

Populate and maintain your CMDB with ServiceNow Discovery

Gain deep infrastructure visibility with reliable data from ServiceNow Discovery

What's in this Success Playbook

This Success Playbook will show you how to set up [ServiceNow® Discovery](#) in a way that keeps your CMDB current and reliable. You'll learn:

- How to create comprehensive goals and get agreement from stakeholders for your implementation of Discovery
- How to implement Management, Instrumentation, and Discovery (MID) servers
- How to establish a credentials strategy and schedules
- How to use patterns to reduce the work needed to run Discovery across new (e.g., serverless) environments

With so much of the modern enterprise powered by IT, visibility into IT infrastructure is mission critical. But as IT infrastructure continues to grow and become more complex due to multi-cloud environments, serverless compute, and containerization, visibility means tracking a moving target. For IT to gain visibility, it faces the challenge of consolidating, maintaining, and understanding complex configuration data.

This means you need an updated configuration management database (CMDB) at all times. Many organizations fail to keep their CMDB current due to the lack of an automated process that discovers infrastructure and applications. Yet, when implementing more automated discovery processes, IT operations groups often fail to establish clear expectations with network, server, security, CMDB, and other groups. This leads to project delays.

A solid configuration management plan will help keep your CMDB healthy—and give you a solid foundation for implementing automated discovery. To set up an effective configuration management plan, see our Success Playbook on [planning your successful CMDB deployment](#).

Key takeaways

The most important things to know

Discovery is a continuous process that can support both your CMDB and effective service mapping. As with your CMDB, your Discovery project should begin with a clear definition of your goals and use cases to ensure focus.

The payoff of getting this right

Your CMDB will be populated with reliable data, giving you complete visibility into your infrastructure. With this visibility, you can improve speed of incident resolution and gain critical, early visibility into the health of your business services.

What you need to get started

Leadership support

- A designated IT admin overseeing the discovery process

Prerequisites

- An intermediate understanding of Windows/Unix/Linux system administration
- A basic to intermediate grasp of networking principals, like IP routing and how to deploy and use primary network analysis tools
- Knowledge of configuration management methodology
- A [ServiceNow ITOM Visibility](#) license – Since our New York release, Discovery (along with Service Mapping) is a feature of the ITOM Visibility product.
- An understanding of configuration management plans

Playbook overview

Follow these four stages to achieve complete visibility into your infrastructure when you have reliable data in your CMDB:

Stage 1 – Set up the goals and strategy

Stage 2 – Configure and deploy MID Servers

Stage 3 – Create a robust credentials strategy

Stage 4 – Automate Discovery with schedules

Terms and definitions

MID Server – Each [MID Server](#) is a lightweight Java process that can run on a Linux, Unix, or Windows server. During discovery, the MID Server executes probes and patterns, and returns the results back to the instance for processing. It doesn't retain any information.

Probes and sensors – Probes and sensors are scripts that collect data on the host, process it, and update the CMDB. Several probes and sensors are provided out of the box. You can also customize them or create your own.

Patterns – These are a series of operations that also collect data on a host, process it, and update the CMDB. Patterns differ from probes and sensors in that they are written in Neebula Discovery Language (NDL) rather than JavaScript. You use them during the last two phases of discovery. Discovery comes with default patterns out of the box, but you can customize them, create new ones using the pattern designer, or access patterns from the ServiceNow Store.

Stage 1 – Set up the goals and strategy

Make a compelling case for a better discovery process and communicate how you'll get there.

KEY INSIGHTS

- Document your company's business goals and highlight how discovery helps achieve with them.
- Get stakeholder buy-in before deployment.
- Break down your implementation strategy into six steps.

Discovery is a continuous process. You need a strategy to manage it effectively. Before you begin, have a solid configuration management plan that protects the CMDB against unnecessary changes, provides governance, and integrates with key business processes, such as incident management, change management, and security. To set up a great configuration management plan, see our Success Playbook on [planning your successful CMDB deployment](#).

BUSINESS GOAL	OPERATIONAL NEED	HOW DOES DISCOVERY HELP?
Reducing data center outages	Greater insights into how infrastructure and applications are connected. Learn about business service relationships.	Discover network, virtualization, storage, and core software relationships, such as apps hosted on servers. ServiceNow Service Mapping will monitor business service changes and their dependencies on systems and applications.
Strengthen security strategy	Track and monitor growing infrastructure and dependencies. Pinpoint where breaches might happen.	Discover and maintain all configuration items (CI) as a result of growing infrastructure, applications, software, and traffic patterns. Keep them updated in the CMDB.
Cloud-first strategy	Monitor changing cloud models and services. Discover shadow IT.	Discover and maintain cloud configurations. Monitor shadow IT spinups and bring them into compliance with corporate policy.

Table 1: Key business goals and how Discovery helps to support them

Get started with your discovery project by establishing goals and defining their outcomes. Focusing on the most important business needs first, drive goals with use cases and business problems. For instance, some ServiceNow Discovery customers, such as [Kimberly-Clark](#) and [Oak Ridge National Laboratories](#), focused their efforts on the security goal of responding to future threats faster.

