Publication date:
September 2021
Author:
James Crawshaw

Migrating OSS to the Public Cloud: Why, How, and When

Commissioned by:
amdocs

Brought to you by Informa Tech

Contents

Introduction

When Amazon launched its Web Services offering in 2006, no right-minded telecom operator would have considered using it to host mission-critical IT applications. Even after 10 years of growing adoption, public cloud was still not considered suitable to meet the performance, security, and data governance requirements of the telecom industry in 2016. It was also considered too expensive to host back-office applications such as operations support systems (OSS).

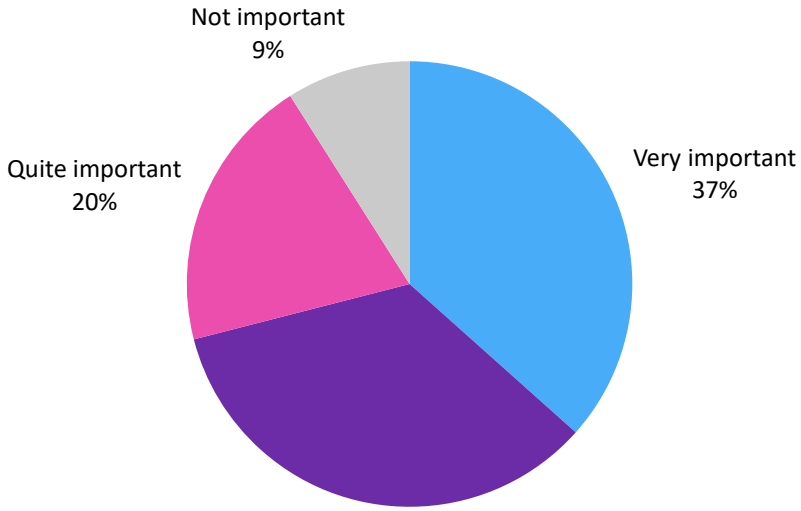
A lot has changed in the last five years. The perceived disadvantages of running OSS applications on public cloud have been turned on their heads. The COVID-19 pandemic has demonstrated the reliability of the public cloud providers. With increasing security threats to telcos' own infrastructure, the strong security of the hyperscale cloud providers is also increasingly well recognized. And for some operators, public cloud is also proving to be cheaper than hosting OSS in their own private data centers.

Most communications service providers (CSPs) still run most of their OSS on premises and in private cloud. After general company back-office IT systems such as finance or HR, business support systems (BSS) have been the trailblazer for public cloud usage in the telecom sector. Examples include customer-facing applications such as web portals and chatbots. OSS was seen as more of a challenge given its proximity to the network, its sensitivity to latency, large data volumes, and need for higher reliability. The closer you get to the network, the more conservative operators tend to be in their technology decisions. However, operators have recently been choosing to host their mobile core on public cloud. If the public cloud is deemed fit for a system as critical as mobile core, there is no reason why it cannot host OSS.

Most requests for proposal for OSS issued by telcos now ask that any new software should be deployable in public cloud with the option to host on private cloud and burst into public cloud as needed. For now, CSPs are typically still choosing to run OSS in private cloud, but Omdia sees this changing over the next few years as the cost and agility benefits of migrating to public cloud become better understood.

As **Figure 1** shows, most telecom operator executives that Omdia surveyed think that moving IT operations to public cloud is either important or very important. Having recognized this importance, it is now time for them to act. However, choosing which applications to move first, where to host them, and what to change (databases, message buses, container orchestrators, etc.) can be overwhelming. This white paper examines the reasons to host OSS on public cloud and the different strategies for migrating there.

Figure 1: How important is moving IT operations to the public cloud?



Note: n=420

Source: Omdia ICT Enterprise Insights 2019/20

Why run OSS in public cloud?

