ORACLE

Oracle Autonomous Database

Technical Brief Series: The Industry's First Self-Securing Database

July, 2020

Public

PURPOSE STATEMENT

This document focuses on the **Self-Securing** attributes of the Oracle Autonomous Database. Autonomous Database is a service offering based on Oracle Database (version 18c and later), which runs in the Oracle Cloud. Self-Securing, combined with Self-Driving and Self-Repairing attributes, comprise the 3 key categories of autonomous capabilities within the Oracle Autonomous Database.

The initial sections of the paper are appropriate for business-level audiences. The details that follow may be more useful for DBAs and IT managers who are unfamiliar with the more recent Self-Securing capabilities of Oracle Autonomous. This document is part of a series of Oracle Autonomous Database white papers. Details on the Self-Driving and Self-Repairing capabilities of Oracle Autonomous Database are provided in separate Oracle white papers within this series.

The **“Introduction”** and **“What is an Autonomous Database?”** sections of this document are intentionally common to all of the Oracle Autonomous Database white papers in this series.

DISCLAIMER

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

TABLE OF CONTENTS

INTRODUCTION[i]

Relational databases have made tremendous improvements in performance, availability and security over the past couple of decades. They can run up to 100x faster; can be configured for zero data loss; and have hardened security capabilities that can protect against malicious internal and external threats. These attributes have been enhanced by cloud databases and infrastructure services that deliver elastic scalability and provisioning for real-time agility and growth. Although a great many databases will remain on-premises due to regulatory and data residency requirements or just to satisfy data access latency for highly connected systems that are difficult to move to cloud, many Database workloads that were deemed too large or "mission critical" to run outside corporate data centers just a few years ago now run in public clouds. In addition, capabilities such as database resource deployment, monitoring and management can also be automated, leading to greater operational efficiencies and cost savings. So, what's missing? The degree of manual intervention required to manage today's cloud databases and all of the above attributes inhibits true Database as a Service – as a utility, or driver-less offering, if you will. As a result, enterprises are unable to realize the full operational and financial benefits of the cloud.

WHAT IS AN AUTONOMOUS DATABASE?[ii]

There is understandably an element of confusion that arises when talking about "automatic" versus "autonomous" capabilities. A process for database backup, failover or resizing that can be accomplished ***automatically*** is still not ***autonomous*** if a database administrator has to respond to an alert, make decisions and click a few buttons (or type a few commands) in order to initiate the automated activity.

A more dramatic example is when an alert related to a component outage or performance degradation appears automatically on a management console, but doesn't provide sufficient information to diagnose the problem, determine its root cause or offer a definitive recommendation for resolution. The automation literally stops with the alert. What happens next and how long it takes until resolution is unclear.

By contrast an autonomous database combines the dynamic agility of the cloud with the intelligent responsiveness of applied, adaptive machine learning. The design goal is to minimize or eliminate human labor – and associated human error – and ensure data safety and optimal performance. Businesses will find that autonomous capabilities can further help IT staff improve efficiencies by enabling them to focus on higher value activities in lieu of mundane, time-consuming tasks. This is significant considering that up to 75% of IT budgets are spent on manual database management.[iii] An autonomous database can help organizations transform IT operations into a modern cloud model that lowers operating expenses, eliminates costly downtime and ultimately enables them to innovate more while using fewer resources.

Oracle Autonomous Database is designed to deliver the above benefits across 3 primary categories, all accomplished with minimal to zero human intervention.

- **Self-driving**: The Autonomous Database automates database and infrastructure provisioning, management, monitoring, backup, recovery and tuning.
- **Self-securing**: The Autonomous Database is more secure than a manually operated database because it automatically protects itself from internal and external vulnerabilities and attacks. The Oracle Cloud provides continuous threat detection, while the Autonomous Database automatically applies all security updates online and provides "always on", end-to-end encryption. This preventative approach is critical because 85% of security breaches today occur after a CVE (common vulnerability and exposure) alert has been issued. [iv]

- **Self-repairing**: The Autonomous Database provides preventative protection against all unplanned and planned downtime – and rapid, automatic recovery from outages without downtime. Autonomous Database availability and performance management is taken to the next level thru the use of AI-based autonomy that integrates multiple areas of diagnostics and enables analysis and action to be taken at runtime to minimize or eliminate operational disruption.

