CES 9 Operational Efficiency

Reducing costs and improving operations in service provider IT environments
Contents

1. EXECUTIVE SUMMARY ........................................................................................................ 3
2. MAXIMIZING OPERATIONAL EFFICIENCY OVERVIEW .............................................. 4
   2.1. The Challenge of Operational Efficiency .................................................................... 4
   2.2. Best of Suite Approach .......................................................................................... 5
3. MONITORING...................................................................................................................... 6
   3.1. End to End Monitoring ............................................................................................ 6
   3.2. Amdocs Monitoring Framework (AMF) .................................................................... 7
   3.3. AMF Toolkit and Gateway ....................................................................................... 8
       3.3.1. Toolkit Module ................................................................................................. 8
       3.3.2. Gateway Module ............................................................................................ 8
   3.4. Summary .................................................................................................................. 8
4. SOFTWARE LIFE CYCLE MANAGEMENT ........................................................................ 9
   4.1. Software Lifecycle Management in IT Environments ............................................. 9
   4.2. Strategies for Improvement ..................................................................................... 10
       4.2.1. Consolidation .................................................................................................. 10
       4.2.2. Single Software Lifecycle Management ....................................................... 10
   4.3. Amdocs Solution for Software Lifecycle Management - XPI ................................ 10
   4.4. Amdocs XPI Key Capabilities ................................................................................. 11
   4.5. Summary ................................................................................................................ 11
5. SECURITY .......................................................................................................................... 13
   5.1. Addressing Security Violations .............................................................................. 13
   5.2. Amdocs Security ...................................................................................................... 13
       5.2.1. Mitigating Security Threats .............................................................................. 14
       5.2.2. SOX Compliance ............................................................................................ 15
       5.2.3. PCI DSS Readiness ....................................................................................... 15
   5.3. Amdocs Security Manager (ASM) ......................................................................... 15
       5.3.1. Integrating with Existing Security Systems ................................................... 15
       5.3.2. ASM Key Capabilities .................................................................................... 16
   5.4. Summary ................................................................................................................ 17
6. CONCLUSION ..................................................................................................................... 18
1. Executive Summary

As a true Best of Suite solution, Amdocs CES can greatly enhance operational efficiency and unify operations to reduce diversity and complexity in IT environments. Deploying the Amdocs CES 9 suite with the Unified Foundation uniquely offers:

- **Best of suite offering** – an end-to-end BSS-OSS portfolio of pre-integrated products
- **Unified Foundation** - a common framework foundation layer and tools shared by Amdocs CES suite products
- **Openness** - open architecture for easy integration with third parties
- **Single product catalog** – using a well-defined common data model and catalog
- **End-to-end design and usability** – focusing on the customer experience and usability
2. Maximizing Operational Efficiency

Overview

2.1. The Challenge of Operational Efficiency

Operational efficiency creates business agility, generates new opportunities, reduces costs and ultimately enhances the customer experience. For service providers, optimizing operational efficiency is a constant and elusive challenge, impacting both technology and business.

Service provider IT environments are large and complex. They are typically assembled from multiple homegrown and third party systems - accumulated over the years following development, acquisitions, mergers, and expansion into new lines of business and services - and integrated to a greater or lesser extent of. Each system may be individually managed, and have proprietary tools and processes for installation, configuration and maintenance. Each system needs to be integrated with other products that are part of the IT environment - such as monitoring and security systems – as well as with a common data model, customer databases, product catalogs and so on.

“NEGLECTING TO LOOK AT AN END-TO-END TECHNOLOGY ENVIRONMENT WILL LEAD TO LOW AGILITY, SUCH AS PAINFUL END-TO-END INTEGRATIONS, SIGNIFICANT DUPLICATIONS AND POOR PERFORMANCE”

GARTNER, MARCH 2011
2.2. Best of Suite Approach

To mitigate these challenges and to maximize operational efficiency, service providers need to ensure that their products and IT environments are characterized by openness, well-defined frameworks and platforms, adherence to industry standards and use of common tools.

