

Fabric Controller Centralized Manager

Centralized network management for Keysight visibility solutions

Introduction

To cope with skyrocketing traffic volume and escalating security threats, today's networks employ sophisticated, pervasive monitoring capabilities. The resulting architecture incorporates hundreds – of taps and bypasses, data monitoring switches, and Network Packet Brokers (NPB), all integrated into a Monitoring Access Platform (MAP) within the network infrastructure. But along with the vital advantages of this architecture, there is challenge of managing these devices for configuration, monitoring, bulk software upgrades, and more.

Keysight's Ixia Fabric Controller (IFC) Centralized Manager is delivering the right high-performance and efficiency features. IFC Centralized Manager also offers High Availability (HA) for robust, comprehensive management capabilities and lets you manage a wide deployment of wired, wireless, and/or virtual devices. This versatile platform allows growing networks to expand their management and planned capabilities to keep pace with increasing needs as devices are added. IFC Centralized Manager eases configuration and monitoring of taps, virtual taps, data monitoring switches, and network packet brokers – turning them all into fully orchestrated and coordinated monitoring resources.

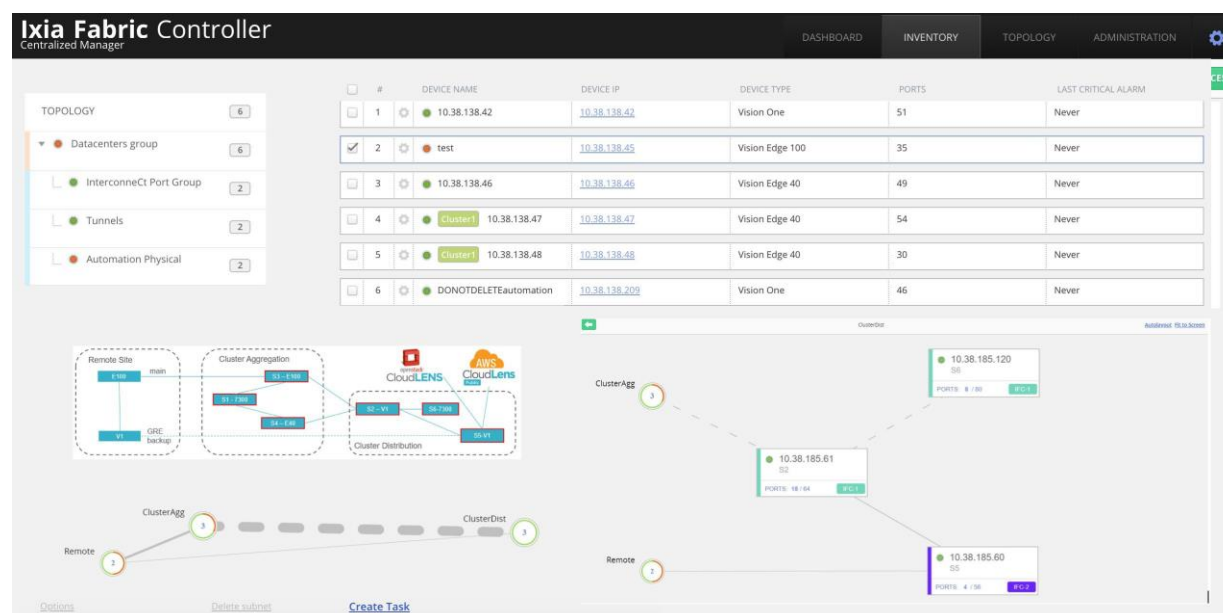


Figure 1. IFC Centralized Manager Dashboard

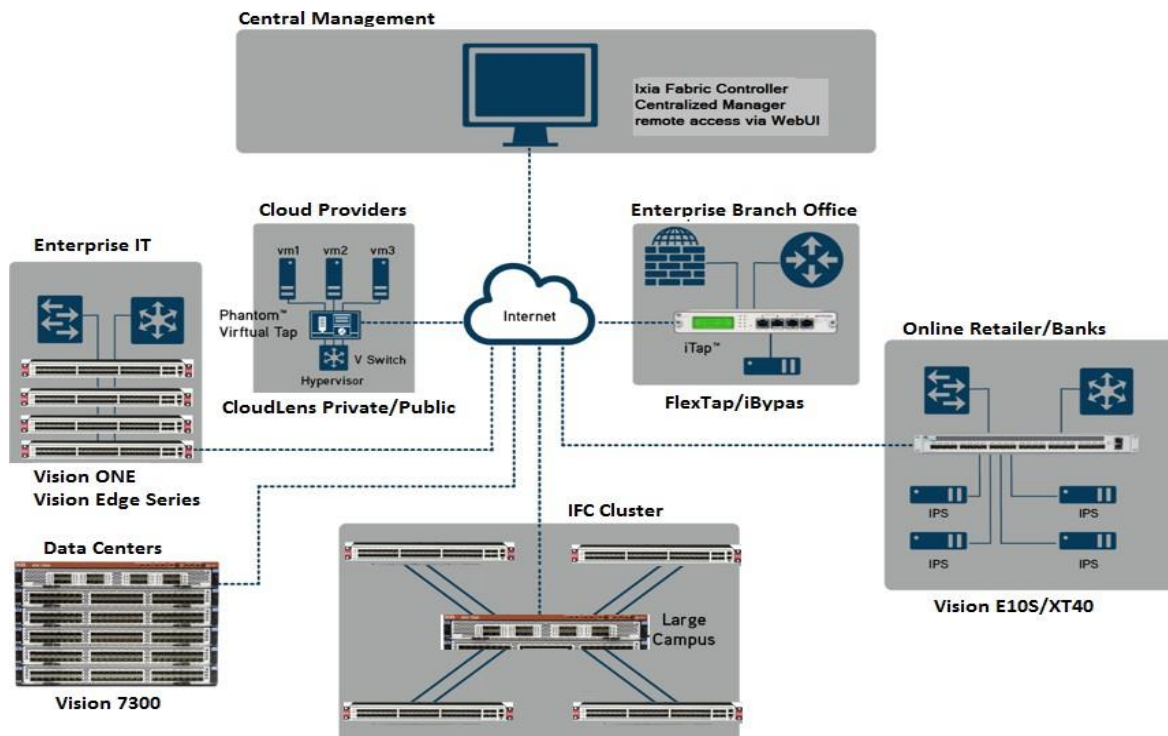
Highlights

- Centralized manager to offer single pane of glass for large numbers of managed devices through auto discovery
- Innovative topology visualization with node grouping, interconnect links, and size, color, width all proportional to the actual # of nodes in group, alarms in each group, and physical bandwidth of the link
- Single Sign On (SSO) and zero touch provisioning for discovered Keysight Vision Packet Broker devices
- Physical or virtual implementation: support for VMware and KVM
- High Availability (HA) with floating IP between active and standby units
- Active/standby can be cross-form configuration: physical-physical, virtual-physical, and physical- virtual
- Northbound Interface to support fault management with another Network Management Solutions
- Device configuration and management
- Alarms and events management
- Audit trail
- Scheduler to support software upgrade, script/policy execution, and configuration import/export across many devices
- Event triggered response to execute custom scripts
- At-a-glance dashboard views
- Snapshot and historical data views
- Trap and email forwarding
- Business logic alerts
- Monitors traffic levels and quality across the network
- Expanded RADIUS, TACACS+ and LDAP authentication

IFC Central Manager Offers a Single Pane of Glass for Visibility Management

