IBM **Guardium**
Discover and Classify

NETWORK MAPPING USER GUIDE

IBM GUARDIUM DISCOVER AND CLASSIFY

VERSION 4.3.2

TABLE OF CONTENTS

NETWORK MAP OVERVIEW

The **Network Mapping** application is a part of the IBM Guardium platform that displays the topology of your organization's network. The network map shows the communication nodes (databases, file systems, and other network elements as PCs) discovered by the analytical appliances, links between the nodes, and the node type like database, central storage, web application and others.

IGDC is designed for operation with the latest version of Google Chrome. Using other browsers is not recommended and may affect performance and functionality

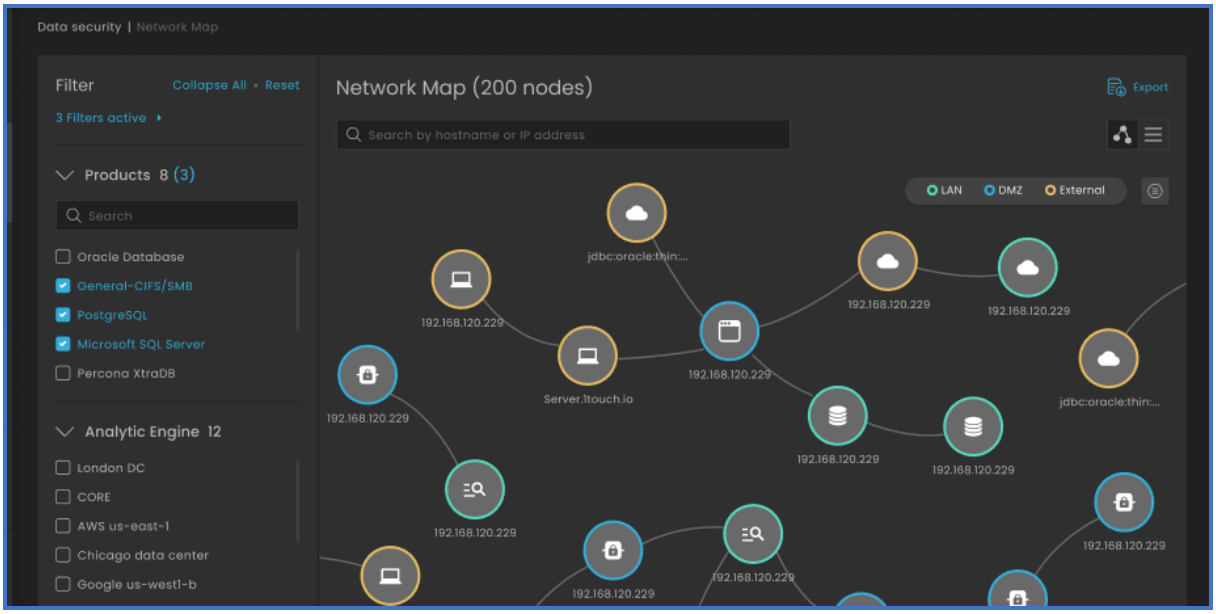

Figure 1: Example of Topology Visualization in the Network Mapping Module

TOPOLOGY ANALYSIS

The IBM Guardium analytic appliances constantly analyze your organization's network to discover new nodes and links between the nodes. The system also determines auxiliary properties like the node's role in the network (server/client) or whether it processes personal data.

After each network analysis cycle, its results are visualized via the topology map in the **Network Mapping Flow** page, so that the number of network elements dynamically changes while the system analyzes your network and the system discovers new nodes.

Although the network is continuously analyzed, you will see any changes on the network map only after refreshing the webpage.

A node may be removed from the map when it is removed/deleted from the network. A link between two nodes is removed if the system did not detect any traffic exchange between said nodes during the most recent analysis cycle. The node/link will be recovered on the network map if and when the system re-discovers the node/detects traffic in the next cycles.