Amdocs CES can greatly enhance operational efficiency and unify operations to reduce diversity and complexity in IT environments. The Unified Foundation of Amdocs CES 9 suite uniquely offers:

- **Best of suite approach** – a pre-integrated portfolio of products spanning BSS, OSS and beyond – representing an important part of a service provider’s mission-critical IT systems
- **Foundations** – a common framework foundation layer and tools such as monitoring, security, software life cycle management and more, shared by Amdocs CES suite products
- **Openness** – open architecture for easy integration with third parties
- **Standard based** – compliance with industry standards
- **Single product catalog** – Using well defined common data model and catalog
- **End-to-end design and usability** – focusing on the customer experience and usability

![Amdocs Unified Foundation Diagram](image_url)

**FIGURE 1: THE AMDOCS UNIFIED FOUNDATION ENABLES THE TRUE POWER OF THE SUITE**

This document focuses on specific areas in which the Amdocs CES 9 suite can assist service providers in their ongoing quest for operational efficiencies.
3. Monitoring

Effective monitoring is critical to maximizing performance of business applications, efficient operations and compliance with Service Level Agreements.

When monitoring systems provide timely and accurate information, service reps can identify trends early, detect system performance changes, make informed decisions, take action to increase productivity, troubleshoot on time and deliver a better customer experience.

However, in complex, diverse IT environments, effective monitoring of uptime and system health poses a daunting challenge.

3.1. End to End Monitoring

Service providers typically use third-party management tools such as HP Open View, IBM Tivoli and WebNMS to monitor their operational environments (including hardware, middleware, applications, and so on).

End to end monitoring requires the ability to collect and analyze all relevant health and performance metrics from the entire suite of products and channel them to visualization and management tools. This is a necessity as in many cases issues arising in the data center span and impact different systems and processes. The complexity and variety of collection points and data mandates openness and standard-compliance. The success of any monitoring solution is dependent on the applications themselves exposing all the required information as a feed to the monitoring tools in a consistent and easy manner.

In addition, a monitoring solution needs to address:

- Troubleshooting - to check the server, application server, database server, network and, of course, any proprietary application layer
- Trend analysis - to extract intelligence from the metrics and data gathered
- Reporting and dashboards - for visual representation of the key processes and metrics to ensure immediate detection of issues without the need to analyze mountains of data
3.2. Amdocs Monitoring Framework (AMF)

Amdocs CES 9 provides end to end monitoring across our comprehensive CES 9 BSS-OSS platform through the Amdocs Monitoring Framework (AMF) – a component of Amdocs Unified Foundation. Data gathered provides accurate and timely information on the applications’ service level state and behavior, facilitating visibility of system health so that system administrators can take proactive corrective measures to maintain the applications within their operational service level agreements.

Amdocs CES 9 Monitoring enables easy integration with market leading monitoring tools by focusing on the following principles:

- **Exposing metrics in a standard and future-proof manner** – reduces the cost of integrating Amdocs products with third-party management platforms.
  - Examples of metrics exposed via Amdocs Monitoring Framework include application queue size, application cache eviction rate, API execution time and process progress.
- **Openness** – enables exposure of additional metrics.
- **Agility** – information is aggregated prior to sending it to the management system. This reduces monitoring implementation costs and allows fast integration with third-party platforms.
3.3. AMF Toolkit and Gateway

Amdocs Monitoring Framework includes Toolkit and Gateway modules.

3.3.1. Toolkit Module

The Toolkit module provides a set of monitoring and metering APIs, including:

- **Counter** – increment/decrement counter timer that computes the timing of a selected code and maintains a sliding average
- **Meter** – measures the rate of events over time
- **Gauge** – simple value holder
- **Status Indicator** – reports current status of application entities

3.3.2. Gateway Module

The Gateway Module maps the entire catalog of available metrics and periodically checks for new metrics created by monitoring processes. The automatic aggregation of low-level metrics performed by this module exposes the higher-level metrics required for external monitoring system queries, reducing the number of metrics the external system needs to collect and increasing the efficacy of the monitoring system.

