Table of Contents

Traffic-based discovery in Service Mapping

Release version: Washington DC

Updated Feb 1, 2024

4 minutes to read

Summarize [Beta]

Service Mapping can discover and map configuration items (CIs) following their traffic-based connections. This method is referred to as traffic-based mapping and it complements the pattern-based mapping.

What is traffic-based mapping

Using traffic-based discovery is like casting a finer net, allowing Service Mapping to find even those CIs that it hasn't discovered using patterns. If a CI has two connections, the traffic-based connection disappears after the next top-down discovery, and any manual or pattern-based connections remain.

Depending on your configuration, the behavior of traffic-based discovery varies. If discovery based on Predictive Intelligence is enabled, Service Mapping automatically adds connections to application services based on connection rules. Service Mapping generates these suggestions based on traffic-related data from the Configuration Management Database (CMDB) and on Predictive Intelligence analysis of application fingerprints, CIs, and processes.

If discovery based Predictive Intelligence is disabled, Service Mapping automatically adds traffic-based connections based on the CMDB data to application services. You may need to remove connections leading to irrelevant CIs to declutter application services. Typically, if the connection suggestions feature is turned off, you use traffic-based discovery at the initial stages of discovering application services. Disable traffic-based discovery after you complete discovery and fine-tuning of application services.

If pattern-based discovery runs after traffic-based discovery runs, it may create duplicate connections between CIs. In that case, the system removes the connection created using traffic-based discovery. The system keeps any connection created by traffic-based discovery and not discovered using patterns.

Traffic-related data from the CMDB

The system uses commands and network flow logs to collect traffic-related data and saves it in the CMDB tables. Service Mapping retrieves this data from the tables to detect CI inbound and outbound connections.

Tables containing data collected using traffic-based methods

Table	Source	Used by Service Mapping to
Flow Connector [sa_flow_connection]	Netflow and VPC logs	Discover dependencies, add connections during top-down discovery.
Flow Services IP/Port and Statistics [sa_flow_service]	Netflow and VPC logs	Discover all services listening on ports. In a base system, Service Mapping does not use data from this table.
Flow Server Communication [sa_flow_server_comm]	Netflow and VPC logs	Discover services communicating to other services. In a base system, Service Mapping does not use data from this table.
TCP Connection [cmdb_tcp]	netstat and lsof commands	Discover connections during top-down discovery.

In base systems, traffic-based discovery uses only TCP-related data collected with the help of the `netstat`, `ss`, and `lsof` commands. Discovery based on Netflow and VPC logs requires additional configuration. You can enrich your traffic-based discovery by configuring Service Mapping to perform data collection using Netflow and VPC logs. In addition, Service Mapping has access to the TCP connection data collected by improved Application Dependency Mapping (ADM). Discovery performs ADM as part of horizontal discovery.

Enabling traffic-based discovery in the system

By default, traffic-based discovery using commands is available in Service Mapping allowing it to use this method at all levels. You can enable traffic-based discovery at different levels, from the most global to the most specific:

Product level

By default, traffic-based discovery in Service Mapping is turned off. The **Traffic based discovery** property `[sa.traffic_based_discovery.active]` controls the traffic-based discovery at the product level.

> **Important:** You can't enable traffic-based discovery at other levels unless it's enabled at the product level.

The connection suggestions feature works at the product level. The `sa_ml.connection_suggestions.active` property controls this feature. If traffic-based discovery was enabled in your deployment prior to Quebec and you used it to discover at least one application service, the connection suggestions feature is turned off by default.

Application service level

You can enable traffic-based discovery for a specific application service. In this case, Service Mapping uses this method for all CIs making up this application service, unless traffic-based discovery is turned off for some CI types or specific CIs.

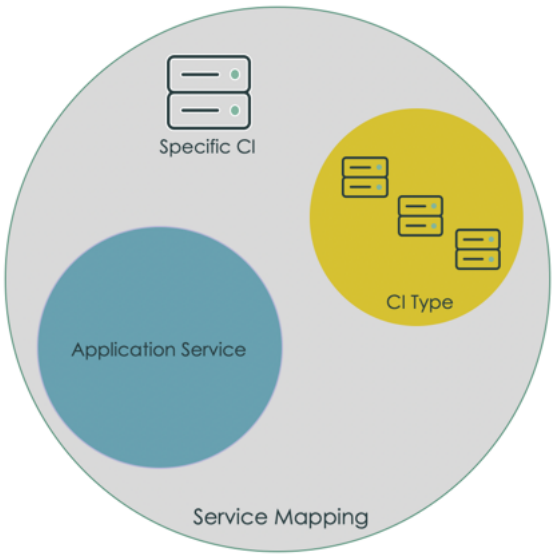
CI type level

You can create a discovery rule to include or exclude a CI type from traffic-based discovery. This rule prevails over the setting you choose for an application service.

Specific CI level

You can create a discovery rule to include or exclude a specific CI from traffic-based discovery. This rule prevails over the setting you choose for an application service.
Rules for specific CIs take precedence over rules for CI types. For example, if you do not want to use traffic-based discovery on any Apache Tomcat servers, you can define a **CI type** rule disabling the traffic-based discovery on the Tomcat table. At the same time, you can create a discovery rule enabling the traffic-based discovery for a specific Tomcat server. In that case, Service Mapping uses the traffic-based discovery only for this specific Tomcat server out of all Tomcat servers.

Enabling traffic-based discovery at different levels



Previous

‹ Tag-based discovery in Service Mapping

Next

Discovery of application services on cloud using Service Mapping ›

servicenow

The world works with ServiceNow.™