The network map will not show nodes if their IP addresses were configured to be ignored by the discovery module in the analytic engine settings.

For assistance in configuring nodes to be ignored, see **Analytic Engine and Console Manager Admin Guide**.

NETWORK ELEMENTS AND THEIR PROPERTIES

In the network map, a network element is a communication node discovered by IGDC in your network. The system focuses on servers (databases, file systems, etc.) or clients exchanging data with the server (PCs or other servers), excluding intermediary network devices like switches.

For each network element, the system also discovers metadata (if available) - node properties used for filtering the elements displayed on the network map like **IP address**, **subnetwork**, **product** , **protocol**, and the **appliance** that discovered the node.

NETWORK MAPPING VISUALIZATION

To see the topology of your organization's network, go to the **Network Map** page (**IGDC Platform > Data Security > Network Map**). By default, the page will show a map of 200 nodes (or less if the system discovered fewer than 200 nodes).

The visualization of the nodes allows analysis of their properties like address, function, and subnetwork as described in the table below.

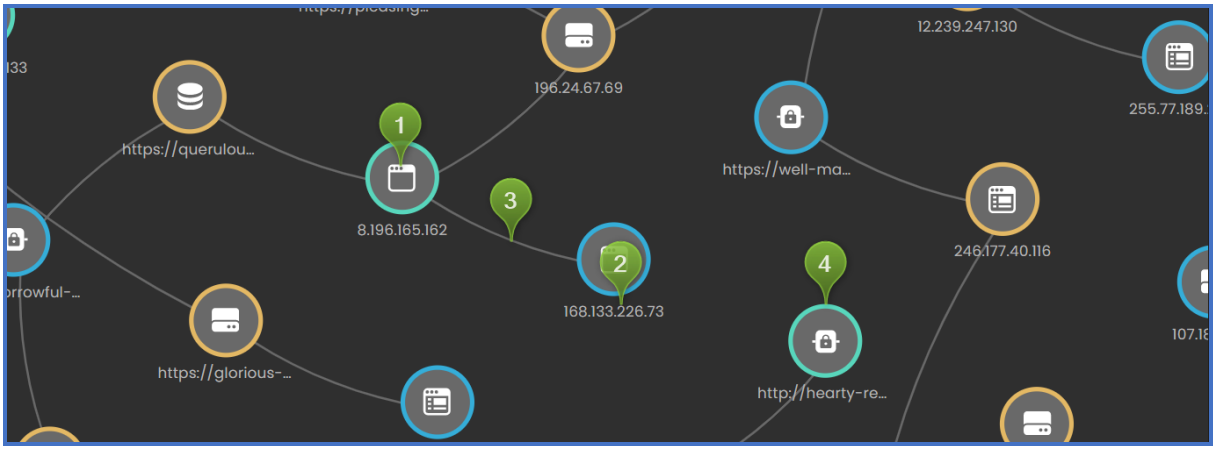

Figure 1: Node visualization on the Network Mapping Flow page

Table 2: Node Visualization on the Network Mapping Flow Page

PROPERTY	VISUALIZATION
Type (1)	The image in the icon indicates the node type, representing its function in the system. For example,  stands for a database. Hover over the icon to see the node type.
IP Address (2)	The IP address of the node is shown under the icon.
Links (3)	Links with other nodes on the map indicate that the system detected traffic exchange between them during the last network analysis.
Subnetwork (4)	The color of the frame around the icon indicates the subnetwork where it was discovered. The system maps the subnetwork based on the subnet and domain configurations in the anaytic engine settings: **LAN** - THE NODE BELONGS TO THE SUBNET/IP RANGE CONFIGURED AS LAN OR THE NODE HOSTNAME MATCHES YOUR ORGANIZATION'S DOMAIN NAME. **DMZ** - THE NODE BELONGS TO THE SUBNET/IP RANGE CONFIGURED AS DMZ. **EXTERNAL** - THE NODE DOES NOT BELONG TO ANY SUBNETS, IP RANGES, OR DOES NOT MATCH ANY DOMAIN NAME FROM THE IGDC UI. If the subnetworks are not visualized on the network map, ensure that the subnetworks and/or domain names are configured in the analytic engine settings.

