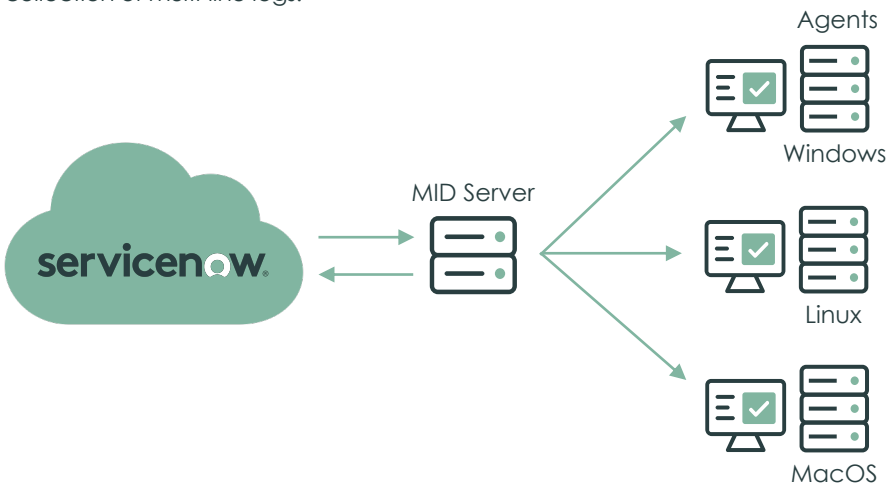
ServiceNow® Agent Client Collector (ACC)

Unified agent-based discovery, monitoring, and log collection that runs natively on the Now Platform®

By embedding agents on host systems, ACC complements ServiceNow's broad credential-based discovery capabilities, augments or replaces your existing monitoring tools, and powers AI-driven log analytics on your ServiceNow instance.

- **Discovery:** Because ACC agents initiate connections to your ServiceNow instance, they don't require host credentials or open inbound firewall ports. This simplifies deployment and makes them ideal for implementing zero-trust architectures. ACC agents are also well-suited for discovering endpoints, other intermittently active hosts, and previously inaccessible hosts. ACC agents provide system-level discovery of Windows, Linux and MacOS hosts. However, they aren't a like-for-like replacement for credential-based discovery. For example, they don't collect and parse configuration files or log in to applications to discover application context for service mapping.
- **Monitoring:** ACC agents handle both events and metrics, providing a unified monitoring solution. ACC monitoring is policy driven, replacing tedious manual monitoring configuration with flexible centralized monitoring policies on your ServiceNow instance. ACC agents collect a wide range of metrics based on these policies and apply adaptive thresholding to generate events. They also perform other policy-based checks—for example, whether a specified process is running—to create events. Events are sent back to ServiceNow® Event Management for correlation with other event sources, and metrics are also sent back to the ServiceNow instance where they can be visualized in the ITOM Health Operator Workspace and Insights Explorer.
- **Log collection:**[1] ACC agents automatically collect logs from servers and applications and feed these to Health Log Analytics (HLA), the log analysis component of ServiceNow® Predictive AIOps. HLA then analyzes these logs using advanced AI capabilities to learn normal log patterns and raise alerts when it identifies significant antipatterns that indicate potential future service issues. As with monitoring, ACC log collection is policy-based, so there's no need to specify which logs to collect when deploying a new ACC agent. ACC log collection also automatically associates logs with specific application services and supports collection of multi-line logs.



Agent Client Collector Architecture

1. Currently supports Linux. Windows and Kubernetes support are planned but not currently available.

Credentialless discovery

Discover IT resources without needing credentials or firewall exceptions. Easily extend discovery to previously undiscoverable hosts and endpoints.

Quickly discover custom applications

Collect comprehensive process information, fueling ServiceNow Visibility's AI-driven application fingerprinting capabilities

Replace fragmented monitoring tools

Runs natively on the Now Platform, works seamlessly with ITOM Health, comes with out-of-the-box support for common IT components, and can easily be extended.

Reduce monitoring configuration effort

Replace time-consuming manual monitoring configuration with flexible policy-based monitoring that automatically adjusts monitoring events, metrics, and thresholds based on CI type, operational status, and metric behavior.