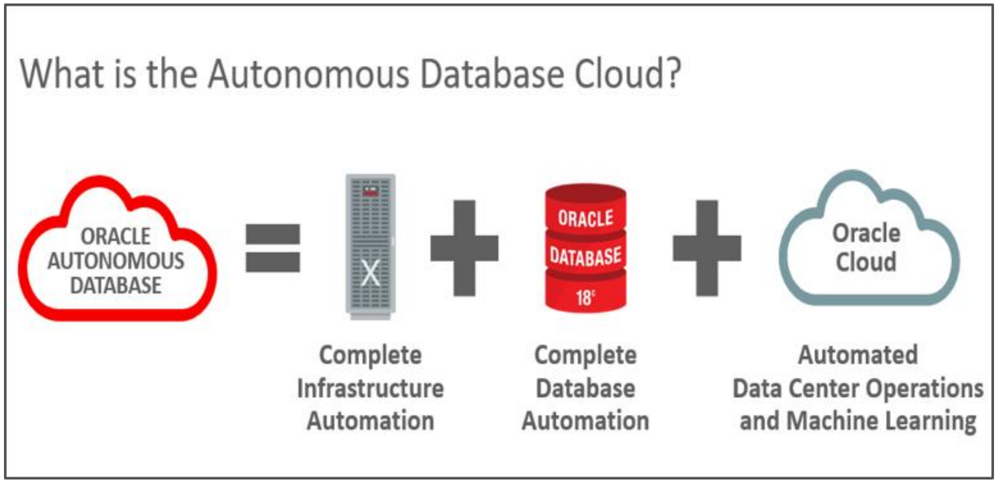
What is the Autonomous Database Cloud?
ORACLE AUTONOMOUS DATABASE
=
Complete Infrastructure Automation
+
ORACLE DATABASE 18c
Complete Database Automation
+
Oracle Cloud
Automated Data Center Operations and Machine Learning

Image 1. Autonomous Database Components in Oracle Cloud

UNDERSTANDING THE NEED FOR SELF-SECURING

Organizations of all sizes are becoming well versed with the risks associated with data theft, misuse of data, and inappropriate access to data. The growing cost of post-breach fines and litigation, combined with regulatory penalties for failure to adequately protect data, make securing sensitive data a top priority for most organizations.

While the importance of securing data continues to grow, the resources available to work on securing the data are simultaneously becoming scarcer. Security administrator jobs typically go unfilled for between six to nine months[v]. The global cybersecurity workforce shortage is projected to reach 1.8 million by 2022, with 68% of workers in North America attributing the shortage to a lack of qualified personnel[vi].

Nearly 60% of organizations that suffered a data breach attribute the incident to a known, unpatched vulnerability[vii]. Organizations wait an average of six months before applying security patches to critical systems – usually because they "can't afford downtime caused by rebooting critical systems"[viii]. Unfortunately, attackers work to leverage security vulnerabilities as soon as they are known – thus creating a security "patch gap" that has resulted in some of the most spectacular data breaches of the past few years.

It’s about much more than just patching though; good security hygiene for sensitive data requires properly configuring the system (including patching), but it also requires encrypting the data within the system, controlling access to that data, and monitoring access to that data for anomalies. The answer is to automate as much of the routine security work as possible – and the Autonomous Database is the first solution to do this.

ORACLE’S LEADERSHIP IN SELF-SECURING CAPABILITIES

Oracle has been a leader in database security for over 40 years. The Autonomous Database’s Self-Securing features are the culmination of decades of both development effort and experience running critical workloads for some of the most demanding customers on the planet.