Discovery provides them with a way to account for all devices, applications, and services within their rapidly growing infrastructure.

Get buy-in from stakeholders

Your discovery project should have buy-in and input from the following stakeholders:

- **Server group** – Make sure they understand how ServiceNow Discovery accesses servers (including cloud-based servers) and finds software running on them.
- **Security group** – Expect them to dictate where credentials are stored and to provide role-based access to maintain patterns. You need to inform them of MID Server locations on the network.
- **Network group** – Make them aware of the network traffic impacts of discovery patterns and probes. Consult them to learn more about network zones, firewalls, switches, and other devices delivering core business services.
- **Business and technical staff** – Communicate that automated discovery requires support from teams that own devices and applications. Let them know that the device or application owner must remediate issues arising as a result of discovery.
- **Project sponsor/executive** – Communicate the scope and timeline for the project.
- **Configuration management team/CMDB administrator** – Align with your configuration management team if it's different than your discovery team. See our Success Playbook on [planning your successful CMDB deployment](#) to identify their roles and responsibilities. They approve changes to CMDB.

Unless there's a compelling business reason for customization, get stakeholders to agree to use the out-of-the-box schema and configuration. Set ServiceNow Discovery as the primary source of truth for all discoverable configuration data. Then, use reconciliation rules to ingest platform data to enrich discovered CIs with additional business information. For example, you should add financial data after performing discovery and reconciling discovery with the CMDB.

Look to your infrastructure and geographical footprint to help guide your discovery strategy, keeping compliance and auditing requirements in view. To avoid issues down the road, consult with your compliance and security teams early. For example, one ServiceNow Discovery customer aligns its ServiceNow instance with PCI audit requirements. This created more work for its discovery team but kept processes in step with business needs.

Implement ServiceNow Discovery in six steps

Plan to assign a minimum two-person team to run ServiceNow Discovery, especially if you have a medium to large network (over 10,000 devices). They should have visibility to the CMDB management team that governs CI change process or, at a minimum, have clear lines of communication with CI owners. Depending on your organization, ServiceNow Discovery will require ongoing configuration and extension to find software products that aren't supported out of the box.

STEP	GOAL	OBJECTIVE	STAKEHOLDERS
Step 1	Architect Discovery	Outline the overall architecture of your MID Server placement, network, and security requirements. Define the scan schedule. Determine all network zones, when zones should be scanned, and stagger schedules appropriately.	Consult with and get buy-in from CMDB, network, security, and server teams.
Step 2	Pilot Discovery	Select a small network footprint to discover in the pilot phase. For instance, pick one device of each type or select a small region.	Engage network admins and security monitoring teams to reduce impact to the network. Test against types of devices that you consider to be old, unreliable, or susceptible to failure if scanned.
Step 3	Review results and remediate	Review results from the initial discovery, paying attention to any missing, inaccurate, and duplicate data in the CMDB. Establish a process for identifying, classifying, distributing, and remediating discovery failures. Send to appropriate support teams for action.	Distribute responsibility for review and remediation across your CMDB, network, security, and groups.
Step 4	Extend out-of-the-box patterns	Extend out-of-the-box patterns for your own applications and products. Ask: Do these applications require new CI classes or will existing ones suffice? Most of the time, you won't need a new class.	Engage your CMDB and CI class owners.
Step 5	Production build-out	Expand discovery to the production environment. Take small steps, such as starting in one region and expanding to others.	Update and communicate progress to stakeholders and get their help where needed.
Step 6	Service relationship mapping	Map service relationships and dependencies to applications and devices. Undertake this advanced step, which requires the Service Mapping application, after you've performed infrastructure discovery.	Involve business application and services owners with detailed knowledge of business services in this more complex step.

Table 2: Six steps to plan your Discovery project

Based on prior deployments, 98% of customers are satisfied with the out-of-the-box (OOTB) capabilities of ServiceNow Discovery to support a large number of devices, applications, and services. To streamline your efforts, start with OOTB patterns, probes, and built-in APIs, limiting customization except where needed. Consult this list to see the [data collected by Discovery](#) before you customize.

For example, customers discover these OOTB elements to use without customization:

- Both physical and virtual servers with over 20 attributes and related record types
- Standard network devices including routers, switches, and load balancers
- 24 OOTB application profiles, including MS SQL, Oracle, and Tomcat
- Software installed with MSI (Windows), pkgadd (Solaris), and RPM (Linux)
- Application-to-application dependency mapping
- Logical network-to-server IP relationships
- Virtual machines, availability zones, and cloud networks and subnets in Amazon Web Services and Microsoft Azure clouds
- Operating system-level virtualization, including containers, engines, images, and tags

