What IT professionals need to know about inventory, configuration and IT Asset Management

White Paper

wanstor

Contents

wanstor

Introduction

It's common knowledge that IT teams are facing a perfect storm of being asked to make process and people efficiencies, have cost constraints placed on them via finance and deal with ever changing compliance issues.

For IT Managers in medium to large organisations it must seem like dealing with these issues takes precedence over what IT is responsible for in the first place - delivering business services that directly support and empower automated processes that drive the business or not for profit organisation forward.

If delivering business services is the core responsibility of an IT team, doing so requires having the right building structure and assets in place; specifically, the IT assets that comprise those business services.

Laptops, servers, routers, hubs, databases, applications... there are ten's of classes, hundreds of types and an endless variety of components that are needed to build a corporate IT infrastructure that works all day every day for a business or not for profit organisation. All are connected, all are related and all are responsible for supporting the people, processes and transactions that make an organisation work on a daily basis.

So it should make sense that these IT assets should be managed, from the day they are initially identified as being suitable for the business, to when they are deployed, throughout their entire lifecycle right through to retirement and disposal.

However at Wanstor we have found through our own customer research of medium sized firms that over 70%+ still do not have a centralised and automated way to manage the physical, operational and financial status of their IT assets, much less the relationships that those assets have to one another.

This is where inventory management, configuration management and IT asset management come together. When joined up, these three IT disciplines form the baseline to a well-managed enterprise IT infrastructure. Together, they empower business service delivery and support.

This document should help IT Managers explore the distinctions among inventory, configuration and IT asset management. It should outline what IT Managers should know about these subject areas, what processes define each of these disciplines, and how they each contribute to improved IT efficiencies, cost containment and mitigation of compliance risk.

Defining inventory, configuration and IT asset management

First of all it's important to define what we mean by inventory, configuration and IT asset management. At Wanstor we base our definitions on industry best practices and define them as follows:

Inventory management

This is about capturing the basics - what assets are available, where they reside and who owns them on a daily basis. It is about maintaining an accurate, up-to-date view of owned hardware and software assets, so that IT Managers at any time can see an "actual state" of the components that comprise their IT infrastructure estate.

Configuration management

This adds a relationship dynamic, so that IT Managers can associate each item with other items in the inventory. In configuration management, classes and components, and upstream and downstream, establish relationships between each CI (configuration item). It involves processes around planning and identifying CI structures, having a controlled environment for changing CIs and being able to report on the status of CIs.

IT asset management (ITAM)

A much broader discipline, which adds several dimensions of management and involves a wider stakeholder base. It introduces the financial aspects of assets, including cost, value and contractual status.

ITAM also refers to the full lifecycle management of IT assets, from point of acquisition or procurement through to disposal, which together account for a comprehensive “expected state.”

> ## Taken together, ITAM is designed to manage the physical, contractual and financial aspects of those assets

As you can see from the above definitions inventory, configuration and IT asset management build upon one another. It’s best advised to undertake inventory management before undertaking configuration management or ITAM, although some processes in configuration management and ITAM can be implemented simultaneously, depending on the process, people and organisational maturity of the IT team.

Starting the inventory, configuration and IT asset management process requires planning and forward thinking. All three should undergo careful requirements planning.

This will help to minimise overlaps in functionality or data collection requirements as the processes broaden and mature.

Building a centralised inventory repository with configuration information forms the basis for a CMDB (configuration management database). The CMDB supports and enables processes in service delivery, service support, IT asset management and other IT disciplines.

The CMDB should hold the relationship among all system components, including incidents, problems, known errors, changes and releases. The CMDB should also contain information about incidents, known errors and problems, and corporate data about employees, suppliers, locations and business units.

The CMDB if managed and maintained correctly enables IT teams powerful insights into the current and ever-changing profile of the infrastructure. Tightly integrated with service management processes, inventory, configuration and IT asset management can be powerful and highly leverageable activities that help IT teams reduce costs, improve service and mitigate risk.

Three enablers to success

From 15+ years experience in asset, configuration and inventory management, Wanstor believes there are three primary enablers to success:

A single, centralized and relational repository

If having a simple inventory list was IT's only objective, then a simple database might suffice as a centralised repository. However, in configuration and IT asset management are the relational attributes of assets to components, contracts, operational status, financial impact and upstream / downstream relationships. Because the data from all three build upon one another, starting with a repository that's capable of managing complex relationships will save time and money in the longer term.

Organisational alignment and defined processes

These three disciplines touch many teams within a business. Within IT, the applications delivery group, infrastructure, desktop support and network operations are just a few of the groups that will rely on inventory and configuration information. IT asset management extends noticeable benefits to people in contracts, procurement and finance, meaning alignment with cross-organisational people and processes makes sense.

It makes IT Managers align requirements and understand all processes that will influence the initiatives, helping them to benefit from a co-ordinated implementation of tools, technologies and interdepartmental processes.

