xAssets Hosted Services

Microsoft SAM Assist Audits with xAssets

© 2007-2010 xAssets.com Limited

xassets
asset • management • software

Introduction

Microsoft sponsors SAM Assist audits through Microsoft Large Account Resellers. These audits serve to establish the licensing usage of MS products for the next term of the Microsoft agreement, and will also enable the customer to understand their licensing position on other products.

xAssets Software Discovery Service (SDS) is one of the preferred tools used by Microsoft Large Account Resellers to audit end customer software implementations. This is a hosted service which discovers the network for 30 days and then extends reporting and recognition fine tuning for an additional 30 days.

This is a low cost service, and any company can sign up direct with xAssets or through their LAR.

At the end of the audit, the customer and the LAR can see the licensing position and can reduce installations or increase/reduce licensing to minimise expenditure while ensuring legal compliance.

These audits also prove invaluable to the end customer. The audit data includes an inventory of all hardware on the network, so anyone involved in Desktop Management, Server Management, Network Operations, Capacity Planning, Help Desk, Security Specialists and many other IT functions, can easily see which assets exist against which users, in which locations, and can start to use this information to help understand the assets present on the network and their status.

Preparation

Like any hosted service which is to conduct discovery, it is essential to have access to the network. xAssets prefers not to open ports or create other vulnerabilities, so we create a small VM inside the customers network to host a “collection server”. This system feeds data to the hosted services and controls all discovery processes through a secure, encrypted and compressed SSL web connection.

The end customer or the Large Account Reseller would also have the Microsoft MLS statement prepared. This statement enables the existing license entitlements to be assessed. xAssets Software Discovery Service includes a function which loads in the Microsoft MLS statement into the Software Asset Register, enabling comparison of used titles against purchased titles.

xAssets SDS also caters for Active Directory (AD) integration, SCCM integration, and the loading of Location to IP relationship spreadsheets. The ability to pull data from

multiple sources ensures that the system knows about all possible assets on the network and therefore makes it easy to check that all known assets have been discovered fully.

Implementation

Once the server is prepared, xAssets SDS consultants connect with the customer to install the collection server software. Usually this process takes about 20 minutes. Then discovery can begin.

Usually the consultant will initiate discovery during the first webex session, and smaller organisations (1000 computers or less) can usually see a first discovery of their entire network within an hour of implementation.

At the end of the implementation session, the consultant and the customer will agree a discovery schedule appropriate to the size, speed, and availability of devices on the customers network. The discovery schedule will then execute automatically, feeding delta data to the xAssets hosted service for the next thirty days.

Execution of Discovery

As discovery runs through the next few weeks, computers of absent staff will begin to appear and the network discovery percentage increases from about 70%-80% on first discovery to between 90% and 99%.

xAssets consultants will then work with the end customer to discuss nodes which failed to discover (because they were present in Active Directory or SCCM), and the customer can then investigate whether these specific nodes still exist, have been reimaged, or have been disposed of.

Throughout the discovery process the customer will have full access to the collection server and to the xAssets SDS web application which shows the results so far and includes compliance reports and asset inventory.

Reporting Phase

Customers will use the built in reports in xAssets to assess the software compliance position and may choose to make adjustments to their network to remove software.

Many customers choose to continue to use xAssets Network Discovery as an extension to the xAssets SDS service. They find that the inventory information collected is invaluable not only for Software Licensing and Compliance, but also for

removing unwanted software on the network, detecting security risks such as computers which are not patching or computers which are missing AV software, and for capacity planning where suitability for upgrades and rollouts can be assessed.

xAssets staff will work through the list of unrecognised software at each discovery and ensure that all software is fully recognised, and properly categorized as licensable or free.

Information Collected

xAssets Discovery collects information by discovering endpoint computers and by querying local systems such as Active Directory and SCCM. Despite being a very fast process and very light on the network and light on the endpoint, comprehensive asset information is returned including:

- Serial numbers, Make, Model, BIOS, chassis type, Time Zone
- CPU Speed, slots, information and architecture
- Full Network and domain information
- OS version, service pack, edition, install date
- Hard disk space, size and serial number
- Software on disk (exe file header scan) and software in registry
- Device manager entries for internal and external devices
- Monitor Make, Model and Serial Numbers, multiple monitors are supported
- Services and Daemons
- User information
- Memory information and memory slots
- Patches installed

Impact on Network and Endpoints

The impact on endpoints is minimal. A typical discovery would consume between 1 second and 4 seconds CPU on a desktop or laptop computer, and about 1 second or less on a server.

The discovery system does not deploy agents and does not write any information to the endpoint's hard disk or registry, so each discovered computer is left completely untouched by the discovery process.

The information transmitted across to the collection server from the endpoint is minimal, about 100k per desktop and about 40k per server. This information is then delta analysed by the collection server, the delta is compressed, and then it is sent up to the xAssets hosted infrastructure server from a lazy write process, ensuring

that there is no measurable impact on the customer's internet connection and associated resources.

Technical Background

xAssets invested substantial funding to develop highly optimized agentless discovery technologies which would run at super fast speeds and yet have no impact on the network. The result is a discovery engine which can run in large corporate environments without a measurable impact on the network or on the endpoints being discovered.

Many agentless discovery tools rely on WMI alone. These tools list software from the registry but often a small percentage of those titles will be ghost installs and WMI has no way of distinguishing between ghost install and real installations. For that reason, we rely on a multi-faceted approach to discovery where we inspect the add/remove software list but we also inspect EXE file headers and test for physical software presence within a network.

Our technology is unique in having access to EXE file headers, Windows API, BIOS, and low level calls on the endpoint, and yet does not require any kind of installation or change on the endpoint to achieve this.

The discovery technology is also open, so if we hit an obstacle on a particular network, our consultants can reshape the discovery process to work around it. This also allows discovery by many different techniques, including email, internet, local deployment, AD push, logon scripts and the default agentless technology.

We combined this excellent technology with some innovative ways of feeding information from customer networks into a cloud environment, and this was achieved without having any significant effect on the customer's internet connection and without requiring open ports.

Finally at the application layer the user interface is deeply configurable so we can insure that all menus, dashboards, queries, forms, reports and alerts are aligned to a customers data set. For example a large company with multiple domains (e.g. from acquisitions) might be focussed on discovery by domain, whereas other organisation might run a single domain and then their reports would be focussed on discovery progress by location (or IP range).