If it ain't broke, don't fix it. If your OSS is running fine on-premises today, why would you consider running it in public cloud? After all, public cloud is just someone else's server. Well, yes and no. Public cloud providers definitely do run physical servers, lots of them. Even serverless computing has a server somewhere. The point is that you, as an application owner, do not need to worry about where that server is, or what operating system it is running, or whether it has the latest security patches installed, et cetera, et cetera.

Elasticity

Let us start with the most obvious advantage that public cloud services offer versus your own data center: elasticity. As far as the needs of any individual telecom operator, enterprise, or government are concerned, the public cloud is infinitely scalable. Therefore there is no need to make projections of your future workload requirements and overprovision resources today. You simply pay for the server capacity you need now, and if future requirements increase or decrease, your application hosting costs will rise or fall accordingly.

Agility

Closely related to elasticity is agility. An on-premises deployment of an OSS application will require requests for server infrastructure well in advance. Using public cloud, the resources can be made available instantly. This enables faster deployments of new IT systems, which allows new services to be introduced more quickly. By reducing the time to market, operators can be more innovative in their marketing and product strategy. According to Pebbles Sy-Manalang, CIO of Globe Telecom, the Philippine operator has managed to reduce its IT provisioning time from 80 days to 2 days using public cloud and has seen a 15-fold improvement in application performance.[1] Globe has refactored many of its legacy applications to make them run better on the cloud.

Availability

The telecom industry is famous for its "five nines" reliability mantra. But when it comes to the availability of server infrastructure, it is hard for any single enterprise, telco or otherwise, to match the availability of public cloud infrastructure. The huge scale and redundancy of public clouds' server farms and networks makes their uptime ultrareliable. Equally, the strong patch management of public cloud providers makes them highly secure.

[1] AWS re:Invent 2018, https://www.youtube.com/watch?v=iwIQNoarVas

Easier upgrades

Hosting applications in public cloud can simplify the process of upgrading software, allowing upgrades to be made more quickly and frequently. The upgrade process can be managed using blue-green deployments where the software is transitioned gradually from the current version (blue) to the new version (green). Both versions of the software run in identical production environments: blue is live, and green is undergoing testing of a new software release. Once the operator is happy that the new software is working correctly, an application load balancer is switched so that all future application requests go to the green environment while blue becomes idle (ready for new software to be downloaded and tested or ready for a rollback if unforeseen problems emerge with green). Blue-green deployments are well suited to public cloud because the additional server capacity that is required during the upgrade process only needs to be made available temporarily.

Development and testing

Often OSS applications will go through a phase of development, adaptation, and integration within the telecom operator's IT environment. The operator will work together with the OSS supplier to test the application during this process. This could be for the deployment of a completely new OSS or to trial a new module with additional functionality. Having to dedicate on-premises server capacity for these needs can slow the process down and can result in low utilization if the servers are not reallocated to another purpose once the testing is complete. By using public cloud, operators and their OSS suppliers can ensure the requisite server capacity is available for the development and testing environments only for as long as it is needed. And to reduce cost further, the operator can take advantage of spot pricing, which can be 90% cheaper than regular cloud services. Spot instances use spare capacity in the public cloud for stateless, fault-tolerant, or flexible applications such as test and development workloads.

Total cost of ownership

While agility and flexibility are strong selling points for public cloud, operators also expect to achieve lower costs. Naturally, they can avoid capex by using public cloud. But operators do not want to just swap lower capex for higher opex. They are looking for a lower total cost of ownership. The experience to date has generally been positive for operators hosting OSS in public cloud. In some cases they have suffered unexpected costs due to chatty applications with high traffic in and out of the cloud. But generally, they have found that paying only for the capacity that they actually need and leveraging the economies of scale of hyperscalers has brought significant cost benefits. The public cloud providers are experts in running IT infrastructure; by tapping into this expertise, telecom operators can reduce their operating expenses.

Managed services

To get the most value out of public cloud, one should not just consider the basic infrastructure services but also the platform-as-a-service (PaaS) offering, which includes managed versions of various open source software components such as Elasticsearch, Kafka, and Kubernetes.