The Autonomous Database takes care of some of the most common and time consuming security requirements, including: encryption (both at rest and in motion), separation of duties, collection of audit data, patching, upgrades, and reducing the opportunity for human error.

Oracle has addressed these issues on-premises for decades using database technologies like Advanced Security, Database Vault, and Real Application Clusters[ix]. Properly applied, these security capabilities are part of the Oracle Maximum Security Architecture (MSA). The MSA is a comprehensive set of security controls that can be configured to address almost any security requirement – from enforcement of trusted path access to fine-grained access control. The MSA portfolio is also available in the Oracle Cloud and has been enhanced with automation and default deployment templates in the Autonomous Database. No other vendor offers the comprehensive autonomous self-securing database capabilities that Oracle does – on-premises or in the cloud.

WHY IS A SELF-SECURING DATABASE IMPORTANT?

A self-securing database is more trustworthy than a manually secured database. Automating basic security requirements like encryption and patching not only removes the element of human error, it eliminates the dangers that are inherent with competing IT priorities and an industry-wide tendency to procrastinate when it comes to applying security controls to databases. In Verizon’s 2017 Data Breach Investigation Report (DBIR), Verizon noted that “findings that aren’t patched quickly tend to go unpatched for a long period of time”[x] We can extend that to note that security controls that aren’t applied during initial system rollout or re-platforming frequently are never applied at all. It’s much more efficient to build security into a system than it is to bolt it on afterwards.

Analyses of over 400 on-premises database security risk assessments conducted globally by Oracle experts reveals that a surprising number of production databases lack basic security hygiene like encryption, auditing, and up-to-date patch levels. In most cases, the root causes of this security gap are lack of time and skills to do the work, and organizational inertia against change. The Autonomous Database solves both problems. It establishes a baseline security posture, including controls that reduce risk and improve compliance to meet data privacy requirements and security regulations.

Shifting responsibility for these routine security tasks to the database service frees up scarce security resources to concentrate on valuable efforts like enabling digital transformation, mitigating application vulnerabilities, and remediating access anomalies.

By replacing manual security tasks (especially patching) with extensive automation, Oracle Autonomous Database reduces security administration costs by up to 55%. Studies also show that 60% of breaches leveraged known vulnerabilities for which patches were already available. Automated patching can significantly reduce this security risk.

APPLICABLE ENVIRONMENTS FOR SELF-SECURING (AUTONOMOUS) DATABASES

Oracle Autonomous Database is an Oracle Database based database cloud service offering. While many security capabilities of Oracle Database are available both on-premises and in the cloud, a number of autonomous elements are unique to the Oracle cloud service offerings. Examples include autonomous patching, encryption by default, secure configuration and the enforced separation of duties inherent in the Autonomous Database model.

Although Oracle Autonomous Database is a cloud-only offering, enterprises that must keep data behind corporate firewalls to meet data sovereignty, regulatory or data access latency requirements can run the Autonomous Database on-premises using Exadata Cloud@Customer. Autonomous Database on Exadata Cloud@Customer can be deployed on-premises, and delivers all of the capabilities of Autonomous Database in public cloud from within the enterprise's data center.

The Autonomous Database can be deployed in a hybrid cloud or all-cloud model; for example, when multiple databases are deployed for production and test environments or as primary and standby systems in a disaster recovery scenario.

There are no workload restrictions associated with the Autonomous Database or its self-securing capabilities. This includes transaction processing, mixed workloads that involve transaction and batch processing and reporting, as well as analytic workloads associated with data warehouses and data lakes.

WHAT CAN A SELF-SECURING CLOUD DATABASE DO?