MAP VIEW MANAGEMENT

The **Network Mapping Flow** page consists of the network map and a sidebar with filters. The map also contains an **Info** pane that provides hints regarding colors indicating the node's subnet. By default, the page shows the topology in map view.

The icons in the lower right corner allow you to change the map view as follows:

- Click **+** and **-** buttons to zoom in an out.
- Click the  (**Full screen**) icon to open the map full screen.

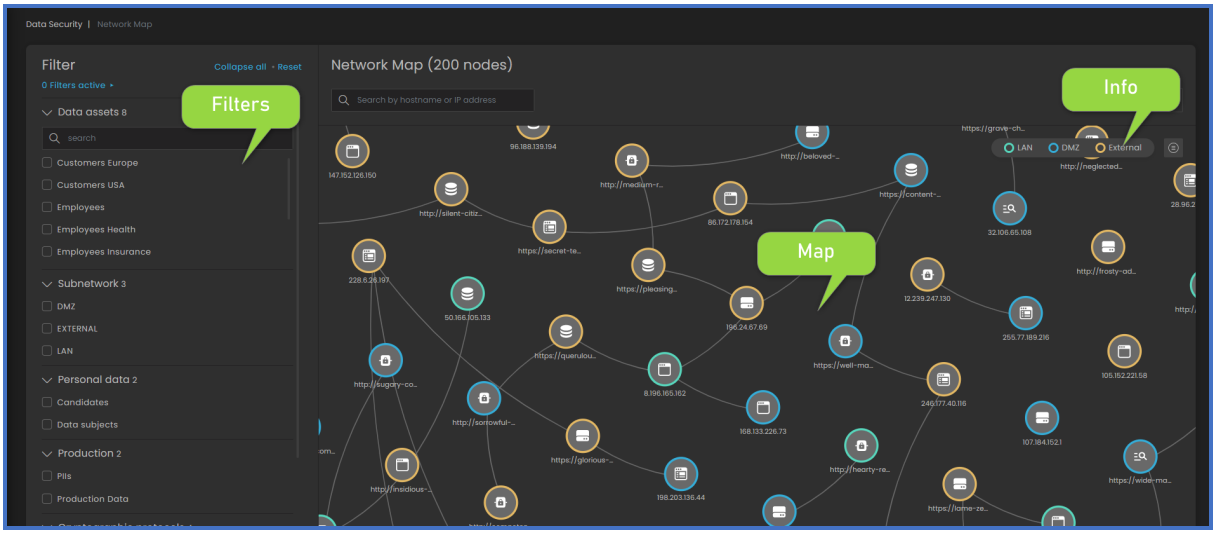

Figure 1: Network Mapping Flow Page with Default Settings

Click the  (**Table**) icon to see the topology in table view. It shows a list of nodes with node URL, node type and subnetwork per node. Click the (**Expand**) icon to see the number of related nodes.