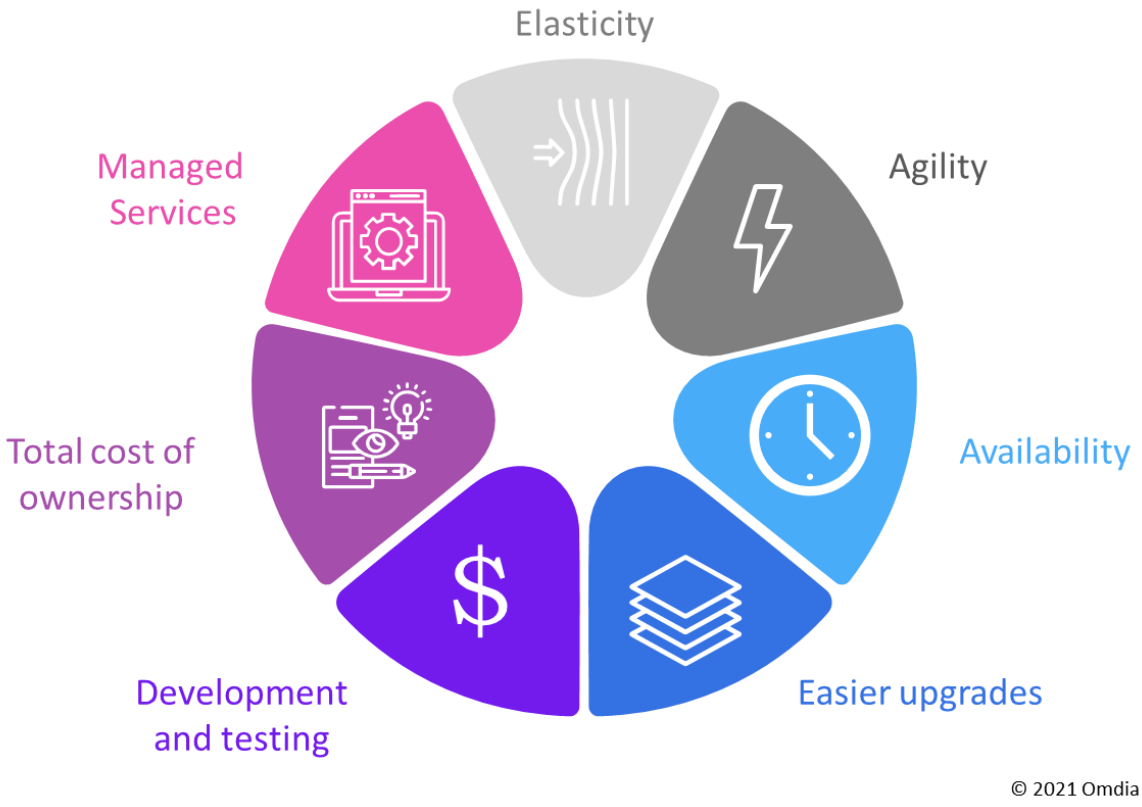
- With a managed service for Elasticsearch management, tasks such as hardware provisioning, software installation and patching, failure recovery, backups, and monitoring are simplified. To monitor your clusters, Elasticsearch services include built-in event monitoring and alerting so you can be notified of changes to your data to proactively address any issues. You can easily scale your search cluster up or down via a single API call or a few clicks in a console. As a fully managed service, this lowers your total cost of operations by eliminating the need for a dedicated team of Elasticsearch experts to monitor and manage your clusters.

- Apache Kafka clusters are challenging to set up, scale, and manage in production. When you run Apache Kafka on your own, you need to provision servers, configure Apache Kafka manually, replace servers when they fail, orchestrate server patches and upgrades, design the cluster for high availability, ensure data is durably stored and secured, set up monitoring and alarms, and carefully plan scaling events to support load changes. Managed Kafka services make it easy to build and run production applications on Apache Kafka without needing Apache Kafka infrastructure management expertise. That means you can spend less time managing infrastructure and more time on more valuable activities.