IFC Centralized Manager is delivered either as a physical appliance or as a virtual appliance in VMware or Oracle Virtual Box format. Deployment is amazingly simple too, thanks to a fast, fully automated discovery process that can quickly identify all supported Keysight Vision products, Keysight iTap/iBypass/xStream/Vision family of products. IFC Centralized Manager also checks continuously for devices being removed or taken offline. It also checks periodically for devices newly added. A dynamic network topology map instantly shows the 'up' or 'down' status of all supported devices, in addition to custom status, based on active alarms (Minor, Major, Critical, SNMP error). Click on a device object/icon to drill down into detailed device status and configuration information, as well as the status of attached links.

Reliability and security features



IFC Centralized Manager offers a spectrum of features to expand authentication support. Your management and administration duties will be easier than ever, thanks to enhanced network visibility and security, plus extended virtual support. The newly enhanced High Availability (HA) feature supports active and standby units in complete sync with one floating IP address; allowing instant takeover by the standby unit when the active unit fails. Best of all, the active and standby units can be either physical or virtual or a combination of both, enabling maximum deployment flexibility.

Comprehensive configuration and fault management

IFC Centralized Manager supports a scheduler that allows automated task execution across many devices. Common management tasks include, for example, script and policy execution, software upgrades, configuration import and export, and many more. More sophisticated mechanism is implemented to allow you to execute customer scripts when one or more general events, or device specific events take place in the entire managed network.

Improved data visualization

IFC Centralized Manager gathers data in real time from discovered Keysight, archives that data in a database for historical trend analysis, and then presents it in rich graphical formats through a web browser interface. IT users benefit from the efficiency, accuracy, and cost savings they realize by employing IFC Centralized Manager to monitor network health and trouble spots. IFC CM can also scale, supporting your capacity planning, and compliance activities.

IFC CM's enriched capabilities include more visibility and presentation options, with an increased number of charts or dashboards per user – and users can now customize their own views of interest. IFC CM even remembers and creates a user-specific dashboard upon login to save time and access to relevant data faster.