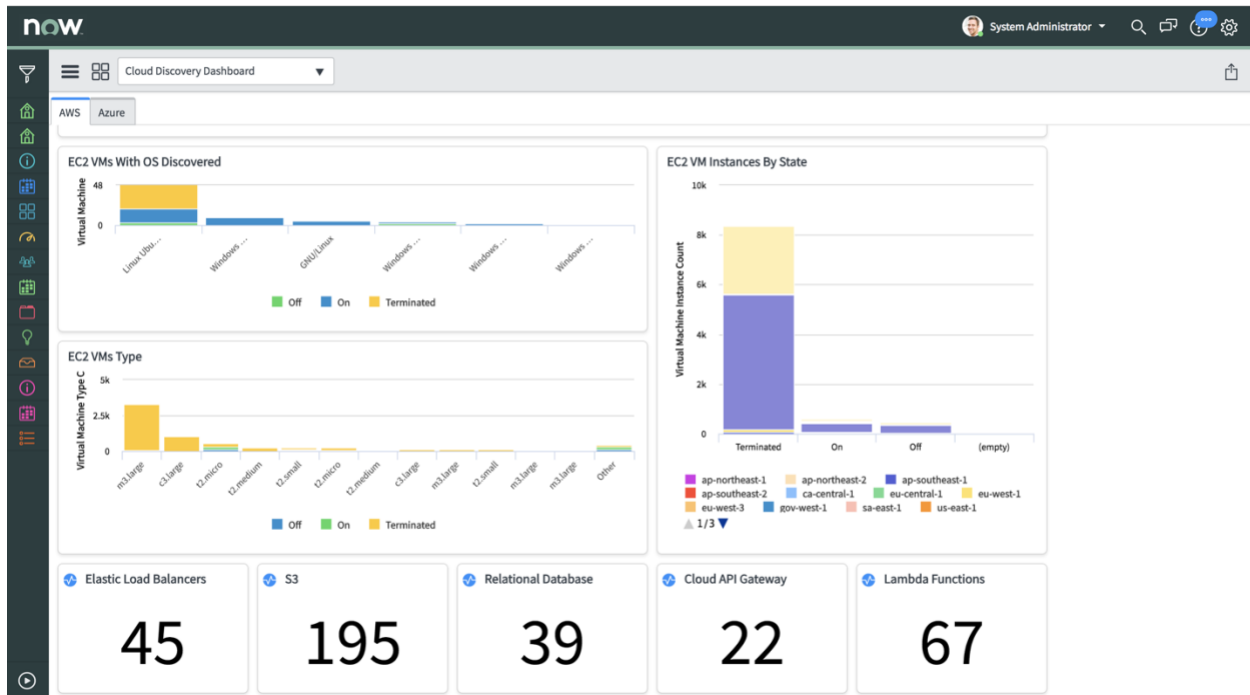


Figure 1: The Discovery dashboard shows the progress of discovered infrastructure and monitors issues

Commonly used networking protocols

ServiceNow customers typically use the following networking protocols to communicate throughout the discovery process:

- Domain Name Server/Windows Internet Name Service (DNS/WINS) for resolving IP address connectivity
- Simple Network Management Protocol (SNMP) for network, printers, and powering devices
- Secure Shell (SSH) for Unix based computers
- Windows Management Instrumentation (WMI) for Windows systems, including Windows PowerShell
- Common Information Model (CIM/SMI-S) for storage servers
- Cloud-enabled APIs for Amazon Web Services (AWS), Microsoft Azure, and VMware vSphere

EXPERT TIP

Set up discovery goals and get stakeholder buy-in before kickoff to speed up the project implementation.

Stage 2 – Configure and deploy MID Servers

Configure and monitor your MID Servers properly for an effective discovery process.

KEY INSIGHTS

- Determine the size of your enterprise network.
- Place your MID Servers at the right locations with appropriate compute configurations.
- Monitor performance of your MID Servers continuously.

An effective discovery process relies on a proper configuration of the MID Server. The MID Server acts as a proxy that interrogates your network assets and reports results back to the CMDB. Before you start using ServiceNow Discovery, make sure MID Server is set up correctly by following the guidelines below. The ServiceNow product documentation includes [additional configuration guidelines](#).

First size your Discovery deployment

Based on your environment, determine how many MID Servers and probes you need to run. This depends on:

- **Number of targets** – How large is the network you plan to discover, and how often do you want to discover devices and applications?
- **Geographic split** – How extensive is your geographical footprint? You should have MID Servers at the continent level with a global deployment.
- **Security** – How many security zones and network firewalls will MID Servers have to traverse?

You can use [this tool](#) to calculate the number of MID Servers and probes needed for your environment.

ServiceNow Discovery customers are often concerned about impacts on network traffic and operational devices along with how long it takes to finish discovery. Here's how you can address these concerns:

1. Place your MID Servers close to the targets that you plan to discover. By keeping your MID Servers close to targets, you get the most out of local resources.
2. When utilizing multiple MID Servers, keep them on their own dedicated virtual hosts within each environment. If you're using Windows-based discovery, make sure you use a supported version of Windows to host the MID Server.
3. Increase the number of threads in the MID Server if you need more patterns and probes. Our customers often increase OOTB threads in Discovery, which ships with 25 to 50—or even as many as 100—to enhance performance.

4. Increase the memory from 1024 MB to a level appropriate for your environment. This allows the MID Server to allocate itself more memory resources from the host. You can do this in conjunction with increasing the number of threads. Use these sizing guidelines.
5. Open the required firewall ports from the MID Server to the target devices.

