ServiceNow Discovery

Benefits

Accelerate Time to Value

Rapidly configure and launch secure, agentless discovery of hardware, software, virtual and cloud resources, and their relationships.

Enable Service Impact Analysis

Seamlessly integrates with ServiceNow Service Mapping to facilitate quicker service restoration from incidents, more effective root cause analysis, proactive problem resolution, lower-risk change execution, and better-informed business decisions.

Extend Discovery throughout IT Infrastructure

Create custom patterns without coding for any discoverable resource; identify custom applications and their dependencies; customize CMDB fields, tables, and relationship descriptions; and federate with other data sources through integrations.

The IT Challenge

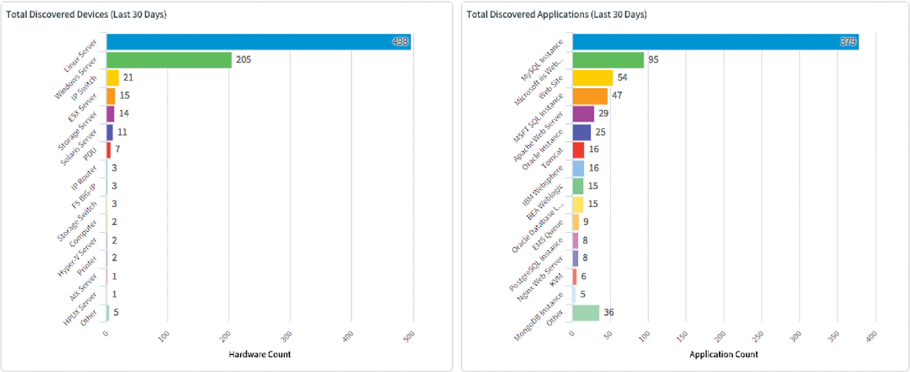
IT organizations rely on the Configuration Management Database (CMDB) to manage infrastructure changes and diagnose problems. But many CMDBs struggle to remain current and do not contain the right type of information to drive processes effectively. As a result, IT staff cannot determine which business services are affected by changes, failures, or performance issues—nor can they easily determine root causes when a business service experiences problems.

Without a repeatable and reliable method to find and identify devices and applications in an enterprise IT infrastructure, it is impossible to capture and maintain an accurate and up-to-date inventory with which to map relationships and dependencies. This poses a significant risk to service stability and can lead to financial waste, such as paying unnecessary hardware maintenance fees and incurring software compliance penalties.

The ServiceNow Solution

ServiceNow Discovery provides IT with visibility into IT infrastructure and its changes. Specifically, Discovery uses agentless technology to discover physical and virtual devices such as laptops, desktops, servers (physical and virtual), switches, routers, storage, and applications, as well as the dependent relationships between them–both on premises and in public clouds like Amazon Web Services and Microsoft Azure. It thereby keeps the ServiceNow Configuration Management Database (CMDB) current. A guided setup enables IT to configure and launch Discovery in minutes by following simple steps. Discovery then identifies the applications that are running on computers and maps dependencies, such as an application on one server that uses a database on another server.

Discovery runs on an on-demand or scheduled basis to help ensure the accuracy of the configuration item (CI) data underpinning ServiceNow applications across the enterprise. IT can create custom patterns to explore any IP-enabled device and can use simple process classifiers to discover running processes. ServiceNow also easily integrates with third-party applications and data sources to collect additional configuration information. When paired with ServiceNow Service Mapping, Discovery provides the infrastructure inventory and relationship information for automated service maps. With Discovery, IT benefits from quicker service restoration from incidents, more effective root cause analysis, proactive problem resolution, lower-risk change execution, and ultimately better-informed business decisions.



Dashboard shows progress of secure, agentless discovery of infrastructure devices and applications

Secure, Agentless Architecture

Discovery is agentless—it avoids the management complexity of having permanent software installed on any computer or device to be discovered. A lightweight Java application called Management, Instrumentation, and Discovery (MID) Server runs as a Windows service or UNIX daemon on standard hardware—including virtual machines already in a customer environment to facilitate communications. Multiple MID Servers, capable of handling thousands of devices each, can be deployed in different network segments to provide virtually unlimited scalability.

The MID Server executes probes and patterns and returns results back to an associated ServiceNow instance for processing; it does not retain any information. It communicates by querying its associated instance for probes and patterns to run and then posts the results back to the instance. Within the instance, sensors process data collected by the probes and patterns.