Traffic statistics displayed include bandwidth utilization, byte and packet counts, errors, and jumbo frames, all viewable on a device-by-device basis. In addition, a dashboard can be configured to confederate the data from multiple links and devices for an at-a-glance overview of network traffic activity.

Security and user management

The IFC CM platform delivers a total solution to all NMS security-related issues. All user actions are inspected and audited against the permissions profile and logged to an audit trail. The system's security is structured in three layers:

- External authentication through LDAP, RADIUS and TACACS
- Authenticated and encrypted sessions between the client web browsers and the server throughout a user's entire sessions
- User authentication by a login session based on a user name and password
- Role-based access control and device locking to ensure that a given user can perform certain actions on specific devices with read or write permissions. These are based on a global policy that meets the organization's compliance standards

Specifications

Specification	Description
Functionality	<ul style="list-style-type: none"> • Fast, automatic device discovery • Device configuration and fault management • High availability with active and standby redundancy in physical, virtual, or combined • Innovative topology visualization with color coded node groups and interconnect links of different shapes to reflect physical interconnects, IFC Cluster interconnects, or L2GRE tunnel • Single Sign On and Zero Touch provisioning for discovered vision devices • LLDP auto discovery and topology display for SPANs, TOOLS, and interconnect links • Data visualization: snapshot and historical, utilization, total bytes, total packets, jumbo packets, CRC errors, dashboard views • Dashboard of graphs • Security: profile-based permissions and views, comprehensive audit trail, and role-based access control • Data export (print, export to CSV file) • Device management (device dependent): port settings, device system settings, device user accounts • Device-dependent event logging and fault management • Scheduler for bulk software upgrade, script and policy execution, and configuration import/export
Virtual Appliances (Optional)	<ul style="list-style-type: none"> • VMware vSphere 5.x and 6.0 support • CentOS 7 (64-bit) • 2GB RAM • 20GB HDD • 4 CPU
Physical Appliances (Optional)	<ul style="list-style-type: none"> • Dell PowerEdge R640 XL Server • 64GB RAM • 640G SSD • Intel Xeon Silver 4110 2.1G, 8C/16T, 9.6GT/s 2UPI
Operating Environment	<ul style="list-style-type: none"> • Operating Temperature: 10°C to 35°C • Storage Temperature: -10°C to 70°C • Relative Humidity: 10% min, 90% max, non-condensing
Physical Specifications	<ul style="list-style-type: none"> • Dimensions: 1.75" high x 23.5" deep x 19" wide • Mounting: 19" rack mount (1U) • Weight: 26 lbs (11.8kg)
Electrical Specifications	<ul style="list-style-type: none"> • Power: 100-240 VAC, 47-63Hz 650W PFC • Redundancy: Dual modules • Maintenance: Power supplies are hot-swappable Indicators • Power, disk activity, network 1 activity, network 2 activity, over temperature warning
Certifications	<ul style="list-style-type: none"> • FCC, CE, VCCI, and C-Tick certified • Fully RoHS and WEEE compliant

Specification	Description
Supported Web Browsers	<ul style="list-style-type: none"> • Internet Explorer, Firefox, Safari, Chrome
Supported Devices	<ul style="list-style-type: none"> • Keysight Vision ONE/X, Vision 7300/7303, Vision Edge 40/100/E10S, 7816 • Keysight NTO ControlTower • Keysight GTP Session Controller • Keysight TradeView • Keysight xStream 40 and xStream 10 • Keysight Director, Keysight Director Pro • Keysight xBalancer • Keysight iTap and iTap2 • Keysight iBypass 1G • Keysight iBypass 10G • Keysight iBypass 3 CU3 • Keysight iBypass HD • Keysight iBypass VHD • Keysight iBypass 40-10 • Keysight iBypass DUO • Keysight IXTP-CU3, IXBP-CU3, IxProbe • ISIP1

Ordering Information

Part number	Description
991-0135	Keysight Vision Management Appliance; Support running IFC CM and Hawkeye Manager. Adjunct or separate node license must be purchased
991-0135-T	TAA Compliant, Keysight Vision Management Appliance; Support running IFC CM and Hawkeye Manager. Adjunct or separate node license must be purchased
LIC-VA025-M	Keysight IFC Centralized Manager, 25 nodes
LIC-VA050-M	Keysight IFC Centralized Manager, 50 nodes
LIC-VA100-M	Keysight IFC Centralized Manager, 100 nodes
LIC-VA250-M	Keysight IFC Centralized Manager, 250 nodes

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.



This information is subject to change without notice. © Keysight Technologies, 2016 – 2023, Published in USA, October 25, 2023, 7019-0147.EN