Ovum
TMT intelligence | informa

On the Radar: Synadia Communications NATS, message-oriented middleware

Cloud-native open source messaging technology

Publication Date: 28 Aug 2018 | Product code: INT003-000217

Michael Azoff

Summary

Catalyst

The messaging backplane that now underpins distributed systems architecture must handle the increased decomposition and scale of hyperconnected environments. There is a need for lightweight communications for ever-increasing microservices, edge platforms, and endpoint devices, and for resiliency with an emphasis on the health of the system as a whole. There are also performance needs, with built-in load balancing, no-config auto-scaling, and identity and security mechanisms that are consistent from edge devices to backend services. NATS was developed by Derek Collison to address these needs in an open source project. It is maintained by Synadia, with the aims of eventually offering worldwide and global connectivity to anyone, and making its adoption easy and its environment robust.

Key messages

- Ease of use enables developers to implement solutions using NATS without training, instead using examples, blog posts, and online documentation.
- NATS is resilient and scalable, dynamically adding servers to a cluster maintaining supported clients, with awareness of topology changes, and providing auto healing by automatic fail-over to new nodes in the cluster.
- NATS is secure, offering full TLS support, CA certificates, user/password- or token-based authentication, and publish/subscribe authorization through permission-based roles. It defaults to the most secure ciphers.
- NATS is highly performant, offering over 20 million messages per second on one server and data streaming with up to 80 million messages per second per server with multiple data streams.
- NATS has a simple, text-based protocol that makes it easy to develop clients, and is an embeddable single binary with a small footprint, which runs on almost any device.

Ovum view

NATS is a new breed of open source messaging system designed for modern, cloud-native architectures with an emphasis on simplicity and performance. While legacy messaging systems often have a deep feature set with a large API and heavy configuration, NATS has a limited feature set but is easy to implement and use, and once set up is always available and highly robust.

With very low resource requirements and no external dependencies, NATS is also ideal for edge computing, and we expect to see growth there in the future. This, combined with new features to allow extremely large and secure clusters of NATS servers, will allow users to create global deployments connecting millions of endpoints over NATS.

Although maybe less well known than more established rivals, NATS is gaining traction and popularity among developers and we expect it to continue to grow market share.

Recommendations for enterprises

Why put NATS on your radar?

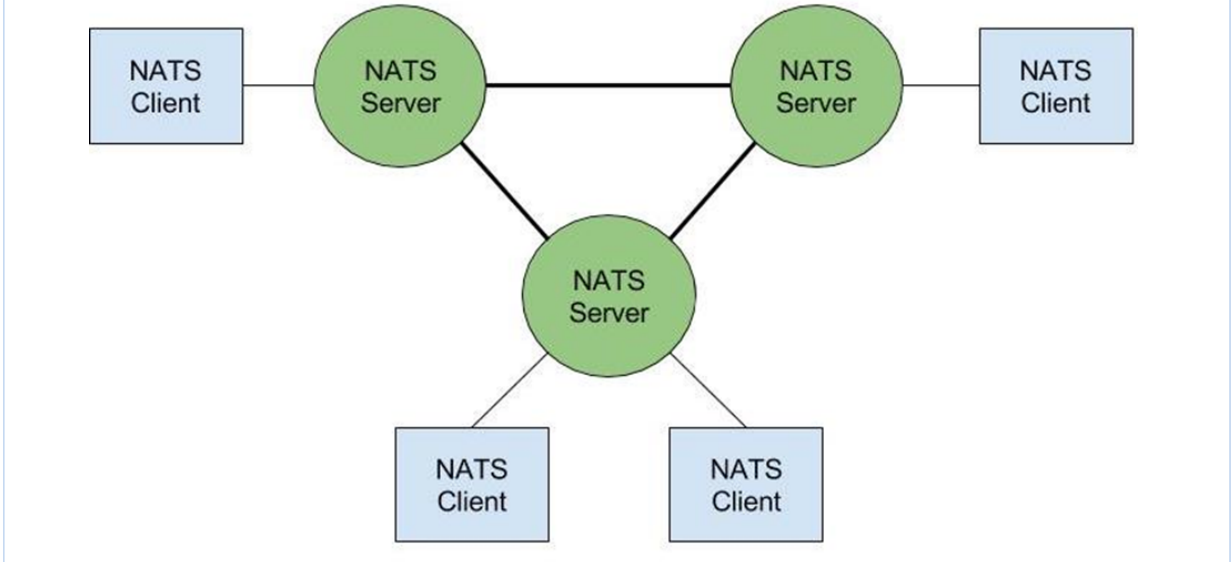
Most users adopt NATS because of its ease of use – it takes only a few minutes to set up – and because of its simplicity in deployment. More advanced users have leveraged NATS auto healing and cloud-native features to reduce their operational costs by adjusting their deployment real-time to meet demand and save cloud resource costs. The auto-healing capability works if servers go down or if clients go down. They all put themselves back together automatically, with no intervention from people needed at all. Ovum believes this feature will appeal to many organizations.