The Gateway module implements the JMX JSR-160 protocol exposing a JMX northbound interface. In addition to a notification mechanism, this module includes a component which provides the REST protocol access to the northbound interface.

3.4. Summary

Amdocs Monitoring Framework, which is part of Amdocs Unified Foundation, addresses the needs of full suite monitoring through:

- Exposure of relevant and aggregated metrics from all applications
- Easy integration with leading third-party monitoring software
- Enabling effective end-to-end monitoring of the Amdocs BSS-OSS suite
4. Software Life Cycle Management

Efficient software lifecycle management can cut TCO, increase agility and even improve the customer experience. In complex distributed and integrated IT environments, such as those typical of communications service providers, modernization and consolidation of existing systems can be an important first step towards simplifying software management. However, to maximize efficiencies, it is necessary to deploy tools that can manage both multiple products and multiple environments in a unified and user-friendly manner.

4.1. Software Lifecycle Management in IT Environments

Software lifecycle management refers to the installation, configuration, maintenance and management of software.

Managing software in an IT environment is a cumbersome, tedious and error prone task. It requires people with expertise in multiple fields. Software management requires the knowhow to manage, configure, update and upgrade each product, complemented with an understanding of the impact that changes made to on one system have on all related systems.

The challenge of software lifecycle management, however, goes beyond the borders of the back office. Fear of extended downtime and adverse impact on service levels reduce confidence in software management processes and may create hesitancy to update/upgrade or introduce new systems.

To address these challenges, organizations with large, complex IT environments must be prepared to adopt strategies that simplify their IT environment software lifecycle management processes.
4.2. Strategies for Improvement

4.2.1. Consolidation

Consolidation and reduction of the number of IT systems is a key goal of many strategic modernization initiatives. Consolidation reduces overheads and TCO, and can return agility to system operations. Amdocs has pioneered modernization projects that have reduced the number of BSS IT systems from dozens to no more than a handful, or even less.

Consolidation reduces the number of third party systems present in the IT environment. However, in many cases vendors may neglect integration between products thus leaving little room for consolidation and extending the need for software lifecycle management tools.

4.2.2. Single Software Lifecycle Management

Typically, software lifecycle management products are provided by a vendor with vast experience in handling integration, configuration, maintenance and other lifecycle management needs. The broader the range of products, the greater the value and, most significantly, the greater the saving the customer enjoys. Successful software lifecycle management requires both a common foundation and a common set of management tools for the managed products.

4.3. Amdocs Solution for Software Lifecycle Management - XPI

Amdocs CES suite shares a common foundation – with common platforms, common security, a common information model, a common monitoring platform and more. A key element in Amdocs’ Unified Foundation is a single unified solution for lifecycle management called Amdocs XPI (Amdocs Cross Portfolio Installation Framework) which handles the installation, maintenance and management of the CES 9 suite’s software lifecycle. XPI spans all phases of the software lifecycle including:

- **Deployment** – a wizard-based installation dramatically simplifies deployment of the Amdocs CES 9 suite with an efficient and straightforward deployment process that eliminates the need to conduct long and laborious integration processes. The entire Amdocs CES portfolio can be deployed in two hours!
- **Update** – software updates (e.g. hotfixes, patch bundles) are provided using XPI packages. During the update process only the artifacts of the product that are impacted by an update are replaced. This minimizes the risk of deployment and the scope of testing associated with the update. Moreover, with XPI you can modify and enhance the installed system by adding additional resources as machines, UNIX accounts and application resources.
- **Repair** – in the event of a failed deployment, a defined procedure repairs only the components of the installation that failed.
- **Rollback** – in the event of unsuccessful software updates, you can easily roll back to the previous version. This capability enables service providers to deploy updates without fear of system setbacks.
4.4. Amdocs XPI Key Capabilities

Additional features of XPI include:

- **Central repository** that holds and displays all system information providing full visibility of the system including the history of changes applied. For example, it stores the history of all software updates applied or configuration changes applied since the system was installed.