Scalable technologies and infrastructure

Important leverage is gained from deploying inventory, configuration and ITAM on an enterprise-wide basis. Cost benefits, service impact and risk mitigation benefits are all interlinked - succeeding in one area will impact positively on others. Planning and executing with enterprise-class scalable tools and technologies are the right things to do.

The value of inventory, configuration and IT asset management extend throughout an organisation's IT and, by extension, customers supported by IT. Thorough planning and implementation will improve IT service quality to the business community, reduce costs of those services and mitigate financial and operational risks associated with IT systems and the business processes they support. If IT Managers structure their goals, processes and tasks, and using a CMDB strategy as a fundamental success requirement, it will pay dividends throughout the implementation phase.

Inventory management: Building the right foundation with an accurate inventory count

The over arching goal of inventory management is to have a complete, up-to-date and accurate view of all network components, including PCs, servers, printers, hubs, routers, switches and software - everything that makes up the IT infrastructure.

As a minimum, inventory management should tell IT managers and System Administrators the device class and what's installed on the device. So, for any given time frame, inventory management provides the actual *real-time* state of all infrastructure components.

Implementing automated inventory management is the baseline (and is critical) to configuration management, IT asset management and all service management disciplines. By delivering a clear, cohesive view into network assets, it delivers a host of direct (as well as indirect) benefits.

The most obvious benefit is the time and effort saved from having IT staff undertaking physical inventories. As well as recovering this time in the IT team, automated inventory practices reduce the interruption to business users, otherwise caused by physical inventory, which can have a sizable impact on business unit productivity.

With a consolidated inventory process in place, the service desk will also see immediate benefits. These will be realised by simply knowing the components of an asset related to a call or incident.

From Wanstor's experience, the first 5 minutes of most service calls (for customers without an accurate inventory of IT assets) are spent trying to correctly identify the profile of the asset in questions.

Just think how much time this adds up to each month and how much more productive and proactive your IT service management team could be if they were saving 5 minutes per call and directly solving the problem.

Improving the utilisation of existing IT assets is another major benefit. Medium to large organisations typically have more hardware and software assets on hand than they really need.

Inventory management enables IT Managers to examine what they actually have so they can begin to make smarter choices about re-deploying existing assets before buying new ones.

Systems that are idle or otherwise go unused can be re-purposed, which reduces spending on new asset acquisition. By deploying the right automated inventory practice, IT teams can immediately stop the tendency to spend before re-using existing assets.

> **When it comes to compliance regulations having an accurate and demonstrable process in place for inventory satisfies control environment requirements**

Finally the other major benefit of an accurate inventory is that the business can reduce CAPEX spend and the amount spent on VAT for example as well.

Technology enablers and best practice advice

If the assets that made up your company network were static, inventory would be a painless one-time project. Of course we know that's not the case.

Laptops are constantly on the move, servers get decommissioned, and software changes and updates on a regular basis. Inventory management has to keep up with the change, and this means IT Managers need an automated inventory management practice that accommodates frequent and regularly scheduled updates.

> **Taking an inventory is the first step in establishing visibility into the infrastructure and provides the basis for populating a CMDB**

Although often initiated with a physical inventory, using automated tools to discover all components on a network saves a significant amount of time and effort for the IT team and provides an immediate view into the actual state of the company's infrastructure.

Determining the right level of asset detail the IT team will need requires planning and forward thinking. Large IT teams may want to see hardware inventory details, such as memory, disk and BIOS information.

For network devices, they might track network equipment, such as hub, routers and switches, down to the operating system level.

Determining the level of software specificity is extremely important, because it is this data that will be used to determine if software licenses meet compliance obligations.

As a minimum, an inventory product should collect all registry and non-registry files and be able to recognise version, release and patch levels.

This provides a baseline to enable more sophisticated software asset management capabilities that can reconcile files against titles as well as against licensable applications.

Best practices for inventory management initiatives

Get organisational buy-in	Although inventory may not involve the variety of stakeholders that configuration that ITAM does, starting early in the process always helps. IT Managers should make sure processes are well defined so that inventory accuracy is maintained. Set policies on frequency of discovery scans and inventory processes. Make sure stakeholders from all departments see reports on a regular basis so they continually buy into a centralised inventory process and configuration management practices.
Set up a centralised, relational CMDB-based repository	IT Managers should ensure there is a centralised repository - one that's capable of serving as a CMDB - to hold inventory items and eventually financial and lifecycle aspects of those assets with ITAM processes. Often, different divisions, branches or business units take inventory and store it uniquely - highly unproductive and giving only a fragmented view of the overall IT infrastructure estate. As we look deeper into value propositions associated with inventory, configuration and ITAM, having a single, centralised repository will clearly pay dividends.
Establish a baseline	Good inventory practices start with an accurate baseline. An accurate inventory of installed hardware and software forms the foundation of a solid ITAM program. This baseline identifies in ITAM which assets need to be redeployed, reused or retired. Doing a physical baseline is a necessary step to make sure you have all connected and non-connected IT assets in your repository.
Go deep, then go wide	At the start of an inventory practice concentrate efforts around getting one asset class correct. Then put processes in place to capture and reconcile the detail you need and test the processes though regularly scheduled updates to ensure they are thorough and yield the right results. Once successful, the same processes can be implemented for PCs, network equipment and detailed software inventory.
Have a process owner	Inventory management needs a single process owner who can consider the needs and requirements from all stakeholders and assure accountability throughout the entire process.

