ServiceNow Discovery

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 IT 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 reliable method to identify IT resources in a dynamic enterprise, it is impossible to keep track of changes occurring in on-premise, multi-cloud, and serverless infrastructure like Kubernetes. This poses a significant risk to service stability and can lead to financial waste, such as paying unnecessary hardware maintenance fees, incurring software compliance penalties, an inability to pinpoint disruptions.

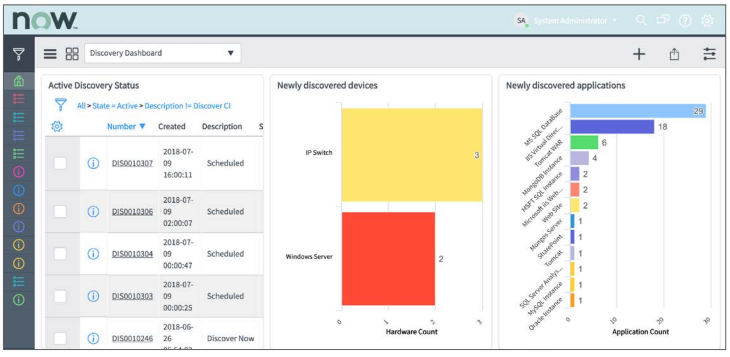
The ServiceNow solution

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 also discovers Kubernetes clusters deployed in cloud, or in on premise environments. It thereby keeps the ServiceNow® Configuration Management Database (CMDB) current as changes occur at a continuous basis.

A guided setup enables IT to configure and launch Discovery in minutes by following simple steps. Once Discovery is set up, it identifies the applications, cloud resources, container clusters, routers, servers (physical and virtual), switches, etc. Discovery also creates dependency views depicting how IT resources relate to one another. It provides a robust mechanism for change management, enabling change requestors to validate modification to Configuration Items (CIs) and update the CMDB.

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 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 IT resource inventory and relationship data for automated service maps. The value to IT is faster service restoration from incidents, more effective root cause analysis, proactive problem resolution, lower-risk change execution, and ultimately, better-informed business decisions.



Discovery Dashboard makes it easy to analyze all IT resources

Benefits

Accelerate time to value

Rapidly configure and launch a secure, agentless discovery of hardware, software, serverless infrastructure, virtual plus 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 incident prevention, lower-risk change execution, and better-informed business decisions.

Extend discovery throughout IT infrastructure

Use out of the box patterns, or customize your own for any discoverable on-premise, cloud, or serverless infrastructure and container orchestration engine like kubernetes, AWS Lambda, and Azure functions.

Improve efficiency in the change process

Change management comes integrated with Discovery to ensure CI changes are accurate and updated in CMDB.

Secure, agentless architecture

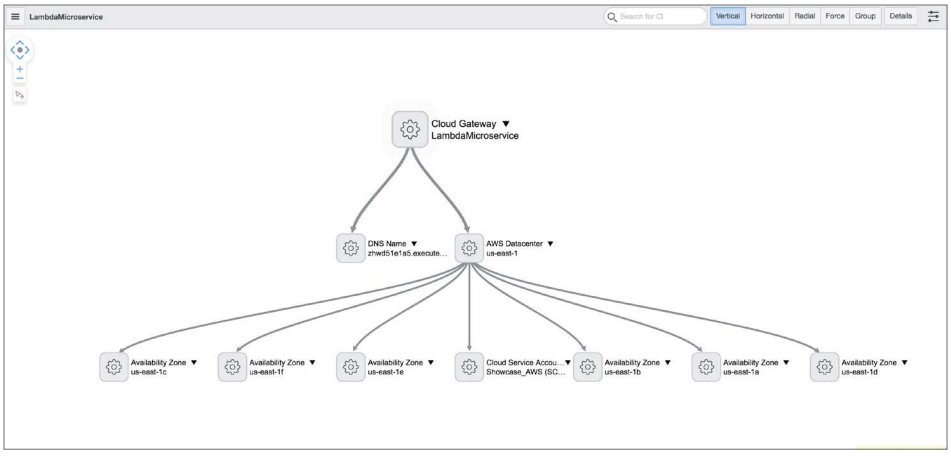
Discovery is agentless—it avoids the management complexity of having permanent software installed on any computer, or device to be discovered. A lightweight Java application called Management, Instrumentation and Discovery (MID) Server runs as a Windows service or UNIX daemon on standard hardware—including virtual machines already in a customer environment to facilitate communication. 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.

The MID Server uses HTTPS to ensure all communications are secure and initiated inside the enterprise's firewall. Discovery provides a quick-start mechanism to populate IP subnets and ranges. Discovery uses that information to stagger jobs by location. This provides more flexibility and robustness to the IT discovery process. Credentials are stored using 3DES encryption or 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 discover 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 APIs are used to discover cloud and container environments. Discovered information is securely sent back to an associated ServiceNow instance for processing by the probe's matching sensors.



Dependency view helps analyze IT resource relationships

Dependency views

Discovery maps hierarchical dependencies and assigns the appropriate relationship type between CIs that it finds. Application dependency mapping (ADM) 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 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

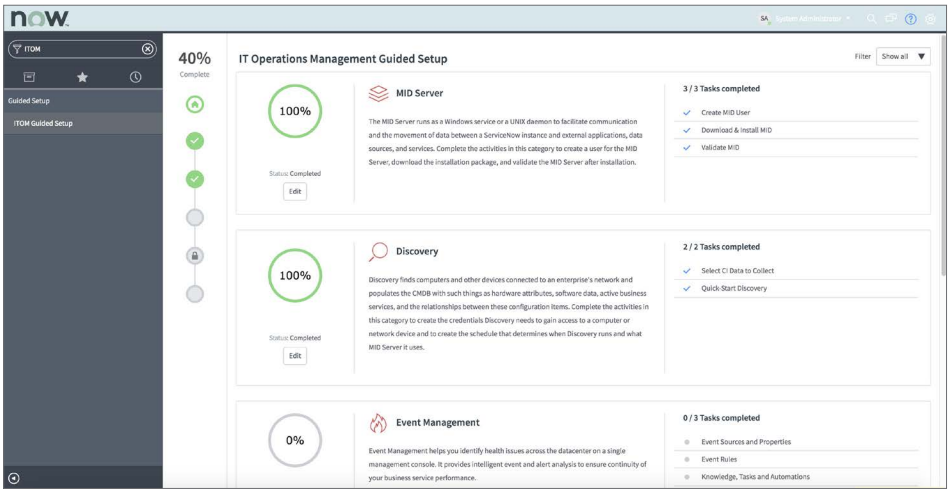
IT can create custom patterns to explore any discoverable resource. Using pattern designer, IT can expand discoverable elements using a codeless engine. IT can also customize data model fields, tables, and relationship descriptions in the CMDB. ServiceNow also integrates with many third-party applications, including industry-standard Privileged Access Management (PAM) solutions such as CyberArk®, BeyondTrust®, and other available via the ServiceNow store. This allows security admins to provide least privileged access and rotate credential updates per their policy with ease.

Quick and easy setup

A guided setup provides a starting point to configure and launch Discovery. IT can follow simple steps to deploy a MID Server, add credentials, and automatically create a schedule based on discovered subnets, a user defined window, and then complete the process by launching Discovery.

Unified discovering of hybrid infrastructure and services

ServiceNow Discovery is tightly integrated with ServiceNow Service Mapping to form a unified collection architecture on the Now Platform™ for discovering enterprise hybrid environments, serverless infrastructure like Kubernetes, and services. All of this data is kept in sync with the CMDB.



Guided set up makes it easy to configure and launch Discovery

servicenow