≡ Table of Contents

Pattern-based discovery in Service Mapping

•••

Release version: [Washington DC ⌄]

Updated   Feb 1, 2024

🕐 4 minutes to read

Summarize [Beta]

Pattern-based discovery is the main method of Service Mapping collecting data about devices and applications used in application services. After Service Mapping collects data, it then creates a map of application services and stores the collected data in the CMDB.

ServiceNow applications refer to devices and applications that comprise an application service as configuration items (CIs).

Service Mapping uses patterns to discover and map CIs. A pattern is a sequence of commands whose purpose it is to detect attributes of a CI and its outbound connections. A typical Service Mapping pattern consists of two types of algorithms for identifying CIs and finding CI connections.

The starting point of any discovery process is an entry point. An entry point is a point where clients access an application service. For example, to map your electronic mailing application service, define an IP address or host name of the email server as an entry point. The discovery and mapping process begins from Discovery performing the horizontal discovery to identify the host. Once the host discovery is complete, Service Mapping starts the top-down discovery to find and map applications running on this host.

Service Mapping uses MID Servers to communicate with CIs in your organization. MID Servers are located inside your organization network and Service Mapping can communicate with them without traversing firewalls.

Note: Currently, pattern operations do not support multi-languages. If values returned from pattern operations are not in English, the returned data cannot be parsed properly and the pattern discovery will fail.

The discovery and mapping process consists of the following interactions:

1. An administrator defines an application service with an entry point for an application CI.
   Service Mapping creates a record for the new application service in the Mapped Application Service [cmdb_ci_service_discovered] table.

2. The device hosting the application is identified.

   a. Service Mapping checks if the device hosting this application CI exists in the CMDB.

   b. If the device hosting this application CI does not exist, Service Mapping triggers Discovery to detect host.

   c. Discovery creates the first set of probes for port discovery, referred to as Shazzam probes, and places them as a discovery request in the External Communication Channel (ECC) queue.

   d. The MID Server checks the ECC queue and retrieves the discovery request assigned to it.

   e. The MID Server runs the probes against the host and discovers open ports.

   f. The MID Server passes information on the host ports to the ECC queue.

   g. Discovery checks the ECC queue and receives information on the host ports.

   h. These steps are repeated for other types of probes: classification, identification, and exploration.

i. Discovery adds the host to the CMDB.

j. During the host discovery using probes, Service Mapping checks the ECC queue if this process is complete. When the host discovery is complete, Service Mapping checks whether this host exists in the CMDB.

Note: For the detailed description of the horizontal discovery flow, refer to Horizontal discovery process flow with probes and sensors.

3. Once the host is found in the CMDB, Service Mapping discovers the application running on this host.

a. Service Mapping creates an application discovery request for the IP address of the entry point. It then writes the request in the ECC queue and assigns a MID Server to the request.

b. The MID Server checks the ECC queue and retrieves the discovery request assigned to it.

c. The MID Server starts running identification sections of the patterns associated with the classifier to find the match for the entry point. When the identification section matches the entry point, the pattern discovers a CI.


d. The MID Server starts running connectivity sections of the pattern to find outgoing connections of the newly discovered CI.

e. The MID Server passes information on the discovered CI, its attributes, and connections to the ECC queue.

f. Service Mapping checks the ECC queue and receives information on the newly discovered CI.
Whenever Service Mapping checks the ECC queue and receives information on a discovered CI, it checks these tables for any data on outbound connections related to the CI: the cmdb_tcp and sa_flow_connection tables. If these two tables contain unique data that patterns did not discover, Service Mapping enriches the information about the CI connections and adds them to the map.

g. Service Mapping writes the information into the CMDB and adds this CI to the application service map.
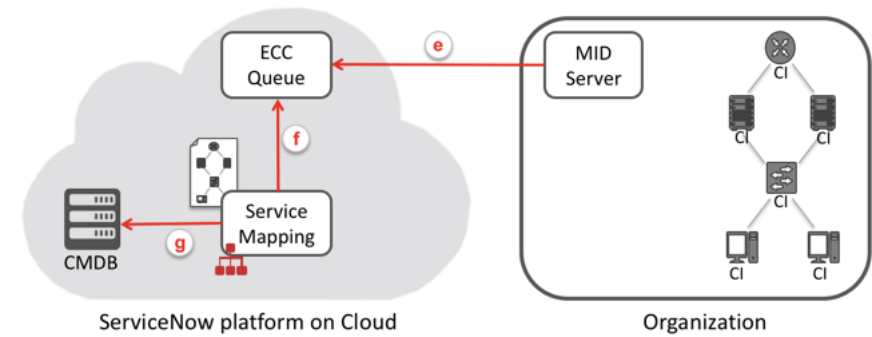
h. Service Mapping creates the discovery requests for all applications to which the newly discovered CI connects. Mapping is complete after Service Mapping maps a CI that either does not have any outbound connections or is marked as a boundary. A boundary makes Service Mapping stop discovery from this point and not follow outgoing connections.

4. The system regularly runs the service recomputation to query the CMDB for the latest CI changes, add data for network and storage paths, and apply CI impact rules.

Previous

‹ Discovery based on Predictive Intelligence

Next

Tag-based discovery in Service Mapping ›