Agent-less and Agent-based Discovery Products

It would seem that having a current IT documentation is a commodity after all those years of bringing ITIL and its processes to IT organizations. IT documentation is essential for every IT organizations to make correct decisions based on solid data.
But why are many IT organizations still struggling with their IT documentation? Once, a CMDB is in place, everything should work smoothly, correct? According to Wikipedia, a CMDB is

> ”is a repository that acts as a data warehouse for information technology (IT) organizations. Its contents is intended to hold a collection of IT assets that are commonly referred to as Configuration Items (CIs), as well as descriptive relationships between such assets. When populated, the repository becomes a means of understanding how critical assets such as information systems are composed, what their upstream sources or dependencies are, and what their downstream targets are.[1]”

The reason is that although discovery tool vendors promise the opposite, it is not easy (with or without tools) to create an initial IT documentation and it is even more difficult to keep it up-to-date. The reason why it is difficult – even with tool support – is the sheer amount of data and the complexity of the dependencies. Let's assume, you have a network of about 3000 servers and another 20000 clients. How do you know whether your discovery tool has discovered all areas of your network? How do you know what the overall data quality of the gathered information is? It could be that you got all details that you need from the devices, but it might also be the case, that you got it only from 20% of your devices. Discovery tools that do not provide any kind of data quality metrics loose their usefulness in larger environments.

There are actually two major network discovery tool approaches. The first approach is the usage of so called ”**Agents**”. An agent is a piece of software (usually provided by the discovery tool vendor) that gets installed on a device on the network. The agent can locally collect detailed hardware and software information and report it back to a central repository. This approach is called ”**agent-based**” discovery, since the discovery relies on agents that get deployed on all devices on a network. While agent-based products have their advantages, one of their most important disadvantages is that the deployment of the agents can be time consuming and complicated. This and the introduction of management protocols lead to another approach called ”**agent-less**” discovery tools. The idea of this approach is to leverage protocols that already exist on devices. Many operating systems and device types provide protocols that expose hardware-, software- and configuration information or that let administrators configure the device. For instance, most network infrastructure devices such as routers and switches offer plenty of information via the **SNMP** (Simple Network Management Protocol) protocol. Windows computers usually support the WMI protocol and many Unix computers either allow SSH or telnet access (besides of other protocols that they might offer). Agent-less discovery products make use of all those protocols to get an as complete as possible picture for a device. The advantages, that there is no need to deploy agents on the network. However, keep in mind, firewalls might be blocking the traffic between the discovery station and the device.

The following sections describe the pros and cons in more details.

”Agent-less Inventory Products are best!”

Agent-less discovery tools do not require the installation of proprietary agents. They typically use the protocols that devices already offer. This approach is best when used for projects or assessments where agent deployment is not feasible.

The protocols that are used differ depending on the operating system platform or device type. For Windows computers, the most prominent protocol is **WMI** (Windows Management Instrumentation). WMI offers plenty of hardware, software, and configuration information for Windows computers. Unix Computers usually offer **SSH** (Secure Shell) and **WBEM** (Web Based Enterprise Management). WBEM is similar to Microsoft's WMI protocol and offers depending on the operating system platform detailed hardware and software information. SSH offers the full power of all Unix command line tools. **SNMP** (Simple Network Management Protocol) is the protocol of choice for most network infrastructure devices such as switches, routers, firewalls, networked printers and others.

The nature of agent-less discovery tools is that multiple protocols and ports are used to obtain a complete picture of a device. In larger networks, this can often cause firewall issues. Protocols required for the discovery might be blocked by firewalls within the network. In this case, it is essential to plan the discovery tool usage. You need to think in which sub-network to install the software for optimal access or whether you have to plan changes of your firewall settings.

Agent-less Discovery Tools

- No time consuming agent installation necessary
- Usually quick to deploy and get results quickly
- The only viable solution for consulting projects or one-off scans.
- Minimal impact on the scanned device.

- Problems to capture occasionally connected devices, such as notebooks or tablets that are only rarely online
- Firewalls prevent agent-less tools from getting information
- Agent-less discovery tools require access credentials for devices which might be difficult to get in large environments
- Agent-less products can only collect device information that is accessible via the available.

”Agent based Products are best!”