Configuration Management: Showing depth and relationship among assets

Configuration management takes inventory management to another level by introducing relationships between assets.

Adding additional levels of asset detail depth to the CMDB, configuration management describes relationship detail for each CI, delivering a more robust informational basis for incident, problem, change and release management.

In summary, configuration management provides a logical model of the infrastructure or a service by identifying, controlling, maintaining and verifying the versions of CIs in existence.

The objectives of configuration management are to account for all IT assets and configurations, provide accurate and up-to-date information on CIs to support service management and IT asset management processes.

It should also provide a baseline for incident, problem, change and release management. The configuration management discipline aims to fully support efficient delivery and support of business services.

The CMDB then becomes the master source of the state of the infrastructure upon which actionable reports, analysis and decisions models can be built to address compliance, performance and cost containment measures.

> **Configuration management practices should result in a complete, up-to-date and accurate account of the status of every CI and reflect this directly within the CMDB**

Reconciliation: At the centre of configuration management

A key configuration management task is reconciling what is found vs what IT Managers believe they have ("actual" vs "expected state.") This is accomplished by having discovery data compared with current repository of data and by identifying any unexpected discrepancies.

There are two potential causes of reconciliation discrepancies: Either an asset enters the infrastructure without going through a change process (e.g. rogue software is installed), or a change process was not properly closed, resulting in an actual asset status that's different from the expected state.

This is where the practical value of configuration management resides. By managing the actual versus expected state of IT assets, IT Managers can gain immediate and specific detail on any new hardware or software assets that may have unexpectedly entered in the environment. They can take corrective actions immediately, enabling quick remediation for potential security or compliance breaches.

If discovering and remediating individual CIs wasn't enough, IT Managers also have to consider the upstream/downstream effect of disruptions caused by discrepancies or unexpected activity.

Configuration management holds this upstream/downstream relationship of CIs so the IT team can better understand the true impact of change, service costs, service delivery and unforeseen service disruptions.

Because service disruptions can happen at any point in a chain of hardware and software dependencies, implementing configuration management practices is really the only way to proactively manage the data required to quickly resolve an outage.

System availability issues can get complex with distributed applications, so the impact of one change to one element of a service can have a domino effect on CIs that are down the line.

Additionally, as the scope, frequency and number of changes increase, automating the configuration of systems enables IT teams to improve the success of repeatable tasks that are often subject to human error.

This means, establishing and documenting configuration management processes is a critical component to a successful managed infrastructure. Ultimately it keeps the CMDB intact so that dependent processes are as efficient as possible in support of business services.

Configuration management for proactive IT management

From a strategic perspective, configuration management plays a crucial role in supporting all other service support and service delivery processes as well as asset management processes.

At the heart of the configuration management discipline, configuration management is about enabling proactive and service-oriented processes by actively recognizing and reconciling actual and expected states, taking action to rectify the situation or fulfil a requirement, and updating the CMDB to reflect the true status of the infrastructure.

A host of benefits result. Firstly, IT Managers can reduce software overspending to a considerable degree by having a software use monitoring process in place. Usage reports tell the IT team which applications can be uninstalled from one machine and re-used on another. Importantly, configuration management manages and reports on this process to maintain software compliance controls.

Through software distribution and patch management processes, IT Managers can control the distribution and installation of applications in a managed environment.

wanstor

Best practices for configuration management

Gain consensus around a federated CMDB strategy	All CI details should exist in a single, federated CMDB, a robust and relational repository easily integrated with other systems. This single point of data access simplifies how people find and use the information for various processes, and is more efficient to administrate.
Define an appropriate level of CI detail	Gathering and documenting the right level of detail is an important task. Start by defining that associated with critical business servers first, then add definition to secondary services. Many companies set the definition of a CI to be recorded at a level of detail justified by business needs, typically, that of independent change.
Define how the CMDB data is maintained	Clearly document process flows to reconcile the CMDB's expected state with inventory management's actual state. Additionally, document the service support processes that modify the operational state of a CI and define the criteria necessary to commit operational state back to expected state.

Co-ordinated with change and release management, software distribution provides staff efficiencies and mitigates risks associated with manual software distribution.

Having CI relationships exposed through network topology mapping and application mapping enables IT Managers the ability to identify, understand and take action, based on upstream/downstream and parent/child asset relationships.

For example, knowing that there are 100 business users on a payroll system that depends on a particular router and hub, which is dependent on a particular server, allows better management decisions around planned changes.

This level of visibility allows the service desk to achieve better response times for unplanned outages. Mitigating this risk is critical both for productivity purposes as well as for process control required for compliance and governance practices.

Configuration management also facilitates trend and impact analysis for change and problem management, key IT service management processes that contribute to lower service interruptions and greater system availability.

In fact, business continuity and disaster recovery strategies are reliant on the degree to which the current infrastructure state is documented.

Technology enablers for configuration management

A variety of technologies can be used to enable configuration management processes. Building on the foundation of discovery and inventory applications and processes, a reconciliation engine is the baseline of configuration management.

As requests for change cycle through the IT team, the reconciliation engine allows IT Managers to constantly monitor the actual state of each CI to the expected state based on the change management process. The extent to which IT Managers catch discrepancies associated with change management processes, as well as rogue hardware and software entering the network, determines the level of risk imposed on IT infrastructure management.

Relationship mapping of business service components is central to configuration management. This means network topology and software mapping capabilities become crucial components of configuration management.

Through these technologies IT Managers can build and maintain a relevant picture of how all assets are related. Strategic in nature, they allow IT Managers to see the network through active assets. With a relational repository in place, both agent and agentless technology can be used to populate the CMDB with asset location, dependencies and relationships, and characterise assets in the context of business services.

Software distribution and patch management are also at the heart of configuration management, because they enable consistent deployment of applications and software components. With automated discovery tools, version and patch levels are identified for proactive management of the current software state.

The value of this becomes quite apparent when a virus strikes: understanding which machines are vulnerable based on their application profile can make a significant difference. Automating the entire software distribution patch management process puts IT Managers in a highly proactive state.

The combination of a centralised configuration management process with software distribution and patch management makes it possible for IT teams to define and manage a Definitive Software Library or DSL, which in turn increases the stability and predictability of what gets installed and updated within the infrastructure.

Although configuration management processes can be called out as distinct, in practice they are tied to so many processes that they should be considered the foundation to any service and asset management solution.

IT asset management: Lifecycle management

IT asset management is often seen as the discipline that covers the financial aspects of inventory management.

Whereas the financial aspect is a distinguishing element of IT asset management, it is much broader in its scope, benefits and deliverables.

At Wanstor we believe IT asset management disciplines include contract management and entitlements, costs and depreciation values, asset leasing, maintenance and ownership status associated with each asset.

> **IT asset management also covers vendor management, service standardization and catalogue and request management**

IT asset management has also become a pivotal discipline for meeting compliance requirements, as it enables fiscal transparency, process control and documentation, and software license management.

From an IT operations standpoint, IT asset management extends inventory and configuration management by layering in processes that manage each asset throughout its complete lifecycle.

For each asset, there is a beginning (procurement), a middle (moves, adds, changes) and an end (retirement). Managing this lifecycle requires a full appreciation of each process associated with the stages of the asset lifecycle.

These processes can be automated through an integrated system that leverages inventory and configuration management systems.

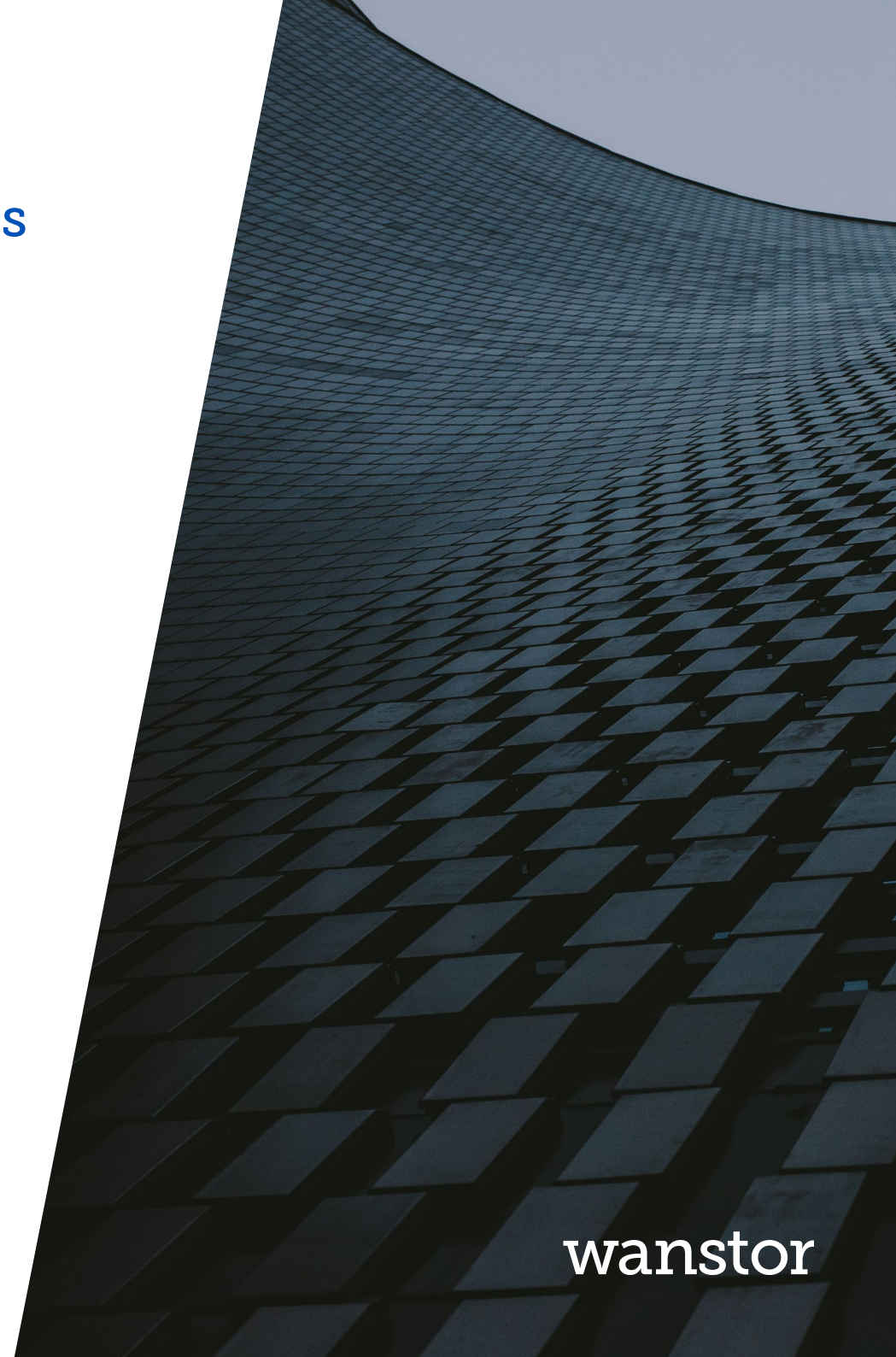
IT asset management for process automation and IT efficiencies