- **Installation** – packaging and installation of the software using either a graphical user interface or a command line interface.

- **Zero risk deployment** for configuration changes across the Amdocs CES 9 suite. Configuration changes can be applied either onsite or can be prepackaged for onsite deployment.

- **Analysis and reporting** - reports generated both prior to and following installation describe the changes applied. The analysis and reporting capabilities deliver improved traceability and clarity of activities performed.

- **Topology editor enables** viewing, editing and managing the topology environment. Users can add components and change the values of configuration parameters. The editor also provides a graphical interface to view, search and filter the environment. The views display all installed components and the relationships between them.

- **Built-in integration layer** – built-in integration points between products.
  - When configuration changes are made to one product the relevant changes are automatically made to dependent products.

- **Remote diagnostics** offer a clear view of environments requiring monitoring, thereby reducing the time required for analysis of environment issues and improving system visibility.

4.5. Summary

Amdocs XPI, which is part of Amdocs Unified Foundation, is revolutionary in its ability to manage, via a single tool, an entire suite of IT applications. XPI can cut costs and TCO, simplify software management, reduce installation effort, increase confidence in software update processes, and enable business agility.
5. Security

5.1. Addressing Security Violations

Service providers require security mechanisms to prevent hostile attacks and abuse of customer data. Today, hackers are organized, business-driven and equipped with financial and physical resources to support their activities. Service providers store data of customer location, habits, payment method, banking and credit information and more. This information can be stolen and sold to competitors, spammers, and others. It can be altered for personal gain and exploited to inflict damage on the service provider and end-customer. Moreover, due to the large number of IT systems in a typical service provider environment, implementing effective security systems typically requires substantial implementation and integration effort.

Service providers have no choice but to address a multitude of threats; application security, in essence, focuses on the controls and mitigations required to protect data and software from malicious wrong doers.

5.2. Amdocs Security

In Amdocs CES 9, Amdocs is delivering its most secure release ever.

Security is built from a number of layers. Amdocs Security Manager (ASM) is a part of Amdocs CES Unified Foundation that handles end-to-end security in the suite. Additional security layers reside in the products and in security measures implemented in the product development lifecycle.
### 5.2.1. Mitigating Security Threats

Amdocs follows guidelines provided by different organizations/forums such as OWASP and NIST, covering the main security-related vulnerabilities. The table below highlights OWASP top 10 threats and Amdocs’ mitigation for each.

<table>
<thead>
<tr>
<th>THREAT</th>
<th>DESCRIPTION</th>
<th>MITIGATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Injection</td>
<td>Tricking an application into including unintended commands in the data sent to an interpreter</td>
<td>Proper validation of any input coming from the user and limiting the characters to a well-defined range</td>
</tr>
<tr>
<td>Cross Site Scripting (XSS)</td>
<td>Raw data from attacker is sent to a user’s browser</td>
<td>Proper input validation as described above or output encoding that replaces malicious characters with their browser-friendly counterparts</td>
</tr>
<tr>
<td>Broken Authentication and Session Management</td>
<td>Missing credentials, tokens or any proof of authentication within every request allows hackers to skip login and bypass authentication</td>
<td>Amdocs protects all pages and access points into the application by requiring submission of credentials or any proof of authentication, denying unauthenticated users from using the protected application’s resources</td>
</tr>
<tr>
<td>Insecure Direct Object References</td>
<td>Application exposes objects (e.g., files) without properly protecting them with authorization. This allows hackers to gain unauthorized access to the various application objects</td>
<td>For each object accessed by the application, a role-based authorization is added</td>
</tr>
<tr>
<td>Cross Site Request Forgery (CSRF)</td>
<td>A victim’s browser is tricked into issuing a command to a vulnerable web application. Vulnerability is caused by browsers that automatically include user authentication data (session ID, IP address, Windows domain credentials, ...) with each request</td>
<td>A randomly generated token, valid for a defined period of time only, is added to each request, making it extremely difficult for a hacker to craft a proper request that also includes a valid token. The token is based on ASM session ID.</td>
</tr>
<tr>
<td>Security Misconfiguration</td>
<td>Configuring the different architecture layers (OS, application server) inappropriately</td>
<td>Amdocs provides secured implementation guides. guides for its major applications. Implementers should follow the guidelines to secure the production platform</td>
</tr>
<tr>
<td>Insecure Cryptographic Storage</td>
<td>Storing sensitive data insecurely</td>
<td>All sensitive data is encrypted in storage using either Oracle TDE or the ASM encryption service</td>
</tr>
<tr>
<td>Failure to Restrict URL Access</td>
<td>Allowing direct access to URLs that should be accessed only by authenticated/authorized users only</td>
<td>All access points to non-public information in CES9 requires authentication/authorization</td>
</tr>
<tr>
<td>Insufficient Transport Layer Protection</td>
<td>Transmitting sensitive data insecurely</td>
<td>CES9 allows usage of SSL for all sensitive data transports</td>
</tr>
<tr>
<td>Invalidated Redirects and Forwards</td>
<td>Redirects frequently include user supplied parameters in the destination URL. If these parameters are not validated, attackers can direct their victims to a site of their choice</td>
<td>The applications validate user originated data properly and eliminate injection of paths or commands that allow a hacker to take control over a valid flow</td>
</tr>
</tbody>
</table>
5.2.2. SOX Compliance

