Vizualiiz

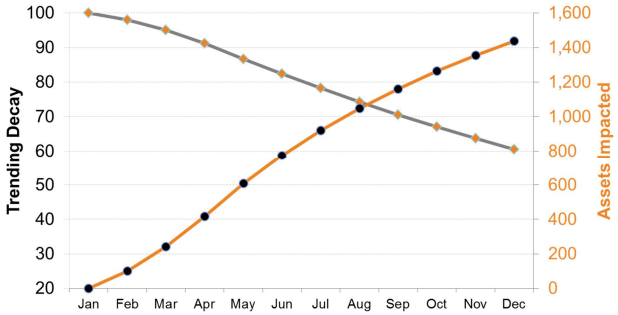
Best Practices Implementing RFID In Datacenters

Part 1: Initial Tagging & Data Scrub

Introduction

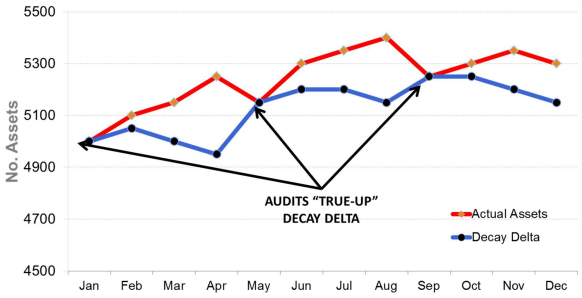
Unless you still believe the world is flat, you have already decided RFID solutions can benefit your company. Used in and around your datacenter, RFID can streamline inventory management of your critical assets, improve the time of inventory audits, reduce capital investments, and mitigate risks from potential disasters of regulatory compliance and corporate governance.

These principles resonate more so when one considers the importance of datacenter audits required to maintain an accurate picture of physical assets. The following illustration demonstrates the dramatic loss of accuracy within a 5,000 asset facility over the course of only 12 months when applying a mere 2%. decay per month.



Audits are the essential process to maintain data accuracy and integrity. However, audits are often still a manual and labor intensive process, prone to error. This challenge is intensified by the fluid nature of datacenter environments: New assets are acquired and existing assets are moved or decommissioned.

Keeping pace with dynamic change is the new order. RFID technologies and proper automated solutions can significantly address these issues. With the right tools, you can undertake a series of audits covering the gamut of stakeholder needs, inside or outside the organization, through pre-planned rapid spot audits, cycle counts, or full audits at the right time, in a fraction of the time normally spent attempting to do so. These "true-up" audits defend against data accuracy decay.



Where to Start

Success cannot be achieved until you know where to start and what to consider, know, and plan for. How will audit processes affect your datacenter operation and organization? How can you demonstrate success? How will other departments benefit from the decision to implement this new system?

This article -- Part 1 of a trilogy -- will outline the framework of best practices of the implementation of RFID in a datacenter, with a concentration on actions and needs. Many datacenters are still not RFID enabled, so we will examine the inception of all processes. Part 2 will address datacenter automation, and Part 3 will address how an RFID-based solution with the right intelligence can dramatically protect you and your business from all manner of risks.

What Assets Need RFID Enablement?

For most organizations, every datacenter asset is a critical one and must be controlled by systems and processes that are RFID enabled. Some companies choose to only tag high value assets. Others choose mission critical assets, those holding sensitive information or systems that are governed by regulations such as HIPAA, SOX, or PCI compliance. Many companies also have corporate governance requirements that may include, or be in addition, to regulatory needs. So, the first decision is to determine what assets require RFID treatment.

If one is considering a selective treatment path (I.e., by asset value), such assets are often dependent on the successful operation of others, and perhaps less valuable ones. In other words, those less valuable assets become critical too.

Physical Asset Placement

Consider where important assets are physically located in the datacenter: Are they in the right place? It may be hard to know at this stage, but we have found best practice to consider the following important issues:

To avoid the threat of a disaster (E.g., fire or flooding), consider having all your critical assets positioned near exits so they can be removed quickly.

Do not concentrate critical assets in one area of the datacenter. This ensures a localized power outage does not take down your entire business.

The same consideration should be given to assets located in receiving bays, hot-spares, staging and retirement areas.

Copyright © Vizualiiz Inc. 2015 All Rights Reserved

Initial Physical Asset Data Scrub

The initial deployment of an RFID solution requires a comprehensive and detailed data scrub of the physical assets in a datacenter during which:

- RFID tags are physically applied to assets.
- Each asset's attributes, such as serial number, hostname, location, and the association of this data with the RFID tag number are captured.

This appears at first to be a laborious task, but as we will discuss later, there are ways to significantly reduce the time and cost of executing this initial data scrub. And, when selecting the right solutions, future audits can be fully automated, which dramatically reduces audit investments of time and labor costs.

Numerous decisions must be made for this phase. While the principles of RFID enablement are common in every instance, each datacenter has its own unique characteristics and challenges:

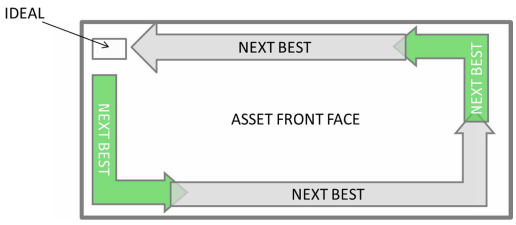
- The number and disbursement of assets.
- Whether assets are in racks, stand-alone, or both.
- Assets possess different sizes and form factors.
- Application of RFID tags must conform to best practices and guidelines.
- IMAC consideration must be given to the pace of asset decommissioning, moves, and changes.
- Physical access at the rack level – doors and access control.

Assets are not physically the same. They differ in dimensions, have different configurations and surfaces. In that normally RFID tags are fixed to an asset's surface via adhesive, different RFID tags with appropriate form factors need to be used.

Examples of RFID Form Factors

A blade for example will need a smaller tag than say a tape drive. Investing the time initially to identify the best location for the RFID tag will save money over time. Correct tag orientation will also yield maximum read performance. So, tag selection and placement is important. Here are some best practices we use in this regard:

- Surface selection needs to be even and flat with direct metal contact underneath the entire tag. You should avoid placing tags on areas of perforation or curved surfaces.
- Attach tags to the front side of an asset. Do not attach to top, side, bottom, back, rack mounts, or leaf ear mounts that are removable or replaceable. The following illustration shows the progression of ideal tag placement.



- RFID labels have human-readable components, so make sure the label orientation is consistent.
- Place tags either horizontally or vertically depending on the asset's form factor. It's generally easier to read a tag with a direct line of sight between the tag and the RFID reader but unlike bar codes, line of sight is not necessarily a requirement.
- If no acceptable position is available, use "hang style" tethered tags. Position tags with labels facing forward.
- Do not place tags over air vents. serial numbers, barcodes, model or logos, host names, LED's or lights, hinged doors, and of course in a location that will interfere with power or toggle switches
- Define the process and required accessories to capture the back peel release liner for tags attached via adhesives.

There are two other important factors to consider.

- Temperature can impact the adhesive mounting RFID tags. Tag selection should account for this including the use of specialty tags for hot or cold conditions.
- Some forward facing assets can have other assets associated with them that are behind them. We recommend flagging these occurrences on the face of the front asset to ensure these "out of sight ones are not overlooked.

Data Capture

There are two schools of thought as to when asset data should be captured during the data scrub process:

Copyright © Vizualiiz Inc. 2015 All Rights Reserved

- Apply tags to all assets first and then start the data capture process; or
- Capture attribute data for each individual asset when the tag is attached.

Both methods are valid and normally subject to the size of team working on the exercise. During the process, the team scans and matches both the asset barcode and RFID tag now attached. Racks also are tagged with RFID , which allows the asset to be associated with its rack. All the data should be captured on a mobile device to simplify the upload process to the system of record. The use of spreadsheets is a thing of the past and should be avoided, because spreadsheets cannot ensure data integrity nor capture the relationships of rack-to-asset or parent-to-child.

The Need To Validate

The last task following the initial inventory is to undertake a validation audit to verify the information captured during the data scrub is correct. Data captured in the system of record is downloaded to a mobile device with RFID reader integration. This provides for a rapid double check of all RFID tags and their associated relationships.

Once completed, clean and verified data must be loaded into an asset management or tracking solution, which will act as a system of truth against which all future inventory audits and IMAC can be monitored, managed, and measured.

Vendor Selection

The key to overall success is vendor selection. Researching solutions providers that specialize in this initial data scrubbing phase is important to the immediate and long-term success of RFID in your business. One needs to consider where the captured data will be stored and managed, to provide a "system of truth." What intelligent asset tracking tools do vendors provide for future audits and day-to-day operations, such as asset adds, moves and changes (IMAC).

Automation is critically important to ROI, so solutions that dramatically reduce manual operations and mitigate errors must be the focus. Different asset data will be required by different business stakeholders, so it's best to consider and understand these needs, as well as how they will be addressed by the solution.

By researching solution providers, you will begin to understand the capabilities of the technology, but we further recommend reading use cases of how others utilize RFID in their businesses.

In Part 2 of this trilogy, we will discuss how technology is now delivering major benefits to asset management through such capabilities as audit automation, structured workflows, and business intelligence -- the core of risk mitigation.

Copyright © Vizualiiz Inc. 2015 All Rights Reserved