You might be running multiple probes per device in a varied frequency. For instance, you might want to complete a discovery job within six hours. Here's how you can accomplish this:

	OLD CONFIGURATION	NEW CONFIGURATION
Devices	2,500	2,500
Probes (7 probes per device)	17,500	17,500
MID Server	1	1
Threads	25	50
Time to complete the job	11 hours	<6 hours

Table 3: Changing the MID Server configuration to finish the job in under six hours

Increasing the number of threads to 50 gets the job done under six hours. If you have a very large network, create multiple overlapping schedules for different parts of the network. See Stage 4 for more detail on this. Some large customers scan their business-critical network on a daily basis while performing weekly discovery on less critical devices and applications.

Monitoring the MID Server keeps you ahead of performance issues

In order to get most out of your MID Server, monitor its performance. The Now Platform™ provides performance metrics for both host and CPU utilization taken at 10-minute intervals. As you run Discovery, you increase memory utilization. And as you run more probes, the MID Server will use more host resources. If you have a large network, monitor performance metrics regularly to ensure Discovery jobs run smoothly.

EXPERT TIP

For optimal MID Server performance, keep host utilization at 80%. If you exceed 80% host utilization, your discovery schedules might not complete within your desired timeframe.

Stage 3 – Create a robust credentials strategy

Get buy-in on your strategy from network, security, and other teams to stay on track.

KEY INSIGHTS

- Align your credentials strategy with network and security teams to avoid project delays.
- Use credential-less discovery to get basic configuration data about devices and apps.
- Run a full discovery to complete the CMDB update process.
- Create a credentials ordering mechanism to speed up the discovery process.

Without working credentials, your Discovery implementation project could fail or see delays. The good news is that the agentless mechanism of Discovery means that you don't have to install agents on every device. But you still need to administrator access via username and password, so set appropriate expectations with network and security teams.

Want a proven credentials management strategy? Consider these two options:

1. Use the internal encrypted table stored in the ServiceNow instance. With this strategy, it's easier for you to keep a credential table updated when there's a change in device credentials.
2. Use the local security vault that you're already using. ServiceNow has OOTB integration with CyberArk. Consult your security team for other credentials management vaults. You can easily integrate these vaults with ServiceNow Discovery. Read the product documentation about using [CyberArk for your credentials storage](#).

In order to gather data, you need to know the protocols used to scan for credentials. Here's a list of the most common protocols to get you started:

- Windows Management Instrumentation (WMI) – You need a domain user that has local administrator privileges on the targets you want to discover. Keep in mind that if you're using Microsoft User Access Control, non-domain and non-admin users won't be able to access the targets remotely. Typically, this step takes longer since Windows access requires full credentials. Prioritize this task early by working with your network, security, and server teams. Note that this may take little bit longer than Secure Shell (SSH) and Simple Network Management Protocol (SNMP) setup.
- Secure Shell (SSH) – For Unix/Linux targets, you need a standard SSH user or private key (with an optional pass phrase) to connect to these systems. ServiceNow Discovery has defined unique commands that run as “sudo nopasswd” to extract all required operational and configuration data. Read the product documentation page for more details on [managing Unix and Linux credentials](#).

- **Simple Network Management Protocol (SNMP)** – You need to get the read-only string for your network-based devices such as routers, switches, and printers. Whitelist MID Servers in the routers and switches access control lists (ACLs). You may also need local shell access for some load balancers to capture configuration data.
- **VMWare** – You need read-only user access that will query the vCenter API when running as a process or as a discovered vCenter appliance.
- **Storage** – You need full administrator user access to the storage agent (SLP) and the host where it's deployed. Discovery uses CIM credentials to query the provider to explore the storage environment.
- **Cloud** – You need to acquire full credentials to access cloud instances and APIs. This means that you have to reach out to all business units using cloud instances and get credentials before you start the discovery process. Some have a master account that allows access to all cloud instances. If your company has such an account, request access to it.

Read this product documentation page for more information on [credentials and connection information](#).

Good credential ordering can speed up Discovery performance

We recommend that all MID Servers have access to the entire credential table, especially in secured zones. This is important because you likely have multiple credentials for one protocol. With the credential affinity method, Discovery performs targeted scans of the network segments where you know a credential works. Discovery usually tries all of these credentials and, after finding the right one, updates the CI with that information. If credentials stop working, Discovery will go through the process again. For this reason, you avoid unnecessary bottlenecks with access to the entire table.