The MID Server uses HTTPS to ensure all communications are secure and initiated inside the enterprise's firewall. No special firewall rules or VPNs are required. Configuration of IP ranges, credentials, and schedules are all handled in ServiceNow. Credentials are stored using 3DES encryption or optionally can be provided by an external credential store. Once entered, ServiceNow has no way of ever displaying them again. On the MID Server, the standard encryption capabilities of SSH, WMI/WinRM, and Simple Network Management Protocol (SNMP) are used.

Probes, Sensors, and Patterns

The MID Server uses several techniques to probe computers and IP-enabled devices without using agents. For example, it uses SSH to connect to a Unix or Linux computer and runs standard commands to gather information. Similarly, it uses SNMP to gather information from a network switch or a printer. WMI and PowerShell are used for Windows computers and there is support for WinRM as well. Storage components are discovered via SMI-S and CIM. RESTful HTTP queries are initiated as well for supported targets such as UCS and AWS. Discovered information is securely sent back to an associated ServiceNow instance for processing by the probe's matching sensors. Patterns-based content is handled by a generic pair of probe and sensor.

Application Dependency Mapping

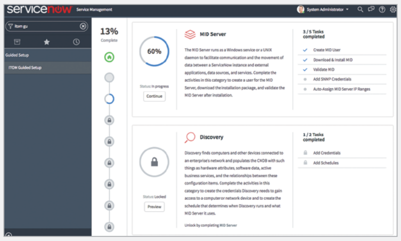
Discovery maps hierarchical dependencies and assigns the appropriate relationship type between CIs that it finds. Application dependency mapping creates upstream and downstream relationships between interdependent applications by identifying which devices are communicating with one another, which TCP ports they are communicating on, and which processes are running on these devices. All this information is used to automatically keep the ServiceNow CMDB up to date.

Discovery uses identifiers to search the CMDB for CIs that match devices discovered in the network. These identifiers can be configured to instruct Discovery to take certain actions when device matches are made, or not made, to maintain data integrity.

When IT uses VMware, AWS, or Microsoft Azure to make changes to their virtual or cloud environments, events from these environments trigger Discovery to detect those changes and then update the CIs and corresponding relationships. This ensures up-to-date accuracy of the CMDB and real-time visibility into virtual and cloud environments.

Customization and Integrations

IT can create custom patterns to explore any discoverable resource. Using pattern designer, IT can expand discoverable elements using a codeless engine. IT can also customize data model fields, tables, and relationship descriptions in the CMDB to meet specific needs. ServiceNow also integrates with many third-party applications, including industry-standard Privileged Access Management solutions, and data sources to collect additional information.

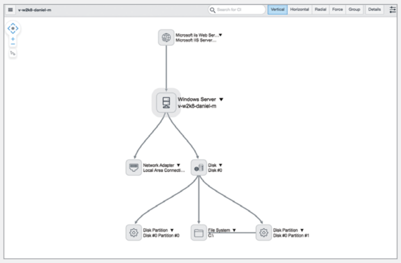


The MID Server runs as a Windows service or a UNIX daemon to facilitate communication and the movement of data between a ServiceNow instance and external applications, data sources, and services. Complete the activities in this category to create a user for the MID Server, download the installation package, and validate the MID Server after installation.

Discovery finds computers and other devices connected to an enterprise's network and populates the CMDB with such things as hardware attributes, software data, active business services, and the relationships between these configuration items. Complete the activities in this category to create the credentials Discovery needs to gain access to a computer or network device and to create the schedule that determines when Discovery runs and what MID Server it uses.

Unlock by completing MID Server

Guided setup makes it easy
to configure and launch Discovery



CI relationships are mapped
automatically for clear visualization

Quick and Easy Setup

A guided setup provides a logical, user-friendly starting point to configure and launch Discovery. IT can follow simple steps to deploy a MID Server, add credentials, and create a schedule, and then complete the process by launching Discovery.

Unified Discovery of Hybrid Infrastructure and Services

Discovery is tightly integrated with ServiceNow Service Mapping to form a unified collection architecture on the ServiceNow platform for discovering enterprise hybrid infrastructure and services. ServiceNow Discovery provides a comprehensive inventory of physical and logical assets within the IT infrastructure. These CIs and relationships are populated into the ServiceNow CMDB. Service Mapping then uncovers the hybrid infrastructure underlying business services and connects these CIs to form individual service maps. IT staff can drill down seamlessly from service maps into detailed asset information, which provides a powerful, integrated environment for resolving service issues and managing service changes.