Amdocs continues to support customers’ compliance with the Sarbanes-Oxley Act of 2002.

Amdocs provides accounting (logs) of events related to financial transactions and security.

5.2.3. PCI DSS Readiness

To minimize risk of credit card theft, service providers need to comply with the credit card companies standards.

Amdocs systems are PCI DSS (Payment Card Industry Data Security Standard) ready. This allows Amdocs’ customers to better prepare for their PCI-DSS audit on site. CES 9 supports PCI requirements, including:

- All credit card numbers are encrypted while in storage and in transport
- Credit card numbers are removed from log files and error messages, and masked on display
- Amdocs does not store CVV data
- Products undergo penetration tests to uncover vulnerabilities such as XSS, CSRF, SQL Injection and many more.
- Amdocs provides mandatory application security courses for developers
- Improved accounting (logging) of credit card access for improved auditing

5.3. Amdocs Security Manager (ASM)

5.3.1. Integrating with Existing Security Systems

Integrating a new security system into an existing environment can be a major undertaking. Implementers need to identify each and every resource and activity requiring restriction throughout the applications, define appropriate policies to protect those resources and activities, and create a wide set of roles to accompany the policies. In addition, each entry point into the application has to be identified as well as have a login process suitable to the solution chosen.
Amdocs Security Manager (ASM) can dramatically cut the cost of deploying and integrating a BSS-OSS wide security solution. ASM enables the products in the suite to “speak” in a common security language to determine user identity and permissions throughout a transaction. Pre-integrated with Amdocs products, ASM acts as a central point of integration for external security solutions, relieving the need for application changes.

ASM has been developed in accordance with leading security concepts and standards. It adopts the Spring Security Framework for better and simpler security mechanisms for authentication and authorization. It also allows faster integration with third-party Single Sign On solutions through a set of ready-made Spring plugins.

As Amdocs BSS-OSS products are typically deployed alongside an existing IT environment which already has a security solution in place, ASM facilitates the deployment by offering a single point of security integration.

5.3.2. ASM Key Capabilities
ASM is a pure Java library allowing fast and easy deployment alongside the applications, and is aligned with industry standards. It utilizes capabilities provided by the open source Spring Security Framework, which allows ASM to be lean and efficient in its authentication and authorization processes.

This framework also allows ASM to support a variety of security solutions found in the industry, and enables quick integration with them. Readymade Spring plugins also simplify Single Sign On with different providers.

