MPLS VPN are not supported.

### [Ordering Information]

Module		Туре	Description	
Software subscription	Software package			
	Basic package of intelligent network analysis	Mandatory	This module is purchased based on the number of CloudEngine switches in the data center.	
	Value-added package of intelligent flow analysis	Optional	This module is purchased based on the number of VMs or PMs in the data center.	
	Big data analysis license - per node	Mandatory	This module indicates the number of big data analysis nodes.	
	SnS			
	Basic package of intelligent network analysis - SnS	Mandatory	This module corresponds to the basic package of FabricInsight intelligent network analysis, which has the same number. You can choose 1 year or 5 years for the SnS.	



Module		Туре	Description
	Value-added package of intelligent flow analysis - SnS	Optional	This module corresponds to the value-added package of FabricInsight intelligent flow analysis, which has the same number. You can choose 1 year or 5 years for the SnS.
	Big data analysis license - per node - SnS	Mandatory	This module corresponds to the big data analysis license - per node. You can choose 1 year or 5 years for the SnS.
Hardware subscription	Analysis server	Optional	This module indicates the number of servers required by the FabricInsight analyzer.
	Collection server	Optional	This module indicates the number of servers required by the FabricInsight collector. If reliability is required, configure two servers for each fabric.

FabricInsight can provide a 180-day trial license. You can obtain the license from Huawei local sales department.

#### <u>More</u>

For more information about the Huawei FabricInsight, visit http://e.huawei.com



### Copyright © Huawei Technologies Co., Ltd. 2019. 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:	http://e.huawei.com