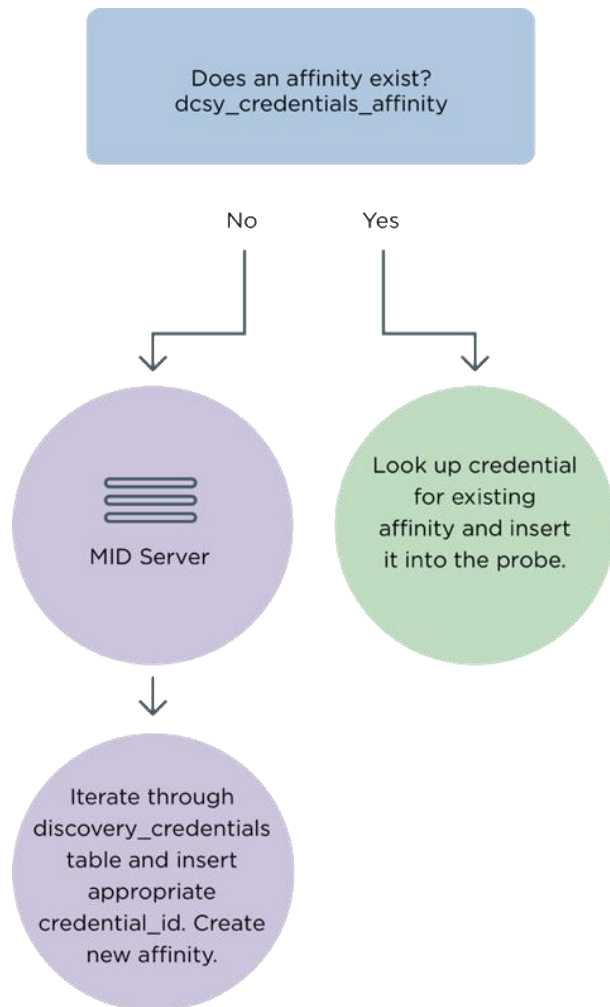


Figure 2: How you automate credential look-up with the affinity method

You can also speed up credential ordering in these two ways:

1. If the table contains 150 SSH credentials and five of those can access 90% of your devices, configure those five with low order numbers, which places them at the top of the execution list. Discovery works faster when trying these common credentials first. After the first successful connection, the system knows which credentials to use the next time for each device.
2. Some organizations have strict log-in security. For instance, access to the Solaris system locks after three failed tries. In this case, you should configure the database credentials with a low order value. This ensures that Discovery tries the database credentials before other device credentials, reducing the risk of lockdown.



Figure 3: ServiceNow Discovery gives you many options for creating a credentials table

Credential-less discovery offers a fast start but gives you limited CI data. You may find that full discovery doesn't work due to authentication failures. You can still collect some basic data with credential-less discovery for some processes, such as applications currently running, IP addresses, and operating systems. ServiceNow Discovery builds a skeleton CI to provide basic visibility when credentials are missing or insufficient. But you still need full access to targets to gather complete CI data. ServiceNow gives precedence to the credentials-based discovery. That means if there's a duplicate record, the CMDB should prioritize the full CI record. Make sure that your security team knows about this approach, since you need to implement an Nmap (network mapper) protocol on the MID Server, which might get flagged by your intrusion prevention systems. Credential-less discovery doesn't work for cloud services—make sure you acquire full credentials beforehand.

Heads up!

Develop a credential strategy with security and network teams early. When you do, you can ensure complete access to discovery targets and reduce project delays.

Stage 4 – Automate Discovery with schedules

Make discovery easy by creating schedules for your infrastructure.

KEY INSIGHTS

- Create schedules that complete in finite time for both on-premises and cloud infrastructure.
- Prioritize scans based on critical business service or geographic needs.
- Use MID Server clusters and behaviors to optimize schedule performance.

To optimize ServiceNow Discovery, set up recurring schedules that complete within your desired timeframe. In order to keep the CMDB current, define schedules for your on-premises and cloud networks by geographic location or IP ranges. Successful completion of your schedules depends on these factors:

- **Size, location, and expected time to scan** – Larger network zones could take considerable time to complete. Schedules that include multiple geographies will also take more time, depending on the availability of the targets.
- **Network link speeds** – Low-bandwidth links can slow discovery.
- **Placement and running of your MID Servers** – You can stagger start times and cluster MID Servers to improve performance. Clustering MID Servers provides you with more resources, failover, and load balancing to ensure that schedules finish on time.
- **Assigning maximum runtime** – This ensures that jobs finish on time or cancel. If network scans don't finish in a finite time, they impact performance by running queues out of capacity. Pay close attention to schedules that don't complete or cancel—you might have to add undiscovered targets manually.

“Our scheduled scans take from one to three hours, depending on the size of the subnet and the device count. The average home page generates more traffic than a ServiceNow Discovery scan.”

– Kimberly-Clark

Use behaviors to focus Discovery schedules

Behaviors are a great way to focus ServiceNow Discovery schedules on a small portion of the network. Using behaviors also limits the chance that you'll populate the CMDB with CIs unnecessarily. The use of specific protocols lets you select the ports to scan in the initial phase of discovery. For example, you can create a schedule to scan for network devices on Sunday afternoon using a specific IP address range. And for this range, you can exclude SNMP but keep all other protocols. Basically, you create a unique schedule that uses specific behavior to populate CIs in your CMDB.

Read this product page for more information on [setting up behaviors](#).

You can also set up WMI scans to select Windows-only servers in the following ways:

Multiple protocols in multiple domains – Configure one MID Server to scan for all protocols on one domain and another MID Server to perform a WMI scan on a second domain.

