SUCCESS STORY

Now on Now: Creating a global IT ecosystem CMDB with ServiceNow Discovery

Optimizing our CMDB to improve and maintain customer and employee satisfaction with faster incident response and fewer outages while reducing the time to populate CIs by 40%

servicenow™

Table of Contents

Mapping our IT ecosystem to improve incident response and prevention

At ServiceNow, every part of our business relies on our global IT infrastructure: service management, human resources, information security, finance, compliance, and more. Having a map of the connections among the devices, services, applications, and endpoints in our global environment streamlines our workflows and helps ensure uptime for the IT components our employees rely on to conduct their daily work and serve our customers. Delivering consistent and reliable services is critical to improving and maintaining both employee and customer satisfaction.

Realizing the dangers of limited IT infrastructure visibility

When a service or application goes down, our IT Operations team needs to respond immediately. Understanding the problem, and what's causing it, is difficult if the IT Ops team has limited visibility into our entire IT ecosystem.

If individual technical teams are managing portions of the global infrastructure in their own individual offline documents and tribal knowledge that isn't shared, our IT Ops teams' visibility is limited, leading to the inability to pinpoint the root cause of an issue.

That's where the Configuration Management Database (CMDB) comes in.

When properly configured, the CMDB is the digital foundation of a company's enterprise ecosystem. It includes configuration data of the data centers, physical equipment, logical systems, databases, applications, and services so that the IT Operations team can understand the IT environment and interdependencies of digital systems and business applications. From planning upgrades to troubleshooting incidents, the CMDB allows IT Ops to quickly identify any impacted services and engage the correct technical/business owners for a faster resolution.

Without a CMDB, when a problem or service outage occurs, the IT team needs to navigate through multiple documents and contact multiple IT teams to determine what went wrong, potentially increasing response times, wasting staff hours, and delaying resolutions for our customers.

Providing monitoring and response through a unified view of the IT ecosystem

Because the CMDB, which is part of ServiceNow's IT Operations Management (ITOM) solution, is a live database, it represents our complex and changing enterprise environments, allowing our IT Ops team to ensure all the interconnected components are queryable, supportable, and monitorable. It also enables monitoring and event management to ensure critical apps and services are alive, available, and active.

But without the proper tools and processes for populating and maintaining a CMDB, we may face challenging issues such as incorrectly populated configuration item (CI) attributes, compliance risk, and unclear CMDB governance, roles, responsibilities, and access.

To overcome these challenges, we deployed ServiceNow Discovery, a type of automation that simplifies the process of discovering all the IT elements and their connections, saving hours of manual work and coalescing of offline data. Discovery provides complete visibility into our on-premises and cloud resources. Discovery allows us to track changes occurring within our on-premises, cloud, and serverless infrastructure in the CMDB.

CMDB Discovery Challenges

- Critical outages with poor visibility
- Lack of governance, clear ownership, roles, and responsibilities
- Inefficient discovery scheduling leading to incomplete discoveries
- Change Management challenges since Configuration Items were not usable

Creating the CMDB with Discovery

We created our first CIs in the CMDB in 2010. We were a much smaller company then and started with one data center. We gradually expanded the CMDB, progressing to more complex elements: load balancers; vCenter virtual machines and servers; all the regional sites and data centers; new sites and data centers as they became active; and most recently our cloud environments, starting with Azure.

The IT Ops team prescribes which networks, connections, and sites they want to examine and what types of devices they want recorded. Our horizonal and base Discovery schedules run weekly during a region's downtime; some Discovery schedules are configured to run on demand. Service Mapping Discovery schedules also run periodically to update our vertical service maps.

A simple examination of the Discovery error logs indicates what's wrong, what worked, and what didn't so IT Ops can adjust accordingly. After each round of discovery and mapping, we verify with the data owners that Discovery is finding all their critical systems, apps, and services—and when the results are not complete, we modify Discovery to fix our CMDB data.

Throughout the deployment process and beyond, we provided training for our teams. We also created step-by-step CMDB process guides and documents that lay out policies, procedures, roles, responsibilities, and use cases. We continue to do annual best practice reviews with Professional Services to ensure we're taking advantage of the latest capabilities and our data is in the best shape.

"We've got automated discovery on all the infrastructure and on vertical services," said Joe Corpion, Director, IT Operations Governance, ServiceNow. "We don't have to go out and inventory data centers, we don't have to go out and inventory what apps and services are installed where. That saves a significant amount of time."

We now have more than 2 million CIs, both **discoverable** data—anything to do with the device that can be queried at the system level—and **undiscoverable** data—which includes who owns, supports, and manages it, which is obtained manually—in our CMDB.

> “
>
> We've got automated discovery on all the infrastructure and on vertical services. We don't have to go out and inventory data centers, we don't have to go out and inventory what apps and services are installed where. That saves a significant amount of time.
>
> – Joe Corpion, Director, IT Operations Governance, ServiceNow

Lessons learned

Lining up all the information, identifying data owners, and working with them to collect their offline data took time and effort for the IT Ops team.

In response, our IT Operations Governance team launched an annual CMDB audit to certify each critical endpoint, app, service, and the overall infrastructure. The audit includes identifying data owners, creating consensus on which critical devices should be "principal CI classes"—those CIs most used in tickets—and enabling data owners to find and update their own principle CIs, critical CIs, apps/services, or devices.

Because not every device/app/service necessary is discoverable with Discovery's out-of-the-box configuration, the IT Ops team is able to create a list of custom discovery, patterns, and devices. For example, we created our own custom class to manage communication and Internet voice data circuit because Discovery's out-of-the-box circuit class is limited to electrical circuits.

Undiscoverable CMDB data acquisition is also handled via integrations and imports. If a CMDB device CI is created via an offline source (e.g. integration or import), Discovery still needs to coalesce when it discovers the same device later to update the same CI device record instead of creating a duplicate.