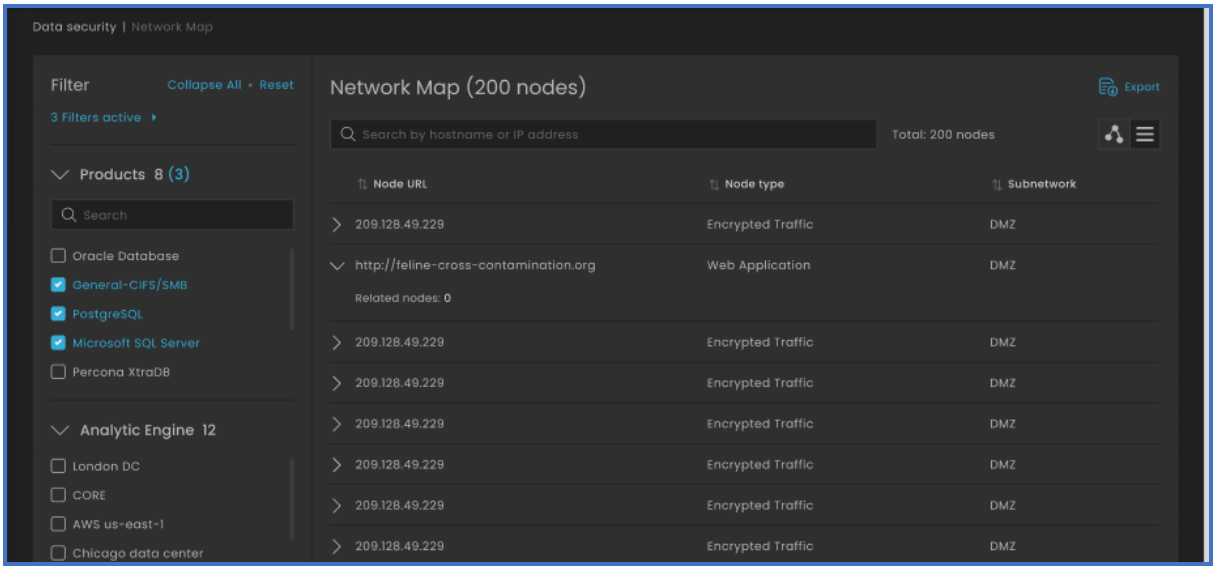

Figure 2: Topology table view

NETWORK MAP FILTERS

You can select multiple options to filter the nodes present in the .

Table 3: Supported Filter Types

PROPERTY	DESCRIPTION
Subnetwork	Subnetwork to which the node belongs according to the subnet and domain configurations in the analytic engine settings. You can select the network elements belonging to the following subnetworks: **LAN** RELATES TO THE NODES FROM YOUR ORGANIZATION'S LOCAL SUBNETWORK, MEANING THAT THE NODE BELONGS TO THE SUBNET/IP RANGE CONFIGURED AS LAN OR THE NODE'S HOSTNAME MATCHES YOUR ORGANIZATION'S DOMAIN NAME; **DMZ** RELATES TO THE NODES FROM YOUR PERIMETER SUBNETWORK, MEANING THAT THE NODE BELONGS TO THE SUBNET/IP RANGE CONFIGURED AS DMZ; **EXTERNAL** RELATES TO THE NODES THAT HAVE NOT BEEN MAPPED TO EITHER LAN OR DMZ. If the **Subnetwork** filters are not present, ensure that subnetworks and/or domain names are configured in the analytic engine settings.
Repository type	Type of the data source. For example, *database*. Refer to the list of supported data source types for more details.
Personal data	Indicates whether the system discovered and retrieved any personal data from the network element in the previous cycles. You can select the nodes with the following personal data types: • **Data subject** is a copy of trusted personal information that was retrieved from the network element and then confirmed against your root data asset; • **Candidate** is a copy of personal data that was retrieved from the network element by the system but was not confirmed against your root data assets If the **Personal Data** filters are not present, ensure that the system has discovered data subjects and/or candidates. For example, check the data at rest and data in motion in the **Default** data asset (**Inventory > Data Asset Management > Default**) or check that candidates are shown in the **Supervised AI** application.
Product	Product name retrieved from the data packets captured in the traffic sent and received by the node.
Protocol	Node's data exchange protocol. For example, *HTTP*. Refer to the list of supported data source types for more details.
Analytic Engine	Unique identifier of the appliance that discovered the network element. The filter will appear when the first node appears on the network map.