- A managed Kubernetes service automates key tasks such as patching, node provisioning, and updates. Managed services run the Kubernetes control plane across multiple availability zones. They automatically detect and replace unhealthy control plane nodes and provide on-demand, zero-downtime upgrades and patching. With managed node groups, you do not need to separately provision compute capacity to scale your Kubernetes applications, and a managed Kubernetes service automatically applies the latest security patches to your cluster's control plane.

OSS applications have traditionally used high-performance database software from commercial vendors. These applications carry hefty annual software maintenance fees. By adapting the OSS to use an open source database (e.g., PostgreSQL, MySQL, MariaDB) that is provided as a managed service by the public cloud provider, the cost of ownership of the OSS application can be significantly reduced. Public cloud platform services such as these are highly reliable and scalable and can even lead to an improvement in the application performance. A database service from the public cloud provider can also simplify operations by automating time-consuming administration tasks such as hardware provisioning, database setup, patching, and backups. Managed database services have many other features that enhance reliability for critical production databases, including database snapshots and automatic host replacement.

Figure 2: Reasons to use public cloud



Source: Omdia

Cloud migration strategies

Assuming you have decided to move at least one OSS application to public cloud, what are the options for getting there? Commonly, the cloud migration options are referred to as rehosting, re-platforming, and refactoring.

Rehosting: Lift and shift

Rehosting, often referred to as “lift and shift,” simply moves an existing monolithic application to a public cloud, consuming its server infrastructure as a service (IaaS). This can provide some cost benefits, and unless you have some control over the architecture of the application itself (e.g., a homegrown OSS system), this may be your only option.

Re-platforming: Lift, shift, and tinker

The next option is re-platforming. This uses managed services from the cloud provider as discussed in ***Managed services***. Instead of just consuming infrastructure, you are now consuming a PaaS. Re-platforming is sometimes known as “lift, shift, and tinker.” The tinkering refers to things such as using a managed database service instead of a traditional commercial database software product. Tinkering therefore requires some control over how the software is designed. If the operator built the OSS itself, it has this control. If it is a commercial solution, it is reliant on the vendor to make these changes.

Refactoring

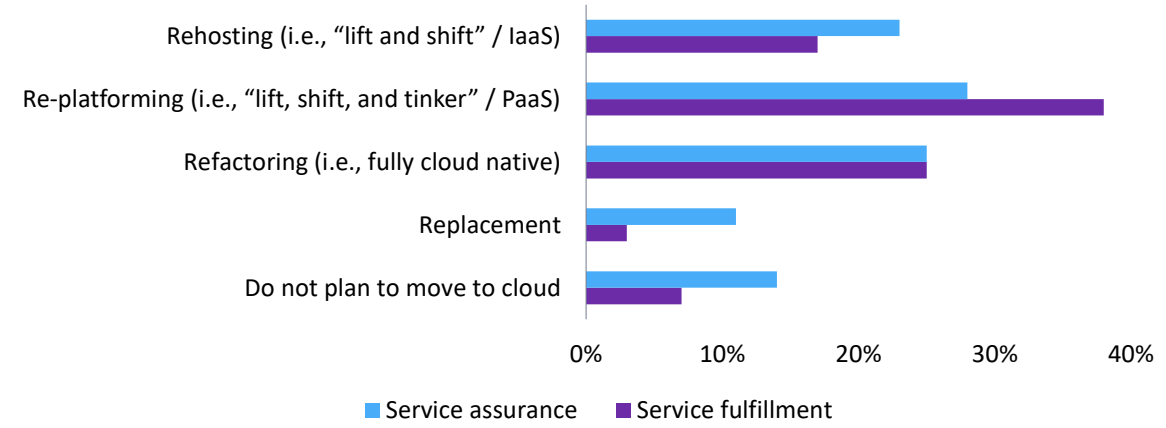
The next level is a complete refactoring of the OSS application using cloud-native principles. Cloud-native applications are a combination of existing and new software development patterns. Existing patterns include software automation (infrastructure and systems), API integrations, and services-oriented architectures. New cloud-native patterns include microservices architecture, containerized services, and distributed management and orchestration. Refactoring an application in this way improves scalability (more instances of an individual microservice can be created rather than new instances of the whole application) and simplifies development (since teams can work independently on each microservice rather than developing a new version of an entire monolithic application). Refactoring is clearly the hardest migration path but, when done correctly, should yield the greatest benefits. For commercial OSS solutions, the operator is reliant on the vendor to refactor the application and make it available in a new release. For homegrown OSS, the operator could either refactor an existing application or retire it and choose a commercial cloud-native offering instead.