As discussed earlier in this document the overarching goals of IT Asset Management are:

- To establish processes that optimise the cost and the utilization of each asset
- To make sure that the supply meets the demands of the business and that IT assets directly support specific business productivity requirements in the most efficient and reliable way possible
- To mitigate risks associated with governance practices, compliance requirements and business continuity

At Wanstor, we believe these objectives can be met through core IT asset management processes:

- **Request management:** A standardised order and approval process gives business users the ability to order assets and to have those assets be approved though a workflow that reflects controlled management criteria for asset acquisition.
- **Stock / inventory management:** Stock and inventory management can expose existing available asset inventory. Having a centralised capability to check stock across multiple physical locations helps reduce the cost of unwarranted purchases by re-purposing existing stock.



- **Procurement:** Integrated with request and stock management, procurement support allows requests that cannot be fulfilled through existing inventory to be included in bulk purchase orders.

  Upon asset delivery and acceptance, the purchase order and the individual request detail can be checked to make sure only requested (and approved) items are received.

  Alternatively, issuing the asset request in a standardized, electronic way to corporate purchasing groups or employees (such as through an ERP system) will help to make sure that delivered assets are associated with the requester and associated cost centre.

- **IMACs:** Installs, moves, adds and changes comprise the majority of day-to-day work in an IT operations organisation. Standardising and automating these processes provide tremendous efficiencies.

  Recognizing the costs, productivity levels and cycle times associated with various IMAC types can help establish baselines for workload distribution and can also be used for chargeback systems.

  For example, IT can show exactly how many IMACs per department were conducted with specific detail on each one, illustrating the exact resource used by any given business unit.

- **Software asset management:** Software license contracting and utilization is a complex subject and requires specific, defined processes to manage it effectively.

  Typical issues around software asset management include overspending to meet compliance requirements, underutilisation of license grants and entitlements, and having a lack of standardisation for software titles, which causes unnecessary support headaches.

- **Contract management:** Lease and maintenance contract management present opportunities to save money and increase efficiencies. Automating the cycle of lease returns results in reduced fines and the ability to actually locate and return assets on time and in the requisite physical state.

  With maintenance contracts, systems can make sure that contracts cover only those assets that are actually in use. In- and out-of-contract repairs can be better reconciled with contract terms, saving time and money associated with unwarranted costs.

- **Financial management:** Key elements of IT asset financial management include cost centre budgeting, service and product pricing, and chargebacks.

Technology enablers

Effectively managing the physical, contractual and financial aspects of assets results in better cost control, improved IT services and improved risk management.

The single most important enabler to accomplishing these benefits is implementing a robust, relational repository.

Of course, having the repository in place when you build inventory management and configuration management disciplines is the perfect set-up, lending a much faster implementation cycle for IT asset management processes.

Even more so than inventory and configuration management, IT asset management requires powerful relational capabilities because of the inherent need to relate physical, contractual and financial status of assets throughout their lifecycle.

Fundamentally, every physical change to an asset affects its contractual and financial status. For example, if a PC changes ownership, the cost centre charge is affected.

> When a new application is installed on a PC, a software license contract needs to be related to the installation

If a server crashes, the financial status may change so that it's written off, and operational records need to show that it is no longer in service, and the associated maintenance contract is updated.

The relationship among an asset, its owner, location, software licenses, physical status and financial value is not difficult to track, but if a system does not automatically make adjustments to the various attributes upon a change, records quickly become old and irrelevant.

Best practices for IT asset management

Stakeholder alignment	Going beyond central stakeholders in IT operations, IT asset management has stakeholders in contracts, procurement, finance and compliance. Because each department is involved in discrete parts of the IT asset management lifecycle, defining cross-departmental processes upfront helps meet multiple goals.
Establish IT asset management project milestones	Implementing IT asset management requires careful coordination between IT and process owners. Best practices call for setting project milestones for process definition, software implementation, integrations, training, testing and rollout.
Set specific operational and financial goals	Most IT teams initiate IT asset management projects to gain specific, measurable results in three areas: cost control, risk mitigation and service level improvement. Specific operational and financial goals can be set to show incremental progress against each of these, using metrics around IT budget impact assessments, service quality levels and decreased risk of compliance irregularities.
Standardise on hardware configurations and software license titles	Putting in place standardised practices means selecting fewer hardware configurations and software titles, which enables significant volume purchase leverage and also reduces the burden on the service desk.
Establish periodic reviews of software usage	Set standards for how long an application remains unused before recalling it for re-deployment on another system. There may be different thresholds for different types of applications or different job types. For example, you might set a three –month usage threshold for Visio or a four-week threshold for a CRM client application.
Conduct internal audits	Regularly review asset management practices to make sure cross-functional processes are supported by automation as much as possible. Document these processes so that you can show proactive resource control in the face of an audit.

ManageEngine Desktop Central Overview

To help business and not for profit organisations manage their IT estates, Wanstor has partnered with ManageEngine to design, deploy and manage their Desktop Central solution for customers in the UK.

Integrated Desktop & Mobile Device Management Software

Desktop Central is a unified endpoint management solution that helps IT teams manage servers, laptops, desktops, smartphones, and tablets from a central location.

By using a Desktop Central solution from ManageEngine, IT teams can automate regular desktop management routines like installing patches, distributing software, imaging and deploying OS, managing IT Assets, managing software licenses, monitoring software usage statistics, managing USB device usage, taking control of remote desktops, and more.

It supports managing Windows, Mac and Linux operating systems. It also helps IT teams to manage mobile devices to deploy profiles and policies, configure devices for Wi-Fi, VPN, email accounts and so on., apply restrictions on using cameras, browsers and so on, and to secure devices by enabling passcode, remote lock or wipe. IT teams can manage all iOS, Android and Windows smartphones and tablets using one tool.

The need for unified endpoint management

IT asset footprints are growing rapidly in today's business and not for profit organisations. Managing these assets has become more challenging for IT teams with the ever-increasing numbers of laptops, desktops, tablets, and mobile phones, which are otherwise known as endpoints.

The best way for IT teams to make sure devices are being managed properly is by employing endpoint management software. Endpoint management becomes even harder with varied devices, or with devices that travel outside of the organisation's network.

wanstor

Benefits of unified endpoint management

Single-solution architecture	A single, centralised platform for endpoint management will help IT teams avoid complicated integrations among different software on multiple platforms. They will no longer need to compile, compare, and evaluate reports from different sources.
Ease of onboarding	A unified endpoint management platform allows organisations to easily push out device policies, applications, and environments, meaning devices go from out-of-the-box to in-use faster and with better baselining.
Helps improve IT security	Security is one of the primary concerns for any organisation today. Recent ransomware attacks just prove how dangerous zero-day vulnerabilities can be. A unified endpoint management solution makes it easy for IT admins to keep track of suspicious activities across all endpoints.
Improved visibility	Enterprises can monitor inventory, usage, vulnerable systems, and much more from one place. This visibility provides not only opportunities for cost saving, but also the ability to troubleshoot, diagnose, and resolve issues remotely.
Unified corporate IT environment	All the benefits of a unified endpoint management platform combine to deliver the single greatest advantage to organisations: a unified corporate environment in which experience is optimised across the organisation on corporate networks.

What is unified endpoint management?

Unified endpoint management is an umbrella approach to managing all the endpoint devices within an organisation from a central location.

In general, a typical unified endpoint management solution provides secure updates, patch management, automatic hardware and software inventory tracking, logging, mobile device management, software and OS deployment, workstation remote control options, license management, and overall quick remediation capabilities for IT professionals.