Through our ongoing process, we've learned the importance of starting small and confirming the initial Discovery requirements are effective before expanding across additional states, provinces, or regions. Also, it is essential that organizations have a dedicated Discovery lead and the Discovery process documented, launched, trained, and included in a knowledge base article.

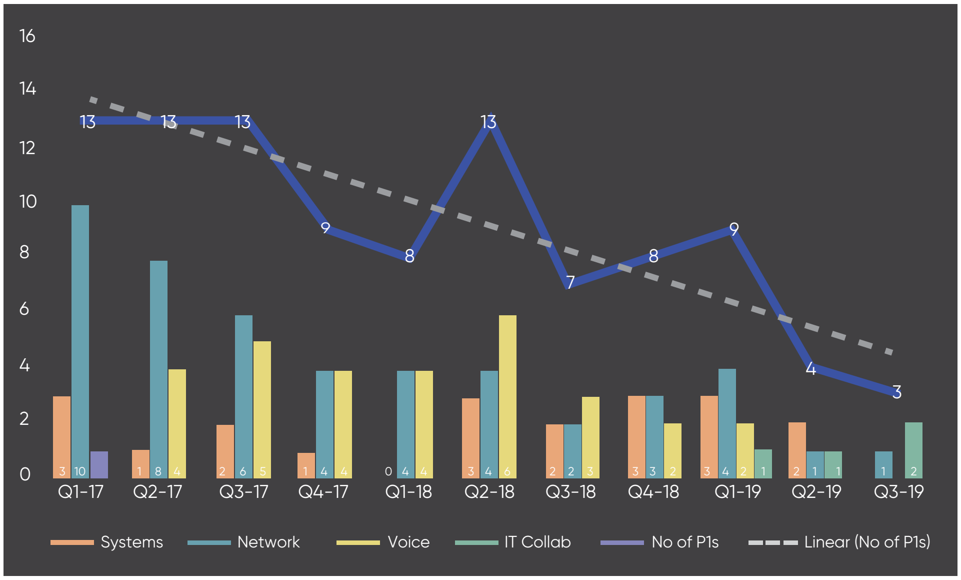
Time and cost savings and improved user experience

The well-configured, audited, and managed CMDB with ServiceNow Discovery is saving us a considerable amount of time and money:

- We're seeing a **40% time savings** on IT efforts to populate devices and relationships by creating CMDB Discovery process documents that contain policies, procedures, roles, and responsibilities
- P1 incidents have been **reduced 58%** over a two-year period
- The time to close vulnerability tickets was **reduced 71%** by correlating vulnerabilities with configuration items
- **91% of changes and configuration items** have an automated approval process
- **Critical Service outages can cost up to $300,000 per hour** (Gartner, The Cost of Downtime, 2014)

"We had a goal several years ago: zero Infrastructure downtime," Joe said. "This depends on network availability and systems resilience, and the foundation of those is our ITOM suite, specifically our CMDB populated by Discovery.

"If we didn't have Discovery, we'd be limited to tribal knowledge and external documents," he said. "Discovery has refined, sped up, and increased value and precision for whoever's trying to use those critical apps, services, and all supporting infrastructure."



CMDB Discovery Solution

- Accurate CMDB is the foundation for operational activities and a single source of truth
- CMDB Health Dashboard gives a clear, concise view of CMDB health: completeness, correctness, compliance
- Operationalizing our CMDB, which includes Discovery, yielded clear ownership, roles, and responsibilities
- Rebalancing mid-server deployment and discovery scheduling based on location and tuned our Discovery windows to ensure the discovery scans complete in a timely manner.

40% **Time savings on IT efforts to populate devices and relationships**

58% **Reduction in P1 incidents over two years**

71% **Reduction in time to closed vulnerability tickets**

Bringing security to our ecosystem

Covering and protecting our information securities vulnerabilities depends heavily on CMDB Discovery, and Finance depends on ServiceNow Asset Management, which relies on CMDB Discovery to tell us what we've invested in hardware, where, when, and whether it's in use or needs rightsizing or refresh.

When there is an incident that disrupts our critical apps and services, our Services Reliability Team knows about it right away thanks to the Event Management dashboard. This team can then resolve the issue faster and smarter.

For example, when we had a p0 outage in our primary San Jose data center, in our core SAP Finance system, we learned that while many independent infrastructure layers and end-user apps/services were available, the data/network connections between these were not fully mapped and monitored. So we focused on identifying and mapping all SAP integrations/interfaces/communication channels in our CMDB. Once we complete this, we'll map all our primary/production global internal instance integrations to ensure these integrations are highly available and monitored.

Looking forward

With the continued growth of our company, there are always additional devices being added to the CMDB. For instance, our Security Architecture team is currently evaluating and performing a proof-of-concept with Internet of Things-secure appliance tools.

Having CMDB Discovery to make our hybrid cloud ecosystem fully transparent is essential to managing the tagging of virtual devices. To support this effort, we're enhancing our cloud management tools to work closely with our CMDB.

About ServiceNow

ServiceNow makes the world of work, work better for people. Our cloud-based platform and solutions deliver digital workflows that create great experiences and unlock productivity for employees and the enterprise. For more information, visit: www.servicenow.com.

Now on Now is about how we use our own ServiceNow solutions to work faster, smarter, and better. With Now on Now, we're achieving true end-to-end digital transformation. To learn more, go to: www.servicenow.com/nowonnow.

> “
>
> If we didn't have Discovery, we'd be limited to tribal knowledge and external documents. Discovery has refined, sped up, and increased value and precision for whoever's trying to use those critical apps and services or communication paths.
>
> – Joe Corpion, Director, IT Operations Governance, ServiceNow