Devices running two protocols – Some devices have SSH and SNMP protocols running concurrently on one device. Create a behavior to control which of the two protocols is used for the devices. Use the behavior to prevent executing the undesired protocol.

Heads up!

OOTB discovery will attempt to identify devices by testing well-known protocol ports such as 22 for SSH. However, if your organization has changed this port to 2222, then you'll need to update the port configuration settings.

How many schedules do you need?

Let's look at an example of how one ServiceNow customer determined the best way to run schedules.

Locations	100
Devices	8,000
Time window	12 hours
MID Servers	Four with 100 threads and 1.5 GB memory (This customer created a cluster to share resources.)
Schedule	100
Schedule end time achieved	Three hours
Schedule times	7 am (33 schedules), 12 pm (33 schedules), 3 pm (34 schedules)

Table 4: Running 100 schedules in three hours

This customer figured out how to use clusters to stagger their schedules, gaining maximum performance. Instead of running all schedules at the same time, they've assigned proper intervals so, at any given time, all the MID Server resources are being used to run 33 schedules instead of 100. This is a great example of using resources to your advantage while also finishing jobs in a three-hour window.

Using patterns to your advantage when running schedules

The value of running patterns and probes is that you get updated CMDB data by gaining deep visibility into the enterprise infrastructure. Running patterns as frequently as possible helps you add new ways of discovering new infrastructure technologies (like serverless infrastructure) without requiring significant work. Before you run patterns or probes to collect data, make sure you do the following:

- **Identify the value of data** – If data you're collecting isn't supported or used by anyone within your organization and business units, then don't collect it.
- **Avoid duplicate data** – Work with CI owners to ensure that they aren't already collecting hidden fields of data.
- **Use patterns over probes for any new configuration** – If you're writing new rules to discover devices and applications, we recommend using OOTB patterns over probes, to reduce the amount of work needed for discovery. Before you write custom probes, see if there's an equivalent pattern already on the ServiceNow Store. Work with your account team to select, download, and configure the right patterns for your environment. If you need to tweak

patterns, use the extension section instead of identification. Explore additional information about [creating and modifying patterns](#).

- **Don't tweak OOTB patterns and probes** – Instead, create new patterns and probes by copying existing probes. Wait till after the exploration phase of discovery to launch custom probes. This helps prevent overloading your system with useless data. This also helps ensure that you carry custom probes through to the next version during upgrades.
- **Always test your patterns and probes in a development environment** – Always use small tests in the development environment to validate information collected. Don't make changes to the production instance. This lets you test the accuracy of your queries without updating the CI.

Steps to extending OOTB patterns

1. Create a shared library for each application to be discovered

Select an existing CMDB class for your new data, such as an application. Extend to your own class if necessary. Explore [how to create or modify patterns](#).

2. Define a process handler to find your software

This [product documentation page](#) provides more information.

3. Reference the shared library in the pattern to do the discovery work

Read more on this [product documentation page](#).

4. Set up a pattern to build the CI and extract useful information

This [product documentation page](#) tells you more.

EXPERT TIP

Use IP ranges when creating schedules. ServiceNow Discovery automates assigning IP ranges and can be used whenever you run schedules after the initial setup.

The takeaway

To have a healthy infrastructure, you need reliable configuration data in the CMDB. You can maintain reliability of data by managing duplicate CIs and through accurate infrastructure mapping.

Identify duplicate CI records and resolve them with your CMDB

When you run ServiceNow Discovery, you might find duplicate CIs. Discovery finds these CIs and adds them as a deduplication task for you via the identification and reconciliation engine. You should work with CI owners to resolve them. For example, one Discovery customer runs a background script that automatically identifies the duplicate CIs and escalates them to the CMDB owner. Since they have automated the escalation process, they don't have to go through each CI manually. All this data is tracked via the [CMDB dashboard](#), which provides a low-cost means to query the CMDB and visualize the CMDB “health status.”