Agent based products require the installation of a proprietary software (the so called ”agent”) on each device to be scanned. The agent runs locally on each device, gets hardware and software information, and reports it to a central station. This approach makes the usage of agent-based tools difficult if not impossible for assessment projects. Customers often do not accept rolling out agents just for the duration of a project or an assessment. On the other side, since the agents run directly on the discovered device, they usually have full access to all system resources and configuration items.

Having access to all resources locally is an advantage but most administrators do not like agents too much. Even though vendors test their agents thoroughly, there is always a chance, that agents run wild (max out CPU or memory) which might have negative impacts on servers and business applications. And since there are often several types of applications (monitoring applications, inventory discovery, license management, ...), administrators get into the situation where they have multiple agents for different purposes running on a single device.

A big drawback of agent-based tools is that devices that do not have the agent installed are not visible to the discovery product. You can never be sure that your discovery result contains all devices that you are interested in.

Furthermore, there may be devices, which do not permit installing agents. Devices such as routers, switches, networked printers and others rarely allow the installation of agents. For those devices, the agent-less discovery is the only way to retrieve information.

The advantage of agent-based discovery tools (besides full access to local resources) is that administrative credentials are only needed for the installation of the software. After that, the agent usually runs as a daemon process in the background. Later changes to the access credentials do not harm the outcome. In environments, where administrative access credentials are not available for the discovery scans, agent-based products are the only solution.

Agent-Based Discovery Tools

- Local access to all resources enables collection of all available information
- No user accounts required after the initial agent installation
- Less firewall issues
- Possibly better data, because the agent can locally access all information available that might not be accessible from remote.

- Defective agents might negatively impact devices
- Administrators acceptance is declining with the number of agents installed for different purposes.
- Not suitable for assessment projects and one-off scans.
- Devices without agents do not get discovered.

”Bringing it all together…”

As always in life, there is no black or white. An optimal solution is usually a combination of different approaches. Therefore, at JDisc we use a combination of both ideas. A purely agent-less mode allows the usage for assessment projects or one-off discovery scans. Unfortunately, the most important protocol for Windows computers **WMI** (Windows Management Instrumentation) is not very firewall friendly. It uses a randomly assigned port between 1024 and 65535 (Windows 2003 or earlier) and ports 49152 to 65535 (Windows 2008 and later).

In environments where firewalls block necessary protocols, we can enable our optional Windows discovery agent. Unlike traditional agents, the JDisc agent gets deployed automatically on Windows computers during the discovery scan. There is no manual interaction required. Once, the agent is installed, the discovery tunnels WMI and access to Windows Registry through the agent. This approach allows accessing WMI and Windows Registry information through a single port (445). JDisc Discovery also uses the agent to execute system commands and collect the output on Windows computers. One essential feature is that the agent destroys and uninstalls itself when the discovery of a device has been completed. Therefore, we call this kind of agent ”zero-footprint agent”. This approach allows collecting information where purely agent-less products fail.

Unix operating systems do not really require agents for inventory purposes, because there is always some kind of shell access (either via telnet or via SSH). Once, the discovery tool has shell access, it can execute locally any system command in order to gather inventory information.

Hybrid Discovery Approach

- Local access to resources allows collecting virtually all inventory information(temporary agent for Windows)
- Less firewall issues
- More accurate inventory information because the agent can locally access information available that might not be accessible from remote
- No time consuming agent installation necessary
- Quick to deploy and quick results
- Minimal impact on scanned devices
- Works perfectly for one-off discoveries
- No additional permanent agents

- Defective agents might negatively impact devices (however, the zero-footprint agent minimizes this risk)
- Administrative access credentials are required for each scan

Conclusion

While agent-less discovery tools are getting more and more popular, there is one case that they cannot cover. Environments of customers that are not willing to supply administrative access credentials for the discovery purpose, cannot be scanned by agent-less products. However in all other situations, agent-less discovery products are often easier and more cost effective to implement. Some products such as ”JDisc Discovery” use a combination of agent-less and agent based in order to get the best out of both worlds.


This article has been written by Thomas Trenz, CEO and founder of JDisc. Thomas has a long history in designing and implementing network inventory and discovery solutions. 2009, he started his own business with JDisc. JDisc's mission is the delivery of automated network inventory and discovery solutions for all kind of devices and all kind of different operating system platforms. Feel free to join the journey with JDisc Discovery on http://www.jdisc.com or Thomas's blog on http://blog.jdisc.com.