Predict future service issues

Automatically collect logs and feed them to Health Log Analytics for AI-based analysis and proactive identification of potential future service issues.

Lightweight, scalable, and resilient

ACC can scale to an almost unlimited number of agents, with each agent having a minimal host footprint. To ensure monitoring continuity, ACC can also be deployed in a redundant configuration.

Highly secure

Meets stringent security requirements, including encrypted communications, in-memory encryption, non-root permissions, command line obfuscation, and other security best practices.

Easily discover custom applications

ACC collects comprehensive process information, which allows ServiceNow Discovery to discover custom applications through a process known as application fingerprinting. This uses machine learning to categorize and classify running processes, creating groups of processes that represent potential applications—for example, homegrown applications or new off-the-shelf applications not yet supported by ServiceNow Discovery.

Reduce software license costs

In addition to discovering endpoint hardware, ACC also discovers installed software, including key information such as the last time software was accessed. This accurate software inventory powers ServiceNow® Software Asset Management (SAM)—for example, by enabling SAM to reclaim unused or non-compliant software.

Efficient. flexible monitoring and log collection policies

Traditional monitoring need to be continually tuned—for example, adjusting metric thresholds as you learn more about your infrastructure behavior. These standalone tools also have no visibility of your service lifecycle, so they can't automatically adjust when you add new IT components, carry out maintenance, or take infrastructure out of service.

ACC's policy-based approach drastically reduces this effort. It allows you to define monitoring policies that are tied to specific CI types in your CMDB. For example, you can create one policy for in-service Linux servers, another one for service under maintenance, and another one for servers in your test environment. You don't need to track or make changes for individual CIs. Instead, ACC automatically sends the correct policy to each agent, including information such as the specific data to collect, hold off/hold periods, collection frequencies, and other parameters.

ACC also extends this policy-based approach to log collection. Simply specify which logs to collect for a specific CI type—for example, Tomcat on Linux—and log collection is configured automatically.

ACC comes with a rich set of out-of-the-box policies for widely deployed infrastructure components, such as operating systems webservers, application servers, and databases, and more. You can easily modify these policies, and you can also create additional policies to support new infrastructure types.

End-to-end transaction monitoring and SNMP polling

You can configure ACC agents to carry out remote synthetic transactions on HTTP service endpoints, providing application service performance and availability monitoring. By combining this synthetic monitoring with nodal ACC monitoring using service maps, you create a complete view of service health that ties the service to its underlying infrastructure. ACC Agents can also be configured to poll SNMP devices.

Highly extensible

ACC agents are based on Sensu Go, a widely deployed open-source monitoring framework. The Sensu community has produced hundreds of plugins that you can use. You can extend ACC capabilities by developing your own plugins in any programming language conforming to the Nagios specification, and you can also use existing Nagios plugins without modification. ACC also supports OSQuery, allowing you to query hosts and run remediation commands on demand or from ServiceNow workflows using the IntegrationHub spoke available on the ServiceNow Store.

Lightweight, scalable, and resilient

Embedded ACC agents consume less than 0.1% of host CPU resources when idle and typically less than 3% under load (i.e. performing 80 checks a minute). Agents also enter silent mode to conserve CPU resources when CPU activity exceeds a configurable threshold. Disk and memory footprint is minimal, with agents requiring approximately 140 MB of disk space and 50 MB of RAM.

Agents communicate with the ServiceNow instance via MID Servers, providing a scalable and robust monitoring architecture. Each MID Server can support up to 5,000 connected agents, allowing you to grow the number of agents simply by adding MID Servers. MID Servers can also be deployed in clusters, ensuring monitoring continuity if a MID Server fails.

Robust security

ACC is designed to meet the most stringent security requirements. Agents initiate connections with MID Servers over encrypted WebSocket connections, with no need to store host credentials in the MID Server or to open inbound firewall ports. Communication between MID Servers and the main ServiceNow instance is encrypted.

Agents run as non-root users. Agent files can't be read by other non-root accounts on the host system. Agents locally encrypt sensitive information in memory, such as MID Server passwords and sensitive command line parameters. Sensitive command line parameters are also obfuscated when displayed or logged.

servicenow

SN-Datasheet-ITOM-ACC-091721