Key Desktop Central Features: Desktop Management

Desktop Management
Manage Windows, Mac and Linux

Patch Management
Automate patch deployment per OS and other third party applications, shield Windows and Mac from security threats

Asset Management
Manage your IT assets, Software Metering, Software License Management, Prohibited Software, and more

Active Directory Reports
100+ out-the-box reports provides a quick and complete insight of the Active Directory infrastructure

USB Device Management
Restrict and control the usage of USB Devices in the network both at the user-level and at the computer-level

Remote Control
Troubleshoot remote desktops with multi-user collaboration, file transfer, video recording, and more

Service Pack Installation
Scan and detect missing service packs of OS and Applications and automate deployment to stay up-to-date

Software Deployment
Simplify software distribution to install and uninstall software with built-in templates for package creation

Windows Configurations
25+ predefined configurations including Power Management, USB Device Management & Security Policies

User Administration
Define roles with selective privilege and delegate users to these roles for effective management

Power Management
Apply energy saving power schemes, shut down inactive computers and get system uptime reports

OS Deployment
Comprehensive disk imaging / deployment feature supports deployment needs in both offline and online mode

Mobile App
Start managing your desktops and servers on the go. Download mobile app for iOS devices

Key Desktop Central Features: Mobile Management

Mobile Device Management
Manage iOS, Android and Windows

Device Enrollment
Enroll devices manually, in bulk or let users self-enroll their iOS or Android devices with two factor authentication

Asset Management
Scan to fetch details of installed apps, enforced restrictions, installed certificates and device hardware details

App Management
Distribute in-house and store apps to devices, remove or disable blacklisted apps, assign redemption codes for commercial apps and more

Security Management
Configure stringent security policies such as passcode, device lock to protect corporate data from outside threats.

Profile Management
Create, configure and associate policies and profiles for different departments, roles or groups

Audit and Reports
Audit mobile devices with out-of-the-box reports such as Rooted Devices, Devices with Blacklist Apps, etc.

In-depth focus: Asset Management

An IT administrator must be up-to-date on the information about the software and hardware used across the organisation they work for. Manual compilation and reconciliation of IT assets is effort-intensive and error-prone.

Desktop Central's web-based inventory management not only helps automate this task, but also provides out-of-the-box network inventory reports.

Inventory management features

- Perceive audit ready hardware and software inventory details.
- Schedule scanning of systems to collect inventory data.
- Manage software licenses, category, and compliance.
- Detect, block, and auto-uninstall prohibited software in the network.
- Have real time access to software usage statistics.
- Automate alerts on specific events such as installation or uninstallation of new software, removal of hardware, etc.
- Over 20+ out-of-the-box reports and the ability to create custom reports across different formats.

wanstor

Scheduled inventory scanning

Desktop Central scans the Windows desktops and servers in the network periodically to collect hardware and software details and stores them in your the database. The inventory scanning interval is flexible and can be configured to meet the real-time needs of your organisation. This enables administrators to have access to up-to-date inventory information any time, without any manual intervention.

Alert notifications

Desktop Central sends email notifications to IT administrators for the following events:

- New hardware is added or removed in the network
- New software is installed or uninstalled in the network
- Non-compliance of software licensing policy
- Prohibited software is detected in the network

Hardware inventory

The hardware inventory provides complete details about the hardware used in the network. The hardware inventory reports helps IT administrators to:

- Sort computers by memory
- Sort computers by OS and service pack version
- Sort based on hardware manufacturers
- Sort by age, disk usage, type

Software inventory

Software inventory in Desktop Central gives IT Administrators access to:

- **Software metering:** Usage details of specific software such as number of times it has been used, total usage duration, systems with specific software etc.
- **Software details:** View commercial and non-commercial software information including vendor name, installation date, and software version.
- **Software license compliance:** Provides the ability to view the compliant and non-compliant software being used in the network.
- **Prohibited software:** Blacklist software, block executables through, and auto-uninstall prohibited software in the network.
- **Warranty management:** Track the warranty information of the hardware assets managed by your IT team.

Network inventory reports

Desktop Central provides out-of-the-box reports to view the software and hardware details of the network. These reports help IT administrators to gain a quick and accurate view of the network inventory. The ability to export reports to PDF or CSV formats help integrate with third-party reporting engines or to print it out for future reference.

Achieving ROI from your Desktop Central Investment

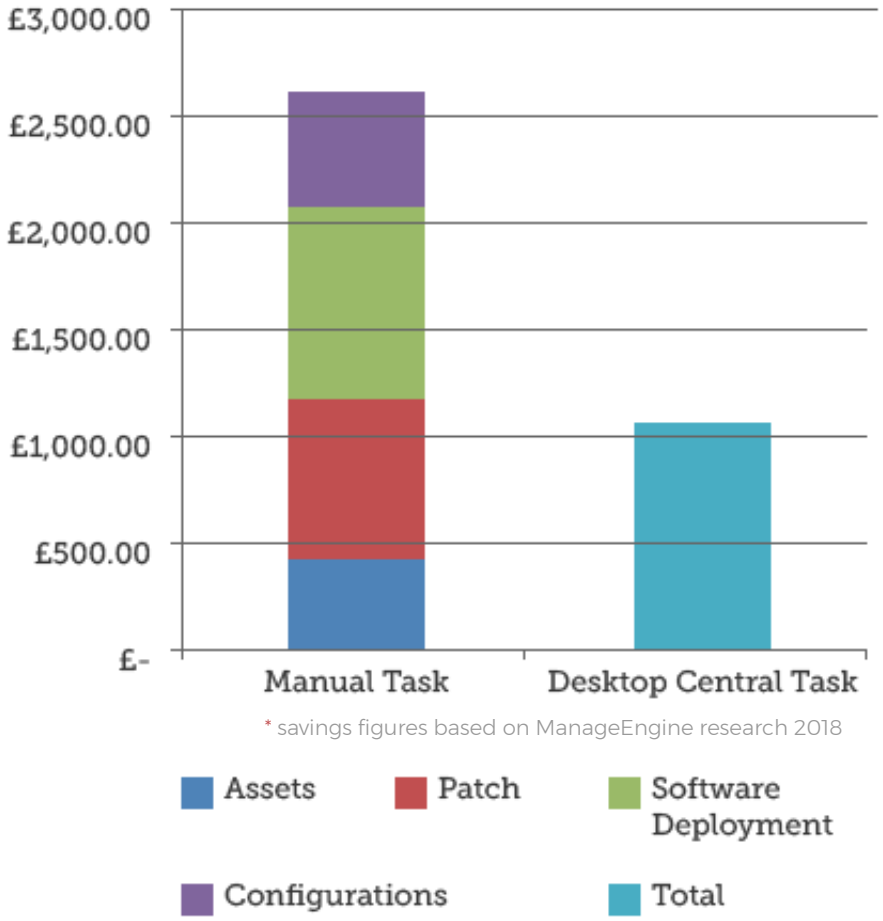
This example will demonstrate how Desktop Central saves IT teams, time, money and effort with a relevant and robust ROI calculation

Assumptions

- Network of 100 computers
- Hourly salary for a technician is £35

Notes

- While the cost of executing each task manually can be calculated, this is difficult within Desktop Central as it is integrated software. The graph to the right shows the total cost of performing these tasks using Desktop Central as opposed to manually.
- Whether IT teams do these tasks once or multiple times a year, the cost of doing it with Desktop Central is going to remain the same or may increase marginally, if you take into account the time spent by the technician in initiating the tasks from the management console



10 Reasons your IT team needs to purchase Desktop Central today

Integrated Desktop and Mobile Device Management Solution	▪ No need to rely on multiple tools for managing Desktops and Mobile Devices ▪ A single management console for all desktop and Mobile management tasks
Enhances Network Security	▪ Helps patch systems and applications automatically ▪ Enables administrators to apply windows security policies ▪ Restricts and customizes external device usages like USB, external hard disk, etc. in enhancing network security
Increases Productivity	▪ Robust support for BYOD ▪ Fosters collaboration between employees with their mobile devices ▪ Enables employees to access corporate resources from anywhere
Manages Distributed Environment	▪ Manages geographically distributed computers, devices and users from a central management console ▪ Allows setting up distribution points to minimize the WAN bandwidth consumption ▪ Provides control on mobile devices irrespective of location
Higher Return of Investment (ROI)	▪ Saves operational costs by automating various routine activities like Patch Management, Software Deployment, mobile application ▪ Manages BYOD and save costs from investing in new devices ▪ Enable and set up Power Management to see immediate savings on desktop power consumption ▪ Effective software license management will save cost of unused licenses ▪ Accessing asset information, installing software, tracking tickets now performed within single console i.e. by integrating Desktop Central with Service Desk Plus
Reduces Training Costs	▪ Simple point and click installation package includes an embedded relational database and webserver ▪ Saves working with multiple packages reducing training costs by providing a simple, user-friendly interface
Completely Web-based	▪ Completely web-based offering unparalleled flexibility in accessing the systems and mobile devices from anywhere
Integration with other ManageEngine Products	▪ Seamless integration of data with ManageEngine ServiceDesk Plus and AssetExplorer ▪ Help Desk and Desktop Management functions can be performed from single integrated console ▪ Integrates with ManageEngine Products such as Servicedesk Plus and IT 360 Applications
Easy Installation & Setup	▪ Single installation package including all required installables such as database and web-server ▪ Installation within 10 minutes and setup within one hour
Affordable Solution	▪ Offers competitive price and ease of deployment on standard hardware, supporting desktops, mobile devices and servers ▪ Accustoms without steep learning curve

Wanstor Customers using ManageEngine Desktop Central

Final Thoughts

Today's modern worker is no longer confined to a physical office or a Windows desktop or laptop. Although traditional Client Management Tools (CMT) would have been sufficient in the past, they are no longer enough to manage the increasing diversity of platforms and devices, BYOD, and frequent Windows 10 updates.

While many business and not for profit organisations have adopted Enterprise Mobility Management (EMM) solutions to manage mobile endpoints, maintaining both CMT and EMM without any integration is highly inefficient. Instead, IT teams need to select the right Unified Endpoint Management (UEM) solution.

Unified Endpoint Management combines traditional Client Management with Enterprise Mobility Management providing the IT team with a single view to manage devices, apps and data.

For more information about Wanstor and ManageEngine's Desktop Central solution please email us at **info@wanstor.com** call us on **0333 123 0360** or visit us at **www.wanstor.com**