NATS provides the messaging backplane behind Cloud Foundry and is a CNCF project. With Kubernetes and Prometheus integrations, it also provides client support for over 30 different programming languages. It will also suit users and customers who want to enable cross-cloud communication, such as event propagation, when moving from the cloud to edge computing and toward IoT devices.

Highlights

NATS is highly performant: the core server can process over 20 million messages per second for a single stream, and up to 80 million messages with multiple data streams. This performance, alongside a very small footprint (7Mb Docker image) and no external dependencies, makes NATS simple to deploy and operate in many environments.

Figure 1: NATS architecture



Source: Synadia

NATS deployments are always-on and available through auto-discovery of servers and clients, and self-healing with automatic reconnect of servers and clusters. This allows a NATS server deployment in the cloud to withstand network partitions, node crashes, or planned topology changes with no

configuration changes or downtime for clients. The NATS streaming component provides data streaming with features such as message playback, persistence, and durable subscribers.

The request/reply, publish/subscribe, and queue subscriber load-balance patterns are supported. This makes NATS flexible enough to accommodate many use cases, and load-balancing features allow applications built with NATS to scale in the cloud by simply adding instances with no configuration changes.

NATS is secure by default, with bidirectional TLS support, user- and token-based authentication, and authorizations through role-based permissions to determine what applications are authorized to connect and what data can be sent and received.

Architecture

NATS provides a layer between the application and the underlying physical network. Application data is encoded as a message and sent by the publisher. The message is received, decoded, and processed by one or more subscribers. A subscriber can process a NATS message asynchronously or synchronously.

NATS implements three primary patterns for users:

- **Publish Subscribe:** NATS publish subscribe is a one-to-many communication. A publisher sends a message on a subject. Any active subscriber listening on that subject receives the message. Subscribers can register interest in wildcard subjects.
- **Request Reply:** NATS supports two flavors of request reply messaging: point-to-point or one-to-many. Point-to-point involves the fastest or first to respond. In a one-to-many exchange, users set a limit on the number of responses the requestor may receive.
- **Load-Balanced Queue Subscribers:** NATS provides a load balancing feature called queue subscriptions. Using queue subscribers will load-balance message delivery across a group of subscribers. It can be used to provide application fault tolerance and scale workload processing. This involves no server configuration.

Background

Derek Collison, the founder of Synadia, has 25+ years of messaging experience, including periods at TIBCO and Google. He created NATS to be the microservices transport for Cloud Foundry during his time at VMware. Moved to Apcera, NATS was maintained and cultivated into a popular messaging system with drastically improved performance and greater visibility and awareness throughout enterprise and open source communities. NATS stewardship was moved to Synadia at the beginning of January 2018, and NATS became a CNCF-hosted project in March 2018.

Current position

Synadia currently has eight employees located around the US, in California, Oregon, Colorado, Minnesota, and Texas. Synadia expects large revenue growth of over 3,000% for 2019.

The company does not have exact numbers for its user base, mainly because it is open source. But its Docker image has been downloaded over 30 million times and there are more than 200 contributors to the project with 30+ public repos and 8,000+ GitHub stars across repos.

Users and adopters include Acadiant, Apcera, Aporeto, Baidu, Bridgevine, Capital One, Clarifai, Cloud Foundry, Comcast, Ericsson, Faber, Fission, General Electric, Greta, HTC, Logimethods, Netlify, PEX, Pivotal, Platform9, RapidLoop, Samsung, Sendify, Sensay, StorageOS, VMware, Weaveworks, and Workiva.

Implementation partners include Bitnami (Bitnami Application Catalog, Azure Marketplace) and Logimethods. Technology partners are Ericsson, GE, VMware, Pivotal, and Siemens.

Product roadmap

Synadia is currently building a new technology to allow clusters of NATS servers to achieve a network of millions of endpoints, planned to be released in 4Q18. A revolutionary new end-to-end security mechanism utilizing the Ed25519 public keys and JWT for authorizations will be provided in 1Q19.

Data sheet

Key facts

Table 1: Data sheet: NATS

Product name	NATS	**Product classification**	Message-oriented middleware (messaging)
Version number	1.2.0	**Release date**	July 2018
Industries covered	All industries	**Geographies covered**	Global
Relevant company sizes	NATS can be found in companies of all sizes.	**Licensing options**	NATS is free open source software, Apache 2.0 licensed.
URL	https://nats.io	**Routes to market**	NATS website, word of mouth through the open-source community, conferences, meet-ups, partnerships
Company headquarters	Los Angeles, CA, US	**Number of employees**	8

Source: Synadia

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Authors

Martin Gandar, Associate Senior Analyst

martin.gandar@ovum.com

Michael Azoff, Principal Analyst, Infrastructure Solutions

michael.azoff@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum
TMT intelligence | informa

CONTACT US

ovum.informa.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo