

Brought to you by:



HDIM

for
dummies[®]
A Wiley Brand

Use DCIM as the
cornerstone for HDIM

Organize and implement
your hybrid strategy

Operate and monitor
hybrid infrastructure



Lawrence Miller

Nlyte Special Edition

About Nlyte

Nlyte Software is the leading company helping organizations with their digital transformation objectives. Our solutions address your hybrid digital infrastructure management (HDIM) — from desktops to networks to servers to IoT devices — across facilities, data centers, colocation, edge, and to the cloud.

Nlyte's approach to taming the hybrid cloud extends the reach of classic Data Center Infrastructure Management across the entire compute infrastructure. Using Nlyte's monitoring, management, inventory, workflow, and analytics capabilities, organizations can automate how they manage their hybrid digital infrastructure. Organizations can

- Reduce costs.
- Automate discovery and inventory of all networked asset and all associated attributes.
- Map dependencies between devices, network connections, and application workloads.
- Track asset and environmental changes planned and unplanned.
- Deliver inventory, operating status, change notifications, and alarms.
- Automate workflows, manage their progress, and provide an audit trail of all activity.
- Broker information with and between other critical systems including BMS, ITSM, and finance from a single source of truth.



HDIM

Nlyte Special Edition

by Lawrence Miller

for
dummies[®]
A Wiley Brand

HDIM For Dummies®, Nlyte Special Edition

Published by

John Wiley & Sons, Inc.

111 River St.

Hoboken, NJ 07030-5774

www.wiley.com

Copyright ©2020 by John Wiley & Sons, Inc., Hoboken, New Jersey

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Trademarks: Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

ISBN 978-1-119-71555-9(pbk); ISBN 978-1-119-71558-0(ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Elizabeth Kuball

Associate Publisher: Katie Mohr

Editorial Manager: Rev Mengle

Business Development

Representative: Karen Hattan

Production Editor: Siddique Shaik

Special Help: Michael Schmitt

Table of Contents

INTRODUCTION	1
About This Book	1
Foolish Assumptions	2
Icons Used in This Book	2
Beyond the Book	3
CHAPTER 1: Hybrid Digital Infrastructure Management 101	5
Recognizing Why HDIM Is Needed	5
Understanding the Evolution of HDIM	7
Looking at Key HDIM Components	8
Establishing DCIM as the Cornerstone of HDIM	9
CHAPTER 2: Organizing Your Strategy for Hybrid Digital Infrastructure	13
Taking Inventory of Current Space, Power, Physical, and Digital Assets	13
Forecasting Budgets for Service Delivery	17
Considering Supplier Relationships and Interrelationships	18
CHAPTER 3: Implementing Your Hybrid Digital Infrastructure	21
Leveraging Automation and Orchestration	21
Discovering IT Assets and Dependencies	22
Automating DCIM	25
Standardizing Catalog Offerings	25
Supporting DevOps Pipelines	26
CHAPTER 4: Operating Your Hybrid Digital Infrastructure	27
Ensuring Timely Request Fulfillment, Patching, and Updating	27
Enabling Continuous Improvement	28
Leveraging AIOps	28
Managing Backups and Failover Activities	29
Addressing Threats, Vulnerabilities, and Risks	30
Communicating Business Value	31

CHAPTER 5: Monitoring Your Hybrid Digital Infrastructure..... 33

- Getting Visibility into the End-to-End Environment 33
- Validating Licensing and Regulatory Compliance 34
- Analyzing Network and Infrastructure Performance..... 37
- Gaining Security Insights from Audit and Log Data 38
- Delivering a Superior Digital Experience 38
- Optimizing Workload Placement..... 39

CHAPTER 6: Ten (Or So) Questions to Ask a DCIM Vendor 41

Introduction

Modern organizations — whether long established or newly created — tend to use a large mix of information technology to power their business operations. These technologies often extend from the on-premises environment and hosted data centers to multiple public and private clouds. In the public cloud alone, most organizations today leverage numerous software as a service (SaaS) offerings — such as Office 365, Salesforce, and Workday — and platform as a service (PaaS) and infrastructure as a service (IaaS) offerings from providers such as Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, and Oracle Cloud.

This hybrid digital infrastructure has evolved because organizations understand that placing the right workloads in the right place to address the unique requirements of their business is critical to successful digital transformation. Strategically, this is the right approach, but it inevitably adds complexity and creates new challenges for the teams that manage the competing demands of heterogeneous hardware and software platforms.

To effectively manage this growing complexity, organizations need a complete suite of hybrid digital infrastructure management (HDIM) tools and solutions that work together to ensure they can drive the best business value from their infrastructure and operations (I&O) platform.

About This Book

HDIM For Dummies consists of six chapters that explore the following:

- » The basics of hybrid digital infrastructure management (Chapter 1)
- » Getting started with your hybrid digital infrastructure strategy (Chapter 2)
- » Implementing key hybrid digital infrastructure capabilities (Chapter 3)

- » Managing day-to-day operations in your hybrid digital infrastructure (Chapter 4)
- » Monitoring performance, compliance, and security in your hybrid digital infrastructure (Chapter 5)
- » Evaluating a data center infrastructure management (DCIM) vendor to maximize the business value of your hybrid digital infrastructure (Chapter 6)

Each chapter is written to stand on its own, so if you see a topic that piques your interest feel free to jump ahead to that chapter. You can read this book in any order that suits you (though I don't recommend upside down or backward).

Foolish Assumptions

It's been said that most assumptions have outlived their usefulness, but I assume a few things nonetheless!

Mainly, I assume that you're an IT professional in an organization that is looking to optimize workload placement and deliver a superior digital experience across its hybrid digital infrastructure footprint. Perhaps you're a data center manager, network manager, IT service manager, infrastructure architect, or cloud architect. As such, this book is written primarily for technical readers.

If any of these assumptions describes you, then this is the book for you! If none of these assumptions describes you, keep reading anyway! It's a great book and after reading it, you'll know how HDIM can help your organization manage its growing hybrid digital infrastructure.

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:



REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays!



TIP

Tips are appreciated, but never expected — and I sure hope you'll appreciate these useful nuggets of information.



WARNING

These alerts point out the stuff your mother warned you about (well, probably not), but they do offer practical advice to help you avoid potentially costly or frustrating mistakes.

Beyond the Book

There's only so much I can cover in this short book, so if you want to learn more, check out <https://nlyte.com>.

IN THIS CHAPTER

- » Looking at on-premises and cloud environments
- » Extending DCIM to hybrid environments
- » Exploring key HDIM activities
- » Understanding the role of DCIM in hybrid digital infrastructure

Chapter 1

Hybrid Digital Infrastructure Management 101

In this chapter, you learn how the enterprise digital estate has morphed into a hybrid combination of on-premises data centers, public cloud services, and more, how data center infrastructure management (DCIM) helps you manage hybrid environments, what you need to do to effectively manage your organization's hybrid digital infrastructure, and how DCIM helps establish the foundation for your hybrid digital infrastructure management (HDIM) solution.

Recognizing Why HDIM Is Needed

Modern businesses demand more data, greater agility, faster performance, and reliable access — but not necessarily “at any cost.” Operating budgets and resources aren't increasing just to meet these demands. In fact, the longstanding mantra to “do more with less” continues to ring true as infrastructure and operations (I&O) teams must address these ever-growing business demands with less money and fewer people.

Not surprisingly, most organizations today have adopted a public cloud strategy to address many of these demands. Migrating certain workloads from their on-premises data centers to a platform as a service (PaaS) or infrastructure as a service (IaaS) public cloud offering enables these organizations to address business demands for on-demand capacity, flexibility, scalability, and reliability. Many core business applications are also being offloaded to the public cloud in software as a service (SaaS) offerings, such as:

- » **Office productivity and collaboration (including email)**, such as Microsoft Office 365 and G Suite by Google Cloud
- » **Customer relationship management (CRM)**, such as Salesforce and Microsoft Dynamics 365
- » **Finance systems**, such as Oracle NetSuite and SAP



TIP

The 2019 *RightScale State of the Cloud Report* from Flexera found that 84 percent of enterprises have a multi-cloud strategy and that organizations use an average of nearly five different clouds.



REMEMBER

To realize the benefits of the cloud in a cost-effective manner, I&O teams must properly manage their public cloud environments.

At the same time, not all workloads can, or should, run in a public cloud. For example:

- » Many custom business applications can't be easily refactored to run in the cloud.
- » High-performance, low-latency performance demands in some applications need the close proximity of an on-premises data center.
- » Strict data governance requirements may limit an organization's public cloud options.

As a result, most organizations today must still run at least some of their workloads in an on-premises data center. To do so more efficiently, these data centers often need to be modernized so they can be operated as private clouds. Many organizations are also beginning to deploy edge computing assets in micro data centers that are purpose-built to support various business use cases, such as remote locations, consumer gaming and media, and the Internet of Things (IoT).

The hybrid digital infrastructure has, thus, evolved, consisting of multiple public clouds, hosted facilities, and on-premises data centers. For I&O teams, managing a hybrid environment creates new challenges that require a comprehensive suite of tools and solutions that extend across all of their operating environments.

Understanding the Evolution of HDIM

The hybrid digital compute infrastructure (sometimes referred to as the hybrid cloud) can be both organic (that is, evolved from numerous disconnected IT projects and initiatives over time) and planned (architected as the desired future state of an organization's IT infrastructure). The intended end state is to have a seamlessly connected digital infrastructure that enables and ensures the optimization of workloads to deliver the best end-user experience and efficient cost management.

HDIM is the next step in the evolution of DCIM. HDIM extends the monitoring, management, automation, optimization, and reporting capabilities of DCIM to the entire hybrid digital infrastructure, which includes on-premises data centers, public clouds, private clouds, and edge clouds (micro data centers). By leveraging a secure, scalable, and open platform, DCIM can manage your entire digital estate including physical assets, digital assets, physical workload placement, human resources, environmental systems, and technical systems (see Figure 1-1).

HDIM involves the integration of tools designed to monitor hybrid environments and includes devices, subnets, domains, data centers, and/or service providers. Its focus is on discovery, monitoring, key performance indicator (KPI) metrics, optimization, dependency mapping, and location of both physical and logical assets.



TIP



REMEMBER

You learn more about DCIM later in this chapter.

Fundamentally, the “cloud” is a delivery model for sharing computing resources across a pool of customers (internal or external) as an on-demand, self-service, rapidly scalable, consumption-based service. However, the “nuts and bolts” of the cloud consists of nuts and bolts, and bricks and mortar, electricity, heating, cooling, equipment racks, servers, and so on. In other words, a cloud is

still a data center that needs to be managed by someone — either an enterprise I&O team (if it's a private cloud) or a cloud provider's I&O team (if it's a public cloud).

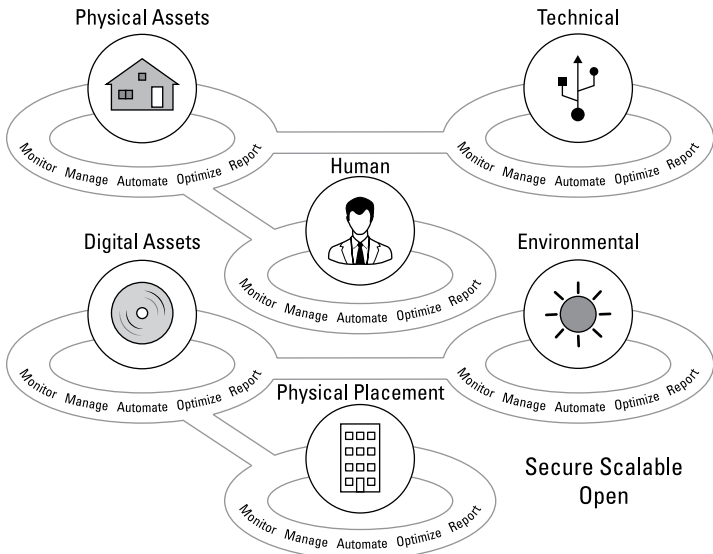


FIGURE 1-1: HDIM is the next step in the evolution of DCIM.

Looking at Key HDIM Components

To successfully maximize the value of a hybrid digital infrastructure, enterprise (and cloud provider) I&O teams must develop their skills and tooling in four key areas:

- » **Organizing** the hybrid digital infrastructure (discussed in Chapter 2) to accurately predict optimal placement of dynamic workloads, ensure high availability and resiliency, and appropriately manage cost effectiveness, operating budgets, security, and supplier relationships
- » **Implementing** the hybrid digital infrastructure (discussed in Chapter 3) through orchestration, standardized self-service catalog offerings, DevOps integration, and auto-discovery of IT assets and their dependencies throughout their life cycles

- » **Operating** the hybrid digital infrastructure (discussed in Chapter 4), including request fulfillment, patching and updating, continuous improvement, fault remediation and root cause analysis, backups and failover, vulnerability and threat assessments, and more
- » **Monitoring** the hybrid digital infrastructure (discussed in Chapter 5) with complete visibility across all environments to maintain licensing and regulatory compliance, ensure adequate performance levels, analyze audit and log data for insights and threats, and deliver a superior user/customer experience

Establishing DCIM as the Cornerstone of HDIM

To effectively monitor today's hybrid digital infrastructure, I&O teams require a complete suite of tools and solutions that provide asset discovery, asset management, facilities insight, power management, machine learning, and workload insight across building management systems (BMSs), on-premises data centers, IT service management (ITSM), public and private clouds, and finance systems. The analytics and workload analysis necessary to deliver effective HDIM is enabled through the capabilities of a robust DCIM platform (see Figure 1-2).

Most organizations today use comprehensive, integrated core business software suites to oversee and manage key aspects of their business, such as sales, finance, manufacturing, and shipping. An organization's digital infrastructure requires this same type of comprehensive, integrated control to ensure the most effective and efficient use of these assets and to deliver maximum business value from its hybrid digital infrastructure.

In simple terms, DCIM is the strategic business management solution for the data center. DCIM is the structured approach to managing change, purpose-built for the modern compute infrastructure — whether physical or virtual, on-premises or in the cloud.

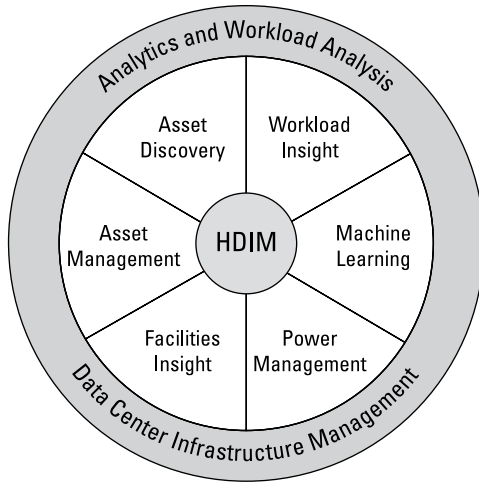


FIGURE 1-2: HDIM provides management and analytics of underlying assets across all infrastructure locations.

In the course of its evolution, DCIM has become a management extension to a number of other systems, including asset and service management, financial and human resource information systems (HRISs), and other core business systems. A well-designed DCIM solution quantifies the costs associated with moving, adding, or changing workloads on the data center floor or in the cloud to ensure optimal workload placement. It understands the cost and complexity of operation of those assets, and clearly identifies the value that each asset provides over its life span.

Figure 1-3 shows how DCIM stands between IT and facilities and joins them together. The physical assets of the facility, such as floor space, electrical power, environmental control, and cooling, are monitored and controlled by DCIM processes, which then interface with the virtual infrastructure overseen by the IT function. The DCIM suite provides an overview of system health and functioning, and also enables drilling down to any desired level of detail for fine-grained control of operations.

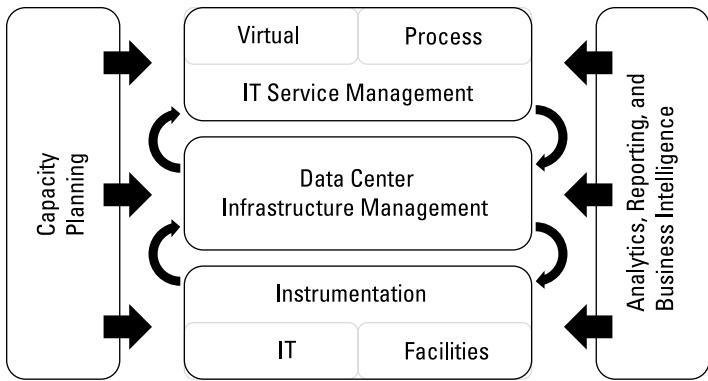


FIGURE 1-3: DCIM works with ITSM and other instrumentation to support capacity planning and analytics, reporting, and business intelligence in a hybrid digital infrastructure.



REMEMBER

Clouds are data centers, too. If you're a cloud service provider, you need DCIM to help manage numerous data centers around the world. If you're an enterprise, you need DCIM to manage your growing hybrid digital infrastructure.

IN THIS CHAPTER

- » Taking stock of your digital assets
- » Creating better budgets for service delivery
- » Thinking about the entire supply chain

Chapter 2

Organizing Your Strategy for Hybrid Digital Infrastructure

In this chapter, you learn about several important areas of hybrid digital infrastructure management (HDIM) that you need to consider as you get organized. These include discovering your digital assets and key asset information, accurately forecasting your budgets to improve service delivery, and ensuring you understand how your various supplier relationships and interrelationships impact your hybrid digital infrastructure.

Taking Inventory of Current Space, Power, Physical, and Digital Assets

It seems only logical that to get organized, you first need to take stock of exactly what it is you're trying to organize. But beyond

knowing what assets you have, you need to know quite a few other things about those assets to effectively manage them, such as:

- »» What assets you have
- »» Where your assets are located
- »» The current state of your assets (including performance, capacity, utilization, security, compliance, and more)
- »» The value of your assets (both cost and business value)
- »» The life cycle of your assets (are they end of life, under maintenance contracts, serviceable, new, and so on)

Of course, accurately collecting and maintaining all of this asset information manually would be impossible, even in the smallest of data centers. Fortunately, there's a solution for that: technology asset management (TAM).



TIP

Download a copy of *IT Asset Management For Dummies* at <https://nlyte.com/resource-type/ebooks>.

IT asset management (ITAM) traditionally included assets such as servers, mainframes, routers, switches, firewalls, desktop and laptop computers, printers, and software — all things managed by IT. But technology no longer only consists of IT assets. Today, there are non-IT assets in organizations everywhere. With the rise of the Internet of Things (IoT), technology is pervasive in things such as heating, ventilation, and air-conditioning (HVAC) systems, devices and sensors, security cameras, medical devices, and more — all connected to the Internet and owned by different areas of the business. Thus, ITAM has expanded and evolved to become TAM.



REMEMBER

TAM is a superset of asset management that includes all the technology across an organization's hybrid digital infrastructure. It includes physical, virtual, and software assets such as networked building infrastructure, data center infrastructure, applications and data in the cloud, personal computing devices, printers, scanners, and millions of IoT devices. TAM enables an organization to discover, manage, secure, and report on all its technology assets — from IT to IoT devices and any other technology assets in its hybrid digital infrastructure.

Successful TAM requires a solution that is agnostic to the types of technology, devices, and operating systems that an organization may own and use. Such a TAM solution must be capable of

collecting all the available information about your organization's technology assets and their configuration items (CIs) in a single, trusted, unified, and normalized source of truth (or system of record).

A modern approach to TAM automates the discovery and cataloging of all things in the hybrid digital infrastructure. It interconnects with other building, IT, and business systems providing a single source of knowledge, bringing transparency and accountability to the entire extended organization.

A TAM solution helps reduce your technology spending and improve efficiency by identifying underused assets, thereby enabling reallocation, consolidation, and/or retirement. A TAM solution also reduces risk across the organization by tracking and reporting on what assets you have, their configuration, who is using them, when they last touched the network, and what resources they're consuming. By integrating this knowledge with other business systems like human resources information systems (HRISs), enterprise resource planning (ERP), security, and data center infrastructure management (DCIM), you gain a complete and accurate picture across your entire hybrid digital infrastructure.

NLYTE ASSET EXPLORER

Nlyte's Asset Explorer software is a next-generation ITAM solution extending its discovery, inventory, and business intelligence engine to include facilities and IoT infrastructure and devices. Asset Explorer is a complete solution set that automatically collects and provides detailed information about every device connected to the network. The solution includes all the tools and technology to identify and visualize the results of the discovered assets — configuration attributes, services/processes, network connections, and applications.

Asset Explorer delivers the definitive source of truth for all other IT and business systems. Being agentless and protocol agnostic, Asset Explorer automatically discovers and inventories everything running on the network, delivering a complete technology asset baseline. With the ability to collect hundreds of data points per asset, the business intelligence engine delivers rich information for finance, compliance, security, and IT applications.

(continued)

(continued)

Key capabilities include the following:

- **Financial reconciliation/cost management:** Transparently and accurately manage license, support, and maintenance expenses; reconcile asset database(s) against ERP and fixed asset system; validate life-cycle disposition of any technology asset (installed, end of life, ghost); consolidate/reduce tools and systems to collect and report (single source of truth).
- **Compliance/security/risk mitigation:** Deliver asset integrity by validating all access and change against IT and compliance policies; increase digital and access security by monitoring authorized/unauthorized changes and patch validation; improve regulatory compliance with accurate up-to-date audit trail and change management validation; ensure accountability for General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standards (PCI DSS), International Organization for Standardization (ISO), and internal policies.
- **IT operations/automation/service-level agreement (SLA) improvement:** Simplify and automate asset data collection, inventory, and life-cycle management; improve service-desk SLA metrics and increase troubleshooting effectiveness with current validated asset location and configuration; meet disaster recovery and business continuity recovery time objectives (RTOs) with accurate asset inventory and configurations at time of failure; achieve a self-aware data center with automated asset discovery improving configuration management database (CMDB) accuracy; reduce manual activities associated with auditing, reporting, and workflow validation.

TAM and Asset Explorer are critical to automating DCIM (and HDIM):

- A TAM solution like Asset Explorer automates nearly everything, from finding and inventorying assets, creating them in the DCIM asset database, and continuously checking for changes across the network.
- The solution automates the association of servers and networks to network ports, providing you a port-to-port mapping of all active network connections.

- This enhanced automation manages the ingestion, in real-time, of bulk data from scans and external data sources such as Excel and CMDBs.
- Communication between other dependent and critical systems occurs automatically, with this next-generation solution acting as the single source of truth; CMDBs, ticketing systems, building management systems (BMSs), and fixed asset databases are all working with the same current data.
- Workflows are automatically generated based on business rules; the progression, tracking, reporting, and systems updates are also automated.

Forecasting Budgets for Service Delivery

Forecasting budgets has historically been a zero-sum game. Or rather, budgets have typically been created using either a historical cost basis (for example, to develop an incremental or activity-based budget) or zero-based. Often, the results of either of these approaches to budgeting are not as accurate or reliable as your CFO would prefer.

As is the case with personal investing, the warning that “past performance does not guarantee future results” holds true for historical cost methods. At its most basic level, historical budgets are created by looking at the capital expenditures (CapEx) and operating expenditures (OpEx) for a department during the previous budget period (for example, last year or last quarter) and adding a flat rate (for example, 2 percent or 3 percent) for cost increases (again, as in our personal lives, costs never seem to do down — only up!).

Zero-based budgeting can be very effective in helping an organization control costs by requiring departments to start at the bottom (“zero”) and justify any costs or investments to build their budgets. However, zero-based budgeting can be very time-consuming to create and often falls back on historical cost information to build. Zero-based budgeting is also typically not used for operating expenses, which constitute an ever-growing

portion of IT budgets as organizations leverage the cloud to shift their technology spend from CapEx to OpEx.

As the cornerstone of HDIM, DCIM helps an organization plan and prepare its budgets across the entire hybrid digital infrastructure. Technology asset baselines can be used to gain a better understanding of capacity and utilization of compute and storage resources across multiple on-premises data centers and public cloud environments. This information can also be used to help an organization take advantage of reserved instances, for example, instead of pay-as-you-go or on-demand pricing in Microsoft Azure or Amazon Web Services (AWS). Some organizations, equipped with granular technology asset baseline information, may even be able to leverage AWS spot pricing to cost-effectively bid on spare compute capacity at a given price point.



TIP

Although workload placement decisions typically focus on performance optimization, cost can also be a factor to consider when determining which data center or cloud should run a given workload.

Considering Supplier Relationships and Interrelationships

In a global economy, it only makes sense that organizations have become more dependent on the global supply chain than ever before. Cloud providers own or lease numerous data centers in different countries and regions around the world and must rely on various local services to keep those data centers running. Likewise, enterprises rely on various local services to provide power, cooling, telecommunications, and maintenance services, among others, in their on-premises and hosted data centers.

To effectively manage critical and increasingly complex supplier relationships and interrelationships, organizations need a secure, open, and scalable DCIM platform that can be integrated with a multitude of different systems. This capability helps enterprise

I&O teams successfully manage security, costs, and SLA performance across the hybrid digital infrastructure.



WARNING

Many high-profile cyberattacks and data breaches have targeted vulnerabilities in an organization's ancillary systems or third-party systems in their supply chain. The 2013 Target breach used stolen credentials from an HVAC maintenance company. More recently, the 2019 Quest Diagnostics breach targeted a third-party billing collections vendor to gain access to customer information.



TIP

It is unlikely that a single vendor will provide 100 percent of the technology needed to deliver all the functions needed in the HDIM architecture. However, every technology vendor needs to ensure that its solutions provide transparency and data access for every other solution in the architecture.

When selecting a DCIM vendor as part of your HDIM tool set, look for a broad ecosystem of third-party vendors and partners that offer out-of-the-box integrations with the DCIM solution. Also, look for open, secure application programming interfaces (APIs) to build custom integrations when out-of-the-box integrations to your DCIM solution aren't available from certain vendors.

Key attributes that any DCIM or HDIM vendor's solution should have include the following:

- » Automation of tedious, time-consuming, and redundant tasks to free up staff to work on more strategic projects
- » Machine learning and artificial intelligence (AI) to process the millions of continuous inputs that can provide valuable insight to managing your infrastructure, greatly reducing risk, and providing data for workload optimization
- » Hyper-scalability in all components of an HDIM solution to manage the scale and complexity of the infrastructure
- » Centralized management of remote locations and the ability to centrally monitor and manage various locations, including "lights out" environments

NLYTE COMMAND CENTER

Nlyte Command Center works in harmony with Nlyte Energy Optimizer to enable operators to control facility and IT devices locally or remotely within a dark site. It visualizes, manages, and reports on the compute infrastructure across and outside the extended organization, obviating the need for costly on-site human presence. Key capabilities of Command Center include the following:

- Enabling credentialed personnel to log in and perform specific tasks on individual end devices from a remote location
- Providing power cycling of assets that have frozen or need to be hard-booted
- Remotely managing physical access by locking/unlocking cabinets
- Allowing authorized personnel to make changes to environmental systems, such as changing fan speeds or adjusting set points
- Extending capabilities to data centers, data rooms, remote facilities, and colocation footprints

IN THIS CHAPTER

- » Keeping up with constant change
- » Mapping dependencies across your hybrid digital infrastructure
- » Using TAM to automate DCIM
- » Making self-service easier for your users and customers
- » Enabling continuous integration and continuous deployment

Chapter 3

Implementing Your Hybrid Digital Infrastructure

In this chapter, you learn how a properly implemented data center infrastructure management (DCIM) platform supports automation and orchestration, asset discovery and dependency mapping, self-service through your service catalog, and DevOps pipelines across a hybrid digital infrastructure.

Leveraging Automation and Orchestration

A key characteristic of the hybrid digital infrastructure is the velocity of change across the environment. Change is now constant, particularly in highly dynamic DevOps (discussed later in this chapter) and cloud environments. The once-utopian “steady state” has become an idealistic relic of the past.

The only way for enterprise infrastructure and operations (I&O) teams to keep up with the pace of change and effectively manage a hybrid digital infrastructure is to maximize automation and orchestration in their processes and workflows.

Key areas that should be automated in your hybrid infrastructure include the following:

- » **Asset discovery and inventory:** The automation should start at the receiving dock, continue during the production life of assets, checking for moves and changes and through decommissioning. By eliminating the time-consuming tasks of physically looking for and identifying both visible and out-of-sight attributes (such as obscure serial number tags), many valuable staff hours can be put to better use.
- » **Workflow management:** Standard business processes and workflows needs to be coordinated between various groups and automated. Relying on individuals and multiple groups to manually update IT service tickets is problematic and creates unnecessary delays. With automated workflow tracking, teams know precisely when a task is complete, and the next step can begin immediately, thereby saving time, increasing efficiency, and eliminating delays. Additionally, the automation provides a critical audit trail to assist in IT process management and compliance reporting.
- » **Report processing:** Building custom reports that require programming skills and extensive manual effort tends to result in many potentially important or valuable reports not getting created at all — at least not in a timely or effective manner. Automated reports deliver critical information in a timely fashion, so action can be taken on anomalies and compliance reporting doesn't become cumbersome.

Discovering IT Assets and Dependencies

As discussed in Chapter 2, technology asset management (TAM) helps you inventory technology assets across your entire hybrid digital infrastructure. However, an inventory quickly becomes

outdated — particularly in a rapidly evolving hybrid digital infrastructure — and needs to be continuously refreshed through automated discovery of new assets and removal of decommissioned or otherwise deprecated assets.

Cloud-native technologies further complicate this task because many assets, such as a microservice or container instances, are ephemeral by nature and may only exist for a few minutes or seconds — just long enough to perform a specific function or address a brief period of peak demand.

NLYTE ASSET OPTIMIZER

Nlyte Asset Optimizer (NAO) is key to any DCIM solution. NAO is an open and scalable platform that provides automation and efficiency to asset life-cycle management, capacity planning, audit, and compliance tracking. NAO easily manages assets from receiving dock to decommissioning, globally or rack by rack. It simplifies space and energy planning and easily connects to IT service management (ITSM) and other business intelligence (BI) applications.

Effective oversight and management of IT assets, resources, and processes is indispensable. NAO automates DCIM workflows and IT integrations. Many of the world's largest and most sophisticated data centers rely on Nlyte to manage all of their existing data center processes, resources, assets, and interrelationships. As a result, they become more agile, reduce costs, and operate more efficiently. Ultimately, Nlyte empowers CIOs and CTOs to turn their data centers from cost bearers into centers of excellence.

Key capabilities and benefits include the following:

- **Asset life-cycle management:** Real-time reporting on assets, per data center per customer mapping to each life-cycle stage, facilitating warranty renewals, and maintenance contracts; real-time, accurate asset inventory audits for compliance and yearly maintenance reconciliation; the ability to report using a charge-back model; immediate recognition upon asset arrival at your facility, thus avoiding spending on uninstalled assets.

(continued)

(continued)

- **Audit and compliance:** Secure direct support for audit, regulatory, and fiscal compliance; Health Insurance Portability and Accountability Act (HIPAA), Sarbanes–Oxley (SOX), Regulation Systems Compliance and Integrity (SCI), and Data Center Optimization Initiative (DCOI) compliant; capture change to the data center automatically to improve data accuracy and reliability; update the Nlyte Content Database asset information in real-time as changes occur; improve your financial management of IT assets by getting an accurate reflection of asset inventory.
- **Capacity planning:** Improved capacity planning and project life-cycle management; proactive versus reactive data center management; accurate data center life-span prediction (assess when you need additional capacity and when you don't).
- **Change management connectors:** Save time and effort while lowering risk by coordinating two otherwise disparate change request systems as one; enable faster moves, adds, and changes by allowing preplanning for asset life-cycle management; gain faster root-cause analysis and improved event correlation as asset locations and applications become visible to ITSM.
- **Configuration management database (CMDB) connectors:** Enrich your CMDB with more data for truer capacity planning; gain a federated view (one version of the truth for configuration item attributes); improve compliance by knowing where assets are, who worked on them last, and what was done.
- **Cost savings and return on investment (ROI):** Quantify the cost associated with moving, adding, or changing data center equipment; obtain a full range of financial and operational metrics to measure and track improvements; justify DCIM investment and achieve faster ROI.
- **Migrations and consolidations:** Reduce the cost, time, and risk of migrations and consolidations; obtain easy capacity planning required to support moves and changes; establish a pre-move baseline to measure success; visualize and model the entire process from start to end.
- **Operational efficiency:** Optimize your resources and personnel with measurable, repeatable intelligent processes; make individuals more efficient by providing task focus and progress status; support cross-team assignment for tasks shared by multiple teams;

extend the adoption of ITIL and Control Objectives for Information Technologies (COBIT) into the data center without any additional development or service.

- **Tech refresh:** Facilitate the tech refresh process by automating manual tasks; improve flexibility to move workloads as needed via intelligent asset provisioning and workflow management; improve warranty and lease management to avoid paying “overtime.”
- **Virtualization connectors:** Reduced complexity and cost of managing a virtualized data center. Track changes automatically and continuously as virtual machines (VMs) migrate; increased control and optimization of both physical and virtual resources, avoiding multiple management systems, manual and time-consuming processes to coordinate the views; clear identification of guests and hosts during outages and support to assure that affected applications have contingency plans.

Automating DCIM

By automating DCIM with a TAM solution, your organization can now work with one data set — the single source of truth for other dependent systems across the entire hybrid digital infrastructure.

This new automation improves your risk management, helping to prevent unplanned disruptions by ensuring all teams and systems have the most current and accurate data. It delivers consistent adherence to operational procedures and provides accurate audit trails and reporting when things occur that are out of compliance.

Network automation gives visibility to port utilizations, their relationship to an asset, and what happens if the connection is broken. The automated tracking of an application’s workload dependencies on power, compute resources, and network connections delivers the next step toward the ultimate goal of true application workload optimization.

Standardizing Catalog Offerings

Providing your users and customers with more options provides greater flexibility but can also confuse and overwhelm them. This can quickly become the case in a hybrid digital infrastructure that

offers, for example, a dizzying array of infrastructure as a service (IaaS) virtual machine offerings of different sizes, speeds, and operating systems.

By helping you organize your hybrid digital infrastructure (see Chapter 2), DCIM can provide you the information you need to categorize and then standardize your service catalog offerings and present them in a manner that helps your users and customers identify their options and select the best solution to meet their needs.

Supporting DevOps Pipelines

Organizations everywhere are embracing DevOps to enable their developers to rapidly create infrastructure as code to support new projects. Cloud-native technologies, such as containers and Kubernetes orchestration, enable self-service at massive scale (for example, hundreds of pods or scale set instances within a Kubernetes cluster) for DevOps teams.

Although these infrastructure assets are often short-lived and rapidly evolving, costs can quickly escalate if the DevOps environment is not properly managed. Orphaned assets can quickly consume a project budget, as velocity often supersedes proper infrastructure life-cycle management, particularly in a public cloud environment.

DCIM supports DevOps pipelines through automated discovery of highly dynamic infrastructure assets, including configuration changes and life-cycle management.

IN THIS CHAPTER

- » Fulfilling service requests and keeping systems up to date
- » Driving continuous improvement
- » Automating IT operations
- » Enhancing backup and failover
- » Keeping the hybrid digital infrastructure safe
- » Supporting decision-making and actionable insights at all levels

Chapter 4

Operating Your Hybrid Digital Infrastructure

In this chapter, you learn how data center infrastructure management (DCIM) supports the efficient operation of your hybrid digital infrastructure, including service request fulfillment, continuous improvement initiatives, automation of IT operations tasks, business continuity and disaster recovery, security, and auditing and reporting.

Ensuring Timely Request Fulfillment, Patching, and Updating

It's easy to forget in the on-demand, self-service cloud era, but there are still plenty of service requests that require the human touch — and not just any human, but the skills and experience of an IT professional. In a hybrid digital infrastructure, the scale and scope of service requests increases drastically.

To ensure timely request fulfillment, your IT service management (ITSM) solution should be tightly integrated with your

DCIM platform as part of your overall hybrid digital infrastructure management (HDIM) tool set. An integrated ITSM solution can leverage the technology asset management (TAM) database in DCIM as a single source of truth for configuration items (CIs) across the environment.

Similarly, your configuration management database (CDB) can leverage your TAM database to ensure all your systems and devices are properly patched and updated to ensure your applications, systems, and users are protected from the latest threats and able to take advantage of the latest features and capabilities available.

Enabling Continuous Improvement

The goal of business agility in the modern hybrid digital infrastructure is to enable rapid innovation and accelerate time-to-market. Of course, not all innovation is necessarily an improvement, but there's an implicit expectation that change is good, so you need to operate your hybrid digital infrastructure in a manner that supports and enables continuous improvement throughout the organization.

Leveraging AIOps

AIOps uses artificial intelligence (AI) and machine learning technology to automate and orchestrate IT operations functions within a hybrid digital infrastructure. AIOps enables organizations to avoid risk, reduce overhead, eliminate manual errors, optimize performance, and improve their maintenance strategies.

Key AIOps use cases include the following:

» Predictive power and thermal analytics

- Understand patterns and automatically raise and lower data center temperatures accordingly.
- Accurately plan future power needs.
- Improve server density in equipment racks and data centers.

» Workload/hybrid compute optimization

- Improve power usage effectiveness (PUE) and reduce your carbon footprint.

- Identify optimum compute environments for application workloads.
- Plan dynamic workload migrations and repatriations.

» **Placement optimization**

- Install equipment based on thermal, power, communications, and application vectors.
- Improve space and power efficiency.
- Build out a future-ready compute infrastructure.

» **Multi-variate maintenance and failure prediction**

- Analyze granular information for component detail and application history.
- Enhance preventive maintenance routines.
- Refine failure prediction.

» **Alarm and alert management**

- Intelligently filter alarms and alerts.
- Prioritize significant events, either stand-alone or in complex chains.

Managing Backups and Failover Activities

Organizations have greatly matured their backup processes and disaster recovery plans over the past two decades. However, many organizations have not updated these processes and plans to address the challenges of a hybrid digital infrastructure.

On the other side of the coin, many organizations have not taken advantage of the new capabilities and opportunities that a hybrid digital infrastructure brings to their backup and failover activities. For example, organizations are increasingly leveraging cloud-based backups to replace manual off-site storage of backups. Other opportunities might include geo-replication of critical systems and data to separate regions within the public cloud, full simulation disaster recovery tests in a cloud environment, and other business continuity/disaster recovery capabilities.

Addressing Threats, Vulnerabilities, and Risks

The hybrid digital infrastructure enables new opportunities, as well as new threats, vulnerabilities, and risks. Operating your hybrid digital infrastructure in a secure manner requires comprehensive real-time visibility of your entire environment to enable actionable insights, mitigation, and remediation against fast-moving threats and attacks.

As a cornerstone of HDIM, a DCIM platform provides much of the visibility that organizations need across a greatly expanded attack surface that includes not only on-premises data centers, hosted facilities, and public cloud environments, but also building management systems (BMSs), industrial control systems, specialized medical equipment, Internet of Things (IoT) devices, and more.

NLYTE MACHINE LEARNING

Nlyte Machine Learning, powered by IBM Watson IoT, combines Nlyte's solution for managing data center energy infrastructure, Nlyte Energy Optimizer, with the premier machine learning engine of IBM Watson IoT. Tightly integrated, these two solutions enable organizations to rapidly capture, normalize, and analyze large amounts of data to optimize operations and head off potential issues and outages before they happen.

The benefits of Nlyte Machine Learning include the following:

- Risk avoidance
- Overhead reduction
- Performance optimization
- Improve maintenance strategies

Nlyte Machine Learning powered by Watson IoT is a purpose-built framework, developed by two leaders in AI and data center management, IBM and Nlyte. It addresses scale, complexity, and optimization requirements of modern data centers. Nlyte Machine Learning is easy to adopt, leveraging data already generated by sensors, critical infrastructure, IT equipment, and applications. There is a complete framework including data collection, patterns for predictive power and thermal, and command-and-control actions from analytics reporting, as well as tooling for custom pattern development.

Here are the key use cases for Nlyte Machine Learning:

- **Predictive power and thermal:** Understand patterns that allow you to raise and lower data center temperatures appropriately; plan accurately for future power needs; improve server density and rack space utilization.
- **Workload/hybrid compute optimization:** Improve power usage effectiveness (PUE) and reduce carbon footprint; identify optimum compute environments for application workloads; plan dynamic workload migrations and repatriations.
- **Placement optimization:** Install equipment based on thermal, power, communications, and application vectors; improve space and power efficiency; build out a future-ready compute infrastructure.
- **Multi-variate maintenance and failure prediction:** Granular information for component detail and application history; enhance preventative maintenance routines; refine failure prediction.
- **Alarm and alert management:** Intelligently filter alarms and alerts; prioritize significant events, either stand-alone or in complex chains.

Communicating Business Value

DCIM provides a single source of truth in a single management console for a variety of users and use cases. This access to real-time information supports better decision-making throughout the organization. For example, information in your DCIM can be used by for ITSM, change control, compliance auditing, asset control, financial reporting, facilities and maintenance management, and more.



TIP

With an automated DCIM solution as the cornerstone of your HDIM solution, you'll experience increased operational efficiencies, including the following:

- » Reduced costs
- » Freed-up resources
- » Greater cybersecurity
- » Improved data accuracy and enrichment
- » A single source of truth for all systems
- » Enhanced visibility of out-of-process changes providing increased security management

NLYTE ENERGY OPTIMIZER

Nlyte Energy Optimizer (NEO) can ensure IT service continuity, driving real-time analytics into ITSM ecosystems. The breadth and depth of Nlyte's offerings provides unmatched visibility, insight, and solutions into all aspects of your monitoring and alarming needs.

NEO allows for different types of devices to be monitored by the application through industry-standard protocols such as:

- Simple Network Management Protocol (SNMP)
- Modbus Remote Terminal Unit (RTU)
- Modbus Transmission Control Protocol (TCP)
- Building automation and control network (BACnet)
- Object linking and embedding (OLE) for process control (OPC)
- Extensible Markup Language (XML)

Each device, based on the communications protocol, can be configured within NEO to monitor functions or "points." A point is any value or status from a device or other object being polled by the application that is being monitored and trended within the NEO application. Depending on the protocol, the combination of an Internet Protocol (IP) address, Object Identifier (OID), or slave ID is assigned to each device so that a network connection can be made and the selected points can be captured by the polling engine.

Devices typically monitored with NEO include the following:

- Uninterruptible power supply (UPS)
- Computer room air conditioning (CRAC) and computer room air handlers (CRAHs)
- Power meters
- In-rack power strips
- Floor-standing power distribution units (PDUs)
- Environmental sensors
- Branch circuit monitoring
- Any device using a supported protocol

IN THIS CHAPTER

- » Seeing the complete hybrid digital infrastructure picture
- » Managing licensing and regulatory compliance
- » Ensuring network performance
- » Keeping the environment secure
- » Providing a superior digital experience
- » Making the right workload placement decisions

Chapter 5

Monitoring Your Hybrid Digital Infrastructure

In this chapter, you look at the importance of monitoring your hybrid digital infrastructure to ensure you have comprehensive visibility and can effectively address compliance, performance, security, user experience, and workload optimization issues.

Getting Visibility into the End-to-End Environment

Visibility seems to be a challenge in practically any IT environment today, whether the focus is compliance, performance, security, user experience, or cost.

A data center infrastructure management (DCIM) platform is uniquely positioned in hybrid digital infrastructure management (HDIM) to provide comprehensive, end-to-end visibility of the entire environment. DCIM provides the level of data and detail necessary to gain deep analytical insights and support real-time

decision-making for a variety of use cases and users from IT service management (ITSM) to facilities management and more.

DCIM functions as the single source of truth for an organization's hybrid digital infrastructure by integrating with disparate applications, systems, and devices regardless of location, vendor, or protocol.

Validating Licensing and Regulatory Compliance

Much like HDIM, licensing and regulatory compliance hasn't gotten any easier. It's important to continue monitoring the proliferation of assets, especially software assets. Software is easily copied, and in a DevOps environment, entitlement abuse is more common than not. As software and its workloads move about the hybrid infrastructure, the ability to "find" it is critical for maintaining compliance. Although technology asset management (TAM) software does not deliver a complete software asset management (SAM) solution, its discovery and inventory functionality delivers the critical metadata to a full SAM accounting software package. Data that is relayed from a TAM solution such as Nlyte's Asset Explorer include:

- »» What software is being used and for what purposes
- »» Where software is installed
- »» Who is using the software
- »» How extensively the software is being used

With this information in hand, organizations are better able to track and manage the proliferation of software across their hybrid digital infrastructure.



TIP

SAM technology can help you identify opportunities to save on software licensing, support, maintenance, and other costs.

SAM helps organizations:

- »» Gain complete visibility of the software that is installed in their hybrid digital infrastructure
- »» Understand who is entitled to use installed software and what services are being delivered

Similarly, the ever-growing regulatory landscape presents many new challenges for organizations in every industry around the world. In many cases, a hybrid digital infrastructure — and all the accompanying supplier relationships and interrelationships (discussed in Chapter 2) — expands the scope of regulatory compliance requirements for many organizations.

Some examples of relevant regulations and industry standards that must be managed in a hybrid digital infrastructure might include the following:

- » European Union (EU) General Data Protection Regulation (GDPR)
- » U.S. Data Center Optimization Initiative (DCOI)
- » U.S. Health Insurance Portability and Accountability Act (HIPAA)
- » U.S. Sarbanes–Oxley (SOX) Act
- » Payment Card Industry Data Security Standards (PCI DSS)



TIP

Download a copy of *DCOI For Dummies* at <https://nlyte.com/resource-type/ebooks>.

MANAGING THE U.S. FEDERAL GOVERNMENT'S HYBRID DIGITAL INFRASTRUCTURE

The U.S. federal government owns more computing power than any other country or entity of any kind in the world. Most of this computing power is spread throughout the United States in thousands of data centers ranging in size from a rack tucked away in a closet to a massive collection of servers in a building occupying more than a million square feet of floor space. Additionally, the U.S. federal government leverages public cloud offerings such as Amazon Web Services (AWS) and Microsoft Azure. To manage this massive hybrid digital infrastructure, federal agencies must now comply with an updated DCOI

(continued)

(continued)

mandate and two additional executive orders that together form the three pillars of government modernization and optimization:

DCOI

The updated DCOI provides greater alignment to the Application Rationalization and Cloud Smart initiatives by recognizing the importance of considering applications running in agency data centers rather than focusing on the infrastructure alone.

The DCOI now provides greater purview to individual agencies for application and workload placement decisions and encourages greater adoption of virtualization, containerization, and cloud computing consistent with the Application Rationalization and Cloud Smart mandates.

The DCOI also now requires the implementation of a DCIM solution. DCIM is critical to understanding the cost of the facility, as well as to extrapolate the cost of each workload within the facility. With this understanding, informed decisions can be made about optimally placing or ultimately continuing the use of a given application.

Application Rationalization

The goals of the Application Rationalization initiative include the following:

- To help federal agencies mature their IT portfolio management capabilities
- To empower leaders to make informed decisions
- To improve the delivery of key mission and business services

The Application Rationalization Playbook, developed by the CIO Council and the Cloud and Infrastructure Community of Practice, lays out a structured, six-step iterative approach to application rationalization, as follows:

- Identify needs and set governance.
- Take an inventory of your applications.
- Assess the business value and technical fit of the applications in your portfolio.

- Assess the total cost of ownership (TCO).
- Score applications.
- Determine application placement.

Cloud Smart

Cloud Smart, issued by the Office of Management and Budget (OMB) in June 2019, is an update to the Cloud First Federal Cloud Computing Strategy.

Cloud Smart gives agencies broad authority to evaluate their cloud computing options based on their individual service and mission needs, unique technical requirements, and any existing policy limitations. Cloud Smart promotes a culture of continuous improvement and learning by embracing modernization as a constant state of change rather than a periodic refresh activity, and a leadership focus on staff training and education, migration planning, and striking a balance between solution sustainability and implementation of new capabilities.

DCOI was initiated as a U.S. federal government requirement, but it's important to note that in Europe, both the European Union and national governments are calling for enterprise organizations to provide similar or more stringent accountability for their environmental impact and optimization of their digital infrastructures. A similar trend in the United States is happening with regard to corporate responsibility and shareholder transparency. As the hybrid digital infrastructure continues to grow in complexity, it will be ever more important for DCIM to provide the necessary checks, balances, and reporting to accommodate the need for an accurate accountability of an organization's efficiency and optimization progress.

Analyzing Network and Infrastructure Performance

A DCIM platform can automatically capture detailed network information and accurately reconcile that information into the core HDIM solution — updating all assets adds/moves/changes and attributes without human intervention. This reduces the overhead of keeping complex networking information up to date while also reducing inaccuracies due to human error. With this

advanced capability, infrastructure and operations (I&O) teams can free up hundreds of hours of time to work on higher-value tasks while ensuring anyone accessing the data has accurate and current information.

Although many stand-alone solutions — such as application performance monitoring (APM), network performance monitoring (NPM), and end-user experience (EUE) monitoring — may provide similar visibility into network and infrastructure performance, this data is often siloed and available only to certain IT teams within the organization. Other solutions such as network packet sniffers and protocol analyzers produce raw network data that requires further correlation and analysis to become actionable.

Gaining Security Insights from Audit and Log Data

Many security solutions provide valuable audit and log data about various aspects of a hybrid digital infrastructure. For example, a firewall may provide information about what network traffic is allowed or blocked at a data center or other network perimeter; anti-malware software may provide insights into what viruses, ransomware, and other malware are targeting your endpoints; and a web application firewall may uncover vulnerabilities that are being probed within an application stack by an attacker.

Often, security events and alerts are aggregated and analyzed within a security information and event management (SIEM) solution. Similarly, DCIM can provide valuable security information that can be consumed within the DCIM console or integrated with a SIEM to provide valuable insights into operational technology and other nontraditional IT systems and applications.

Delivering a Superior Digital Experience

Ultimately, a key goal of HDIM is to deliver a superior digital experience. Although a hybrid digital infrastructure enables organizations to leverage the best-of-breed technologies they need,

where they need them to deliver that experience, the inevitable complexity that comes with a hybrid environment can inhibit or even prevent the realization of a superior digital experience for your users and customers.

Effectively monitoring your hybrid digital infrastructure to deliver a superior digital experience requires an organization to establish key performance indicators (KPIs) and other meaningful and objective metrics.

Optimizing Workload Placement

Effective monitoring also enables organizations to optimize workload performance within their hybrid digital infrastructure based on a variety of considerations, including performance, latency, security, cost, and others.

NLYTE SYSTEM UTILIZATION MONITORING

As data centers grow in scale and complexity, it's no longer sufficient to only monitor space, power, and cooling. System utilization, or the lack of it, is increasingly being scrutinized as enterprises routinely discover upwards of 20 percent "ghost servers" that idly consume energy but serve no business function.

Nlyte System Utilization Monitoring (N-SUM) extends real-time monitoring throughout the data center from the facilities layers and across the IT stack, providing the first end-to-end real-time utilization view.

N-SUM is a highly scalable monitoring solution that enables customers to understand system utilization levels across the enterprise as a whole and down to specific assets.

Ultimately, N-SUM empowers all infrastructure managers to leverage a comprehensive set of data to better eliminate waste, increase uptime, and ultimately meet or exceed their service-level agreement (SLA) objectives.

IN THIS CHAPTER

- » Supporting out-of-the-box integrations
- » Providing robust what-if scenario planning capabilities
- » Enabling comprehensive cost management
- » Leveraging artificial intelligence and machine learning
- » Maximizing options with an agentless, vendor- and protocol-agnostic platform
- » Building custom integrations and automated workflows
- » Avoiding vendor lock-in with an open system
- » Empowering different teams and use cases from a single console

Chapter 6

Ten (Or So) Questions to Ask a DCIM Vendor

Here are some important questions to ask your vendor when looking at a DCIM solution — the cornerstone of hybrid digital infrastructure management:

- » **Do you provide out-of-the-box integration, aggregation, and brokering of data across building management systems (BMSs), IT service management (ITSM), cloud management, finance, and other business intelligence (BI) systems?** Your HDIM solution tool set needs to be able to exchange information easily with your existing (or planned) systems, including BMS (such as Honeywell,

Johnson Controls, and Schneider Electric), ITSM (such as BMC, HPE, and ServiceNow), cloud management (such as Flexera, Scalr, and VMware), finance (such as Microsoft Dynamics 365, Oracle NetSuite, and SAP), and BI (such as MicroStrategy, Sisense, and Tableau). Make sure the integration capabilities that you need will be available.

» **Does your solution provide impact analysis and what-if scenario planning against impacted/specific workloads?**

Look for a solution that leverages big data analytics, artificial intelligence (AI), and machine learning capabilities to provide impact analysis and what-if scenario planning for various business continuity, disaster recovery, workload placement, and capacity planning scenarios.

» **Can your solution provide cost management across the entire digital infrastructure, including space, power, leased facilities, and cloud?**

According to the 2019 *RightScale State of the Cloud Report* from Flexera, managing cloud spend is the top challenge for 84 percent of enterprises and cloud cost optimization is their top priority. However, cloud spend is only one element of your hybrid digital infrastructure portfolio. Ensure you have complete insight into your on-premises data centers and hosted facilities costs, including space and power. If you're a cloud service provider, look for a DCIM solution that provides you the necessary information to effectively manage your costs across potentially thousands of data centers around the world.

» **To what extent do you use machine learning and artificial intelligence (AI) to provide predictive analytics?**

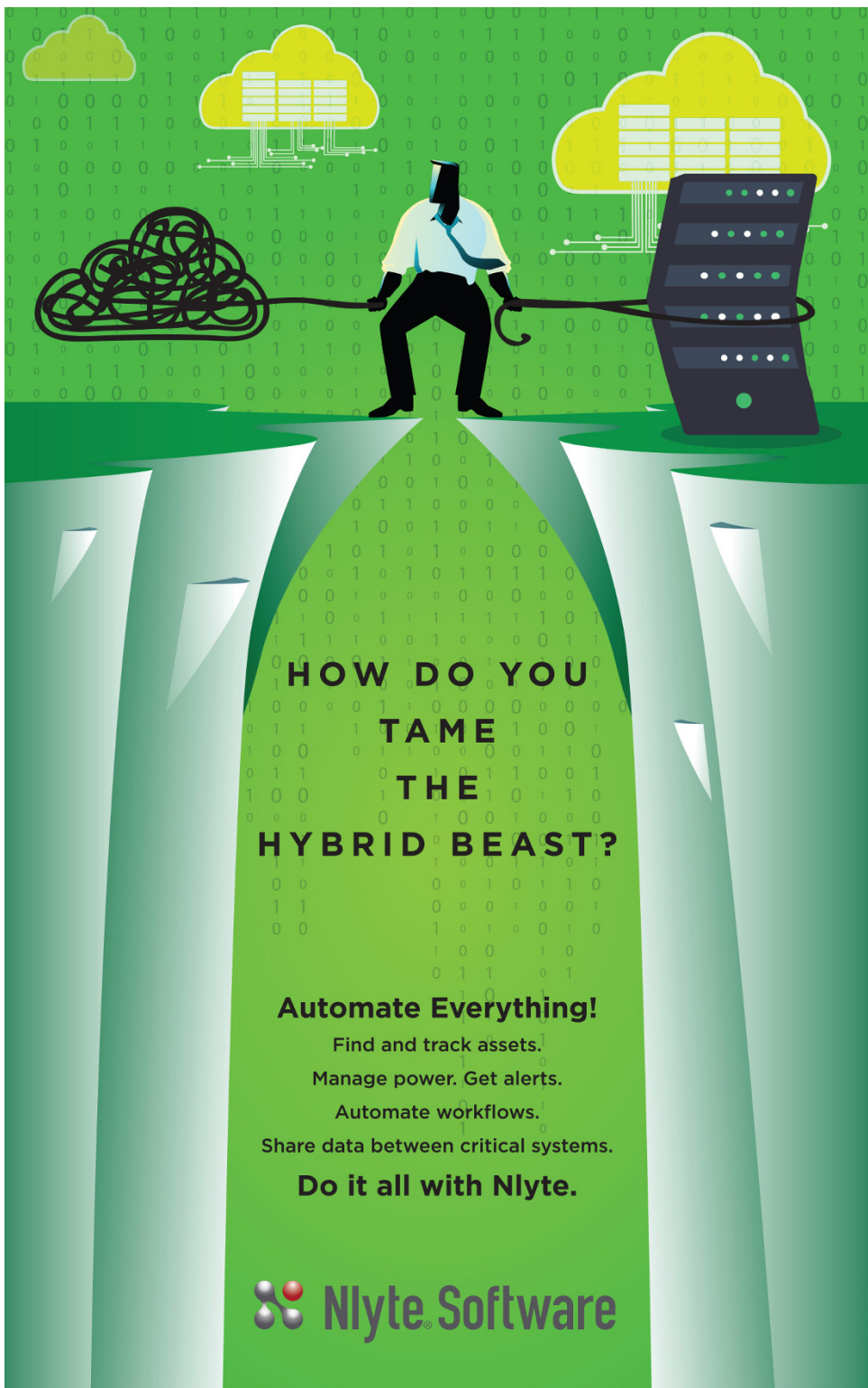
Data centers present an ideal use case for machine learning and industrial AI: complex, energy-intensive, and critical, with a very large set of inputs and control points that can only be properly managed through an automated system. With ever-evolving innovations in the data center, from application performance management (APM) linked with physical infrastructure to closely linked virtualization and multi-data-center topologies, the need for and benefit of AI will only increase.



Public clouds are data centers, too. Google recently invested over \$600 million to build a new data center in Tennessee, and Facebook spent \$750 million on a new data center in Alabama. Microsoft and Amazon have made similar investments in an ever-growing number of data centers around the world. The rise of edge computing will lead to a proliferation of thousands of micro data centers around the world, increasing the size of the hybrid digital footprint, similar to hosted facilities currently operated by popular content delivery networks (CDNs) such as Akamai and Limelight Networks.

- » **Is your software agentless and able to discover hardware, software, and Internet of Things (IoT) devices anywhere on the network?** Many systems and devices (for example, medical equipment, industrial control systems, and IoT devices) may have proprietary operating systems, strict control requirements, or limited memory and storage capacity that precludes installation of a management agent. Look for a DCIM solution that supports a variety of protocols and standards, as well as agent-based, discovery, management, and reporting capabilities to support your entire hybrid digital infrastructure.
- » **Is your solution 100 percent vendor agnostic, or do you have limitations with particular vendors' technologies?** Your DCIM solution needs to be built on an open platform to enable out-of-the-box integration with a broad ecosystem of third-party vendor and partner solutions, as well as an open application programming interface (API) to support custom integrations, when needed. A DCIM that is limited to closed, proprietary technologies can't support an ever-growing hybrid digital infrastructure comprised of numerous systems from different vendors.
- » **Is your solution protocol agnostic or are you restricted to Simple Network Management Protocol (SNMP) for discovery, monitoring, and communication?** Similar to being vendor-agnostic (see the previous bullet), you need a DCIM solution that is protocol-agnostic and supports a variety of protocols and standards in addition to SNMP, such as Modbus Remote Terminal Unit (RTU), Modbus Transmission Control Protocol (TCP), building automation and control networks (BACnet), object linking and embedding (OLE) for process control (OPC), and Extensible Markup Language (XML).

- » **Do you provide open APIs and a web-based interface that lets me create my own scripts, workstreams, and integrations without expensive professional services?** Even with a broad ecosystem of third-party vendors and partners and a platform that is vendor- and protocol-agnostic, you'll inevitably need to develop some custom integrations, build your own workflow automation scripts, and otherwise modify your DCIM solution to support new technologies, processes, workflows, and other requirements. Your DCIM vendor should provide an open API and a web-based interface that supports low-code/ no-code custom development so that you don't have to engage costly professional services every time you need to make a change to your HDIM tool set.
- » **Is the platform a nonproprietary platform, such as Microsoft Azure, so that I can do my own service and maintenance?** Your DCIM platform should run on a variety of supported operating systems, such as Windows and Linux, as well as different operating environments, such as on-premises physical or virtual servers, or public clouds such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure.
- » **Are your workflow and audit capabilities automated and able to communicate across business systems and various teams?** Your DCIM platform needs to not only collect and analyze a lot of disparate data across your hybrid digital infrastructure, but also be able to support a broad variety of users and use cases. Look for intuitive and customizable dashboards, role-based access controls (RBACs), robust auditing and reporting capabilities, and extensive automation capabilities in your DCIM platform.
- » **Can I manage my global hybrid digital infrastructure from a single console?** DCIM provides you with a single source of truth for your hybrid digital infrastructure. It should likewise provide you with a single pane of glass for management. Having to log in to different systems and consoles to manage potentially thousands of systems is inefficient and makes it challenging, if not impossible, to correlate data and make key real-time decisions to support your business.



**HOW DO YOU
TAME
THE
HYBRID BEAST?**

Automate Everything!

Find and track assets.

Manage power. Get alerts.

Automate workflows.

Share data between critical systems.

Do it all with Nlyte.

 **Nlyte Software**

Tame the hybrid cloud

Modern enterprises operate across a mix of on-premises data centers, hosted facilities, and public clouds. This hybrid digital infrastructure has evolved as organizations attempt to optimize workload placement and manage costs. However, infrastructure and operations (I&O) teams struggle to manage this increasingly complex environment using different tool sets and point solutions. Hybrid digital infrastructure management (HDIM) integrates these different tools and solutions to enable the right workloads to run in the right locations and deliver a superior user and/or customer experience.

Inside...

- Understand what the hybrid digital infrastructure is
- Find out why DCIM is the cornerstone technology of HDIM
- Identify the building blocks of HDIM
- See how DCIM helps with managing the hybrid infrastructure
- Know what to look for in an HDIM solution vendor



Lawrence Miller served as a Chief Petty Officer in the U.S. Navy and has worked in information technology in various industries for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 180 *For Dummies* books on numerous technology and security topics.

Go to **Dummies.com**[™]
for videos, step-by-step examples,
how-to articles, or to shop!

ISBN: 978-1-119-71555-9
Not For Resale

for
dummies[®]
A Wiley Brand



Also available
as an e-book



WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.