REPORTING

The **Network Map** now supports network topology reports in CSV, XLSX, and JSON formats. You can export a list of network elements (nodes) and their metadata that IGDC has discovered.

Figure 1: Exporting network topology

2. In the **Export** popup, select the report details. Click the **Export** button and the report will be downloaded to your PC according to your browser settings. To exit without exporting the report, click **Cancel**.

Table 2: Network topology report details

PARAMETER	DESCRIPTION
Format	Select the report file format. Supported formats: XLSX, CSV, JSON.
File name	Enter the report file name. Format: up to 200 characters.
Limit	Set the maximal number or rows in the report. Default is 1000 rows, maximum - 1M.
Offset	Enter the row number at which you wish to start the export.

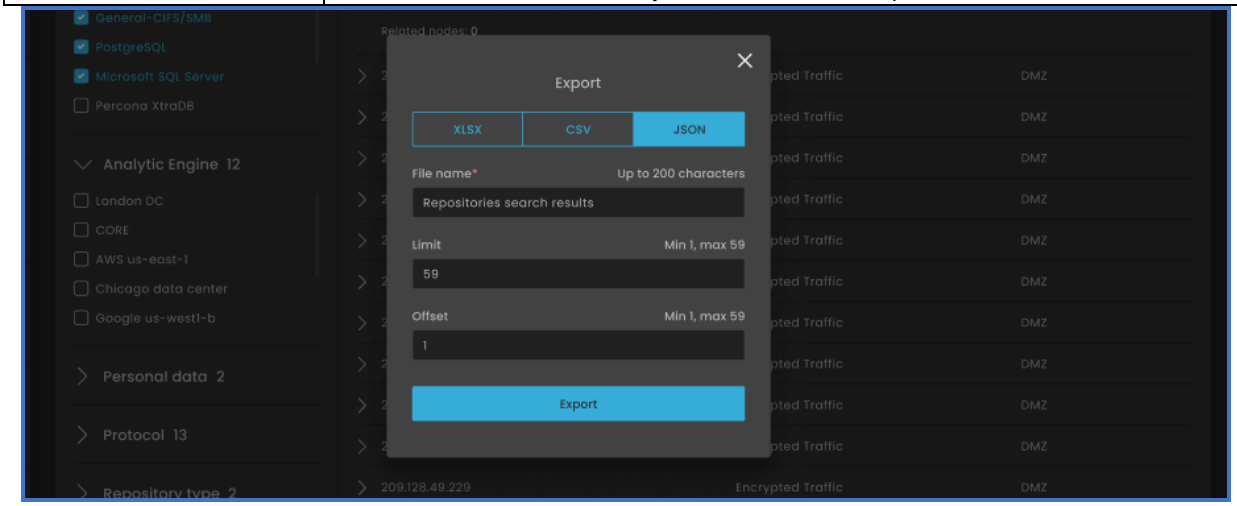

Figure 3: Export popup

APPENDIX A: NETWORK MAP SUPPORTED PROTOCOLS

Table 1: Supported Protocols

PROTOCOL	PRODUCT	DATA SOURCE TYPE
TNS	Oracle Database	Database
SMB/SMB2	General-CIFS/SMB	Central Storage
PGSQL	PostgreSQL	Database
TDS	Microsoft SQL Server	Database
MYSQL	MySQL Database Server	Database
HTTP	General-HTTP; Apache Solr; Microsoft Dynamics; Percona XtraDB	Web Application; Enterprise Search; CRM; Database Engine
COUCHBASE	Couchbase Server	Database
TLS	TLS	Encrypted Traffic
SMTP	General-SMTP	SMTP
KAFKA	Apache Kafka	Stream Processing
DRDA	IBM DB2	Database
NFS v.2,3,4	NFS General	Central Storage
MariaDB	MariaDB	Database
MONGO	MongoDB	Database
ICAP	HTTP	Web Service

IBM, the IBM logo, and IBM Guardium Discover and Classify are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.