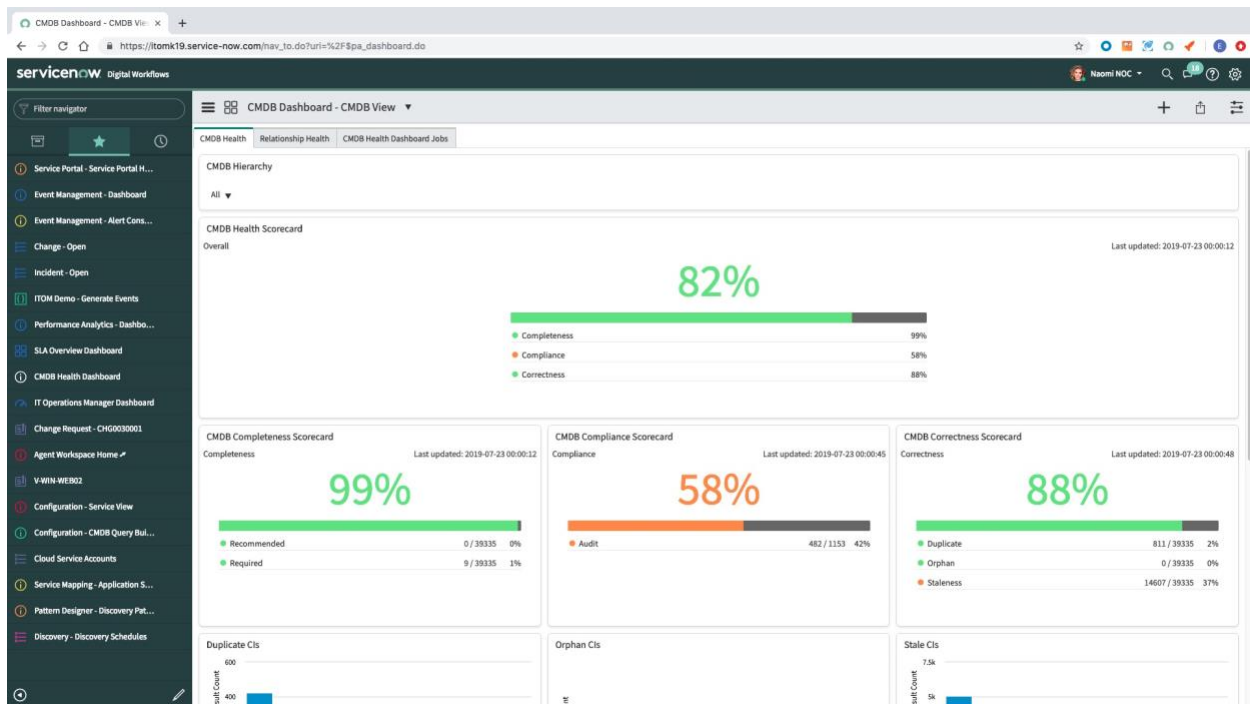


Figure 4: The CMDB dashboard makes it easy to track duplicate CIs and share status with stakeholders

Heads up!

Watch the number of duplicate records showing up in the CMDB.

When the CMDB is manually seeded and the infrastructure targets aren't managed by Discovery, then the CMDB identification and reconciliation process will be unable to reconcile

the data from different sources. We recommend that you match all the CI classes being imported with those found with Discovery when reconciling them. Be sure to review the Discovery identifiers to ensure a match between discovered and imported CI records. That way, Discovery won't return duplicate CIs.

When the Now Platform CMDB is replacing an incumbent CMDB, then the best approach is to upload your legacy CMDB into a user-defined table, and create on-demand scheduled jobs to reconcile what Discovery finds against the legacy CMDB data. This establishes the new CMDB as the source of truth.

Use the Discovery CI schedule manager to access all discovered devices, errors that might occur during discovery, and unidentified IP addresses. The CI schedule manager provides a summary of discoveries triggered from configuration item schedules.