Operator plans for OSS migration

As the survey results shown in **Figure 3** show, the majority (around 85%) of CSP executives that Omdia surveyed indicated that they plan to migrate some OSS to the cloud. Just 15% of respondents had no plans to migrate service assurance or fulfillment to public cloud. The most common approach is re-platforming, then refactoring, rehosting, and—least popular of all—replacement.

CSPs cannot themselves re-platform or refactor their commercial OSS, only their homegrown systems. The ability to leverage public cloud for their commercial OSS depends on the roadmap of the vendor. Therefore the desire to host OSS on public cloud might precipitate the replacement of existing systems.

Figure 3: What path do you plan to use to migrate OSS applications to the cloud?



Note: n=65

© 2021 Omdia

Source: Omdia OSS/BSS Survey 2020

Operator case study

This case study involves OSS/BSS vendor Amdocs, public cloud provider AWS, and a leading Tier 1 telecom operator in the Asia Pacific & Oceania region. Amdocs had already deployed its catalog-driven solution for managing the service order lifecycle, Order & Service Orchestrator (OSO), on Amazon's Elastic Compute Cloud (EC2) for this customer. However, the version of the application that the customer was running was not cloud native, and it relied on expensive proprietary database technology. With the upgrade to the latest, cloud-native version of OSO, the operator benefited from the more fine-grained scalability that a microservices architecture brings. Updates, which are deployed every two weeks, are much easier to test using blue-green deployments. The operator has an automated continuous integration / continuous delivery (CI/CD) pipeline that can test and deploy a single microservice using Kubernetes. This allows the operator to deploy new services to its enterprise customers much faster than in the past.

The upgrade also enabled the operator to utilize a single OSS solution from Amdocs for all its enterprise services spanning 4G/5G mobile, collaboration and unified communications, fiber and internet access, SD-WAN, security, IoT, and its new "network-as-a-service" offering.
The new version of OSO also leverages several AWS services including an open source database, which has saved the operator millions of dollars in annual licensing fees. The new version of OSO also brought functional improvements that have enabled a 40% reduction in manual processes associated with service order management within the operator's enterprise division. In addition, the maximum order throughput capacity of the new system has been increased by a factor of four.

The simplified **Figure 4** below shows the deployment architecture for Amdocs' OSO on AWS. The telecom operator connects to the public cloud via AWS's Direct Connect service. This enables a more reliable private connection between AWS and the operator's data center than using regular internet services. An application load balancer spreads the workloads over three availability zones, logical data centers in a region that are available for use by AWS customers.

Within each availability zone, the OSO processes are split into a web tier with static HTML content and an application tier with the dynamic content. In addition to OSO, auxiliary applications include the Open Network Inventory (which houses the service inventory), fallout management, and downtime management. Fallout management provides troubleshooting steps to resolve a problem with an order. Downtime management helps to avoid order fallouts if a system outside the AWS cloud (e.g., within the telecom operator's data center) experiences an outage.