Whilst ASM keeps evolving and adopting new approaches and technologies, it is fully backward compatible with CES V8.1 and allows interoperability in a mixed version run time environment.
ASM offers:

- Administration capabilities through a UI and APIs
- User management that allows a personal profile definition of each user including a set of privileges for the application
- Password management – complex password policy and password encryption in storage allows safekeeping and un-guessable passwords
- Single Sign On – central session and ticket serving all applications, allowing a user’s identity – and accountability - to accompany a transaction end-to-end
- Policy server that allows the definition and administration of protected resources and protective policies
- Accounting – Logging of security events such as login, logout, authorization events, etc. This serves as evidence and audit material and addresses non-repudiation

5.4. Summary
ASM, which is part of Amdocs Unified Foundation, is field proven in many installations at a wide range of the world’s leading service providers. When deploying Amdocs products, ASM delivers an effective, standard, cross-suite security solution that integrates easily and quickly with existing security systems.
6. Conclusion

As service providers’ IT environments continue to expand in scope and complexity, service providers need to find new ways to reduce cost of ownership, improve operations and maximize operational efficiencies. This requires them, for example, to adopt new cost-effective hardware technologies and address pervasive broad-impact suite-wide challenges.

This white paper has demonstrated how deployment of a single suite with a common foundation can optimize efficiencies in areas such as security, monitoring and software lifecycle management. Amdocs is unique in being able to provide such solutions, based on:

- Our extensive suite of products covering the core, mission-critical BSS-OSS needs of service providers, and
- A true “best of suite” approach with a single foundation and a powerful set of common foundation products – covering installation, maintenance, management, configuration, security, monitoring, and more – in a unified fashion.

The commonalities of the Amdocs CES 9 foundation and Amdocs’ best of suite approach reduce software management overheads, integration efforts, costs and Time to Market while creating operational efficiencies and ultimately improving the customer experience.
About Amdocs

For 30 years, Amdocs has ensured service providers’ success and embraced their biggest challenges. To win in the connected world, service providers rely on Amdocs to simplify the customer experience, harness the data explosion, stay ahead with new services and improve operational efficiency. The global company uniquely combines a market-leading BSS, OSS and network control product portfolio with value-driven professional services and managed services operations. With revenue of $3.2 billion in fiscal 2012, Amdocs and its 20,000 employees serve customers in more than 60 countries. Amdocs: Embrace Challenge, Experience Success. For more information, visit Amdocs at www.amdocs.com

Amdocs has offices, development and support centers worldwide, including sites in:

**THE AMERICAS:**
- BRAZIL
- CANADA
- COSTA RICA
- MEXICO
- UNITED STATES

**ASIA PACIFIC:**
- AUSTRALIA
- CHINA
- INDIA
- JAPAN
- PHILIPPINES
- SINGAPORE
- TAIWAN
- THAILAND
- VIETNAM

**EUROPE, MIDDLE EAST & AFRICA:**
- AUSTRIA
- CYPRUS
- CZECH REPUBLIC
- FRANCE
- GERMANY
- IRELAND
- ISRAEL
- KAZAKHSTAN
- THE NETHERLANDS
- FRANCE
- RUSSIA
- SOUTH AFRICA
- SPAIN
- SWEDEN
- UNITED KINGDOM
- UNITED ARAB EMIRATES - DUBAI

For the most up-to-date contact information for all Amdocs offices worldwide, please visit our website at www.amdocs.com/corporate.asp

Copyright © 2013 Amdocs. All Rights Reserved. Reproduction or distribution other than for intended purposes is prohibited, without the prior written consent of Amdocs. The trademarks and service marks of Amdocs, including the Amdocs mark and logo, Intentional Customer Experience, CES, Clarity, Ensemble, Enabler, Return on Relationship, Intelecable, Collabrent, XACT, OSI, OpenGraphic Software, Qpass, Cramer, SigValue, JacobsRimell, ChangingWinds, jNetX, OpenMarket Inc., MX Telecom Inc., MX Telecom Ltd, Stranace, and Bridgewater Systems are the exclusive property of Amdocs, and may not be used without permission. All other marks are the property of their respective owners. Created 02/2013