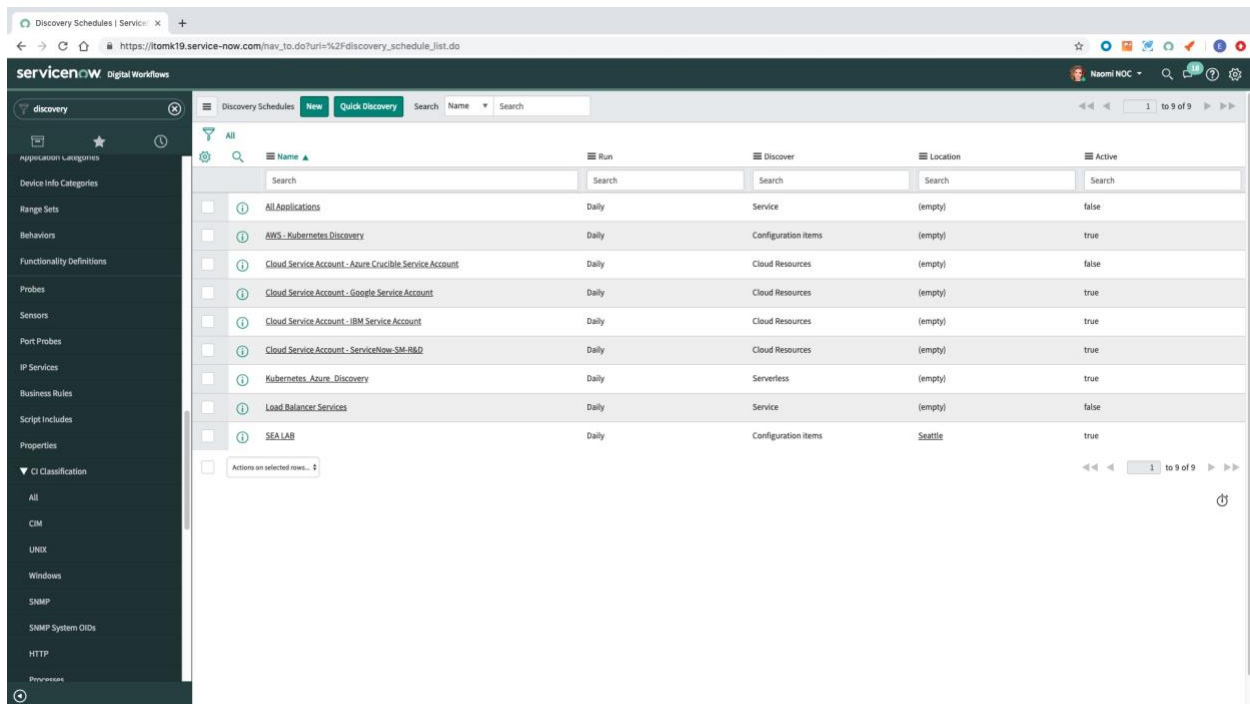


Figure 5: CI schedule manager lets you manage your schedules seamlessly

Reliable dependency mapping gives a complete picture of your infrastructure

Discovery is horizontal data mapping, which means that you find details of each device along with applications and software running on them. We recommend that you enable enhanced application dependency mapping (ADM) to get regular samples of the network traffic to identify applications running on devices. This will let you to find newly added applications on servers.

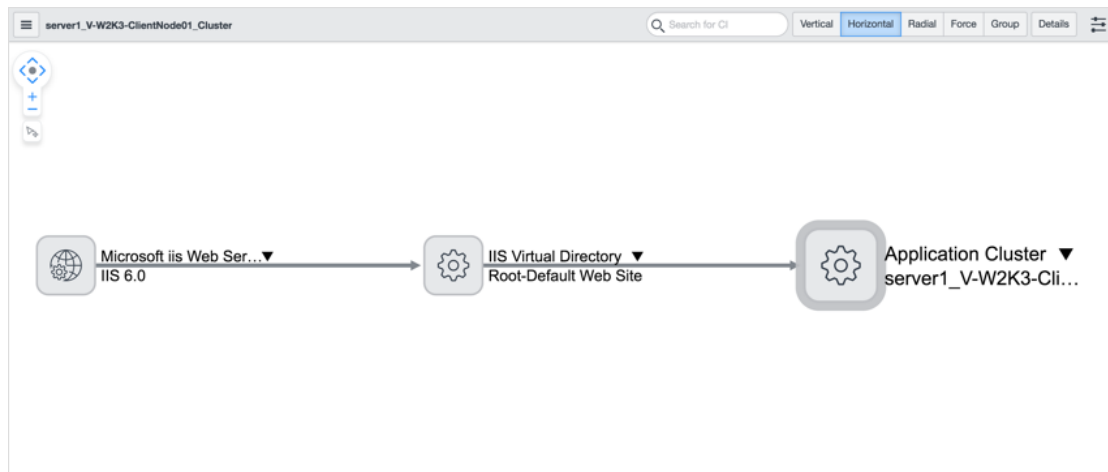


Figure 6: Discovery is a horizontal process that finds all the infrastructure dependencies OOTB

Beyond horizontal discovery, service mapping gives you an additional layer of insights via a top-down discovery approach that also uses ADM. Discovery customers use this approach to find all the relationships and dependencies of applications tied to critical business services. We've found that customers have even better visibility of their infrastructure and a much healthier CMDB with service mapping.

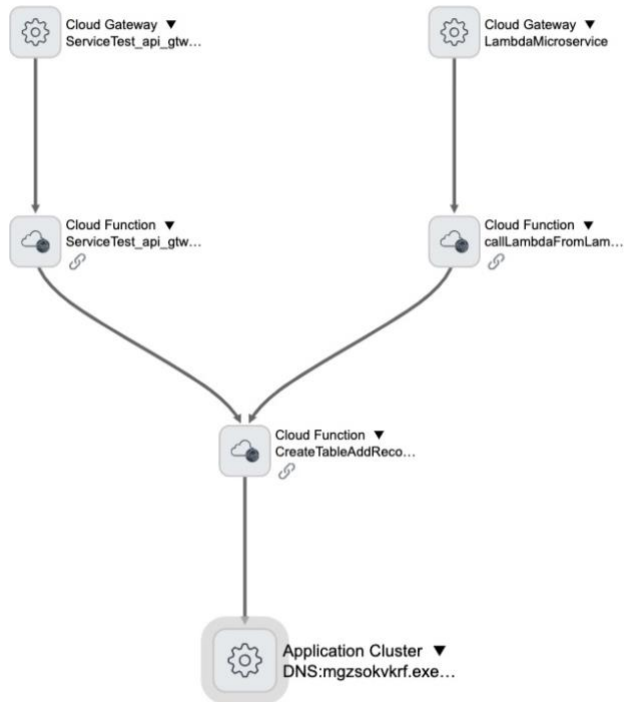


Figure 7: Service mapping gives you infrastructure and service dependencies

A service map builds relationships among infrastructure components, tying critical services to devices and applications.

“Before, if we needed ad hoc enterprise configuration information, it would take more than a day to get reliable information.
Now, that same type of query takes minutes.”

– Oak Ridge National Laboratories

EXPERT TIP

Complete the horizontal discovery of your network before top-down relationship mapping. When you complete the horizontal discovery of your network first, it will give you confidence that you have complete visibility into devices, systems, and applications before you map services.

Appendix

Related resources

- [Discovery best practices](#)
- [Discovery basics](#)
- [Discovery product page](#)