The managed data persistence tier uses AWS services including

- **Elasticsearch Service (ES):** a search engine for use within an application
- **Relational database service (RDS):** available on several database types including Amazon Aurora and open source options PostgreSQL, MySQL, and MariaDB

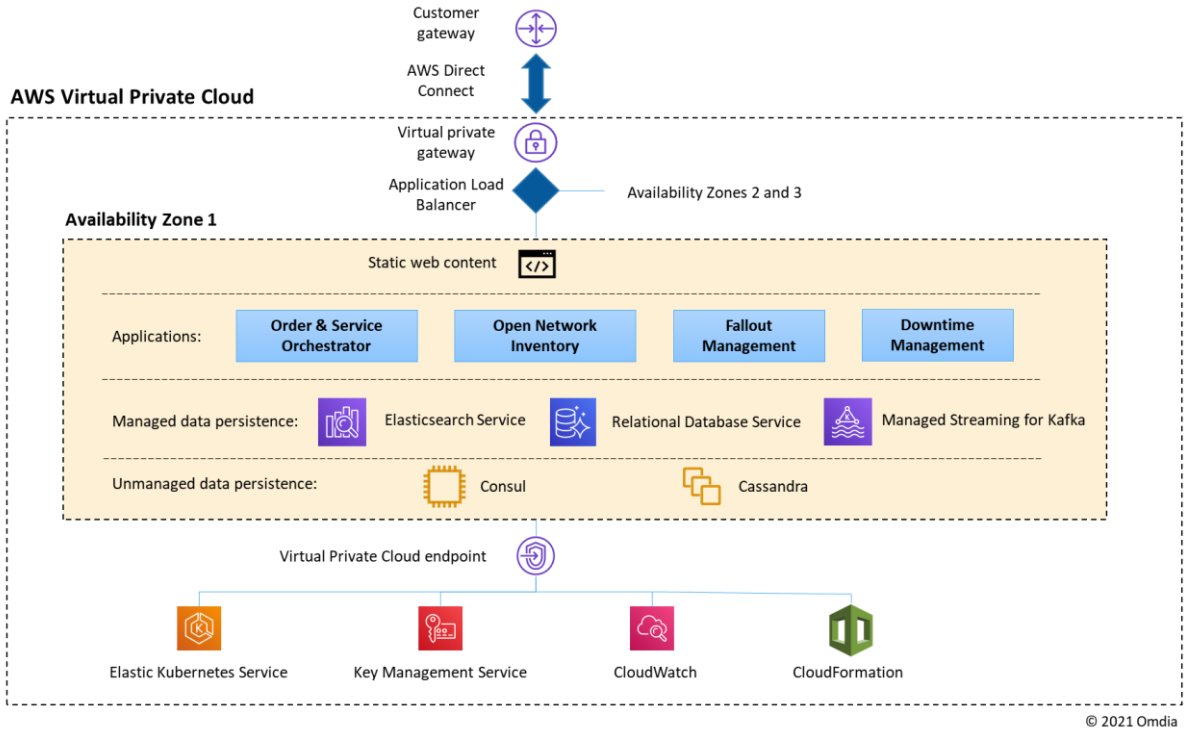
- **Managed streaming for Kafka (MSK):** an open source event-streaming message bus. MSK handles real-time ingestion and processing of streaming data using a managed version of Apache Kafka. This enables the user to use native Apache Kafka APIs to populate data lakes, stream changes to and from databases, and power machine learning and analytics applications.

The unmanaged data persistence tier uses Cassandra, an open source NoSQL database, and Consul, a tool from HashiCorp that provides cloud networking automation. Certain features of Cassandra and Consul used by Amdocs' OSO are not yet available on the AWS managed service version of these tools, so Omdia refers to this tier as unmanaged.

To manage the application on AWS, the IT department of the telecom operator has access to the following tools and services through a Virtual Private Cloud endpoint:

- **Elastic Kubernetes Service (EKS):** used for managing containerized applications
- **Key Management Service (KMS):** to create and manage cryptographic keys and control their use across a wide range of AWS services in the application
- **CloudWatch:** a resource and service monitoring and observability service built for DevOps engineers, developers, site reliability engineers, and IT managers
- **CloudFormation:** a tool for managing AWS resources

Figure 4: Amdocs Order & Service Orchestrator deployment on AWS



Source: Adapted by Omdia from AWS/Amdocs graphic

Conclusions

The advantages of using public cloud to host software are clear: elasticity, scalability, agility, reliability, resource optimization, and automation. However, moving to the cloud can also bring new challenges. Operators will need to modernize their IT processes, adopting agile development and testing methodologies. This may require reskilling of the workforce. When one OSS moves to public cloud, the performance of other systems might be affected because of latency. Data crisscrossing between public and private cloud might lead to unexpected costs.

In addition, operators need to be careful to comply with data privacy and sovereignty regulations. Each country has its own rules, and each service provider has different policies. Sensitive data passes through the OSS given its position at the crossroads between BSS and the network.

To test the waters, operators should experiment by placing some OSS workloads on public cloud to handle capacity spikes, ensure business continuity, and support new lines of business (e.g., 5G private networks). If necessary, they can use edge cloud services to overcome latency issues that might be experienced with a 100% centralized cloud solution.

Operators should avoid the temptation to simply "lift and shift" legacy OSS to public cloud. Hosting the application on someone else's server may achieve some cost savings, but to reap the full benefits of cloud, applications should ideally be refactored using cloud-native principles. Operators should also embrace the public cloud providers' managed services (e.g., databases) to reduce cost and simplify IT operations.

Each OSS application should be evaluated independently. Not all applications will need refactoring and not all cloud-native applications must run in public cloud. Operators need to find the right trade-off between private and public cloud and multicloud or sole source for each individual application.

When migrating mission-critical systems such as OSS to the cloud, to reduce risk most operators will need a trusted partner to determine the target architecture and roadmap and to help with systems integration and testing. Ultimately, by moving applications to the public cloud, telecom operators can free their operations teams from repetitive work, allowing them to focus on more value-added activities. According to Ralf Hellebrand,[2] programme director of technology at Vodafone Germany, by moving Amdocs OSS workloads onto AWS public cloud, "We are getting our people focused on creating more value for the customer." Outsourcing application hosting to the public cloud providers can allow operators to put more of their resources into core activities that enable them to differentiate in the marketplace and delight their customers.

[2] AWS re:Invent 2020 https://www.youtube.com/watch?v=S0Q8z_KnZR0

Appendix

Methodology

This report is based on Omdia's research reports, desk research of publications by various communication service providers, and interviews with executives representing the CTO office of telecom operators and their technology partners.

Author

James Crawshaw
Principal Analyst, Service Provider Operations and IT
customersuccess@omdia.com

Get in touch

www.omdia.com
customersuccess@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

About Amdocs

Amdocs is driving our increasingly connected digital society forward by utilizing the creativity of our 26,000 employees and the power of our innovative, award-winning technology. With almost 40-years of unparalleled industry expertise, Amdocs is a trusted partner to the world's leading communications and media companies, serving more than 350 service providers in over 80 countries.

We accelerate their migration to the cloud, digitalize and automate their operations, and provide their end users with exciting next-generation communication and media experiences.

Our cloud-native, open and dynamic portfolio of digital solutions, platforms and services, built on a microservices-based architecture, enables our customers to achieve faster time to market and provides them the flexibility to follow the most suitable transformation strategy for their evolving needs.

Our Amdocs NEO, innovative Service and Network Automation platform service lifecycle management capabilities can power any automation journey – whether digital-to-network automation, end-to-end service and network orchestration, 5G slice & edge automation, Network-as-a-Service or OSS modernization or migration to the cloud.

We provide comprehensive cloud consulting to help service providers build their vision, strategy, architecture, infrastructure and roadmap and cloud migration, testing and SI services for a seamless cloud migration.

Copyright notice and disclaimer