The self-securing capabilities we've discussed so far are integral to Oracle Autonomous Database. They provide a baseline security posture that is already superior to most on-premises environments and are extensible enough to meet the most stringent security requirements with ease. Most of the Oracle Maximum Security Architecture (MSA) technologies are de-facto industry-standards for protecting and monitoring Oracle Database environments. The self-securing capabilities include:

- **Encryption for data in motion – Each Autonomous Database service is automatically configured to use industry-standard TLS 1.2 to encrypt data in transit between the database service and clients or applications. Required client certificates and networking information are automatically packaged for the service consumer when the service is provisioned.**

- **Encryption for data at rest – Data in the Autonomous Database is automatically encrypted using Oracle Transparent Data Encryption – first available with Oracle 10g in 2004. Transparent Data Encryption has been continuously enhanced and improved since its introduction. Automated encryption for data at rest and in motion are available only with Oracle Cloud.**

- **Automated separation of duties – The Autonomous Database completely eliminates direct access to the database node and local file system, thereby reducing threat surface. Further isolation between the service administrators and service consumers is provided through Oracle Database Vault, first available in Oracle Database 9i. This separation of duties – a key Oracle Cloud differentiator – not only reduces the risk of administrator malfeasance, it also eliminates the ability of the service administrators to view or modify data stored in the Autonomous Database. As with Transparent Data Encryption, Database Vault has been continuously enhanced and improved - with some new features added explicitly to support the Autonomous Database.**

- **Secure, locked configuration – The provisioning automation of Oracle Cloud Infrastructure ensures each autonomous database is provisioned via a security hardened gold image. No additional software components or malware can make their way in once the system is provisioned.**

- **Database auditing configured by default, customizable to meet your needs – Autonomous Database comes preconfigured using Oracle Unified Audit. This feature includes automated auditing for privileged user activity and logon failures and optional pre-configured policies for the Center for Internet Security audit benchmarks, account management, and much more.**

- **Reduced opportunity for human error – Human error plays a significant role in many data breaches and is one of the most difficult threat vectors to eliminate. The Autonomous Database minimizes the chances of human error by automating a significant portion of database administration. Opportunities for human error are further reduced by restricting the range of commands that an Autonomous Database service consumer is allowed to run.**

- **Automated patching, upgrades, and maintenance – One of the most significant advantages of the Autonomous Database is its ability to automatically apply security patches and upgrade them without downtime. Much of this capability builds on well tested, mature Oracle Database technologies like Real Application Clusters (for rolling online RAC patches) and cloud service process automation. The latter draws from experience accumulated over decades – starting with Oracle's On-Demand hosting service, progressing through Oracle Managed Cloud Services and further evolving in the Oracle Cloud.**

- **Managing security across database fleet and development processes – Autonomous databases can leverage OCI Data Safe security service to further enhance database security across entire fleets. Data Safe provides automation for centralized auditing, compliance assessment, sensitive data discovery and data masking. Data masking prevents sensitive data from leaking into non-production environments, streamlining a secure application development process.**

- **Industry standard compliance – Autonomous databases come pre-certified for ISO, SOC1/2, and HIPPA. PCI, FedRamp and C5 certifications are expected in the near-term.**

Together, these capabilities within the Autonomous Database provide a security framework that covers the core security requirements for most organizations out of the box, freeing up operations and security teams to elevate enterprise security posture to the next level.

CONCLUSION

No databases that run on-premises or in cloud environments today are 100% autonomous – but that is the goal toward which the industry is headed. To further the evolution of cloud databases toward this true utility model, Oracle introduced the Autonomous Database, running on Oracle Database (version 18c and later) in the Oracle Cloud. Autonomous Database minimizes or eliminates human labor using self-driving, self-securing and self-repairing functionality. The self-securing capabilities of the Autonomous Database leverage both the Oracle Maximum Security Architecture (MSA) and Oracle operations best practices. Oracle MSA combines advanced technologies, best practices and autonomous functions to proactively protect against common attack vectors, and free up scarce security resources to focus on higher-value activity. Self-securing capabilities include encryption, access control, automated patching, and auditing. This collection of self-securing capabilities offered by the Oracle Autonomous Database is unmatched by any other cloud (or on-premises) database in the industry.

[i] The “Introduction” is intended to be common for each of the three Oracle Autonomous Database White Papers that focus on Self -Driving, Self-Securing and Self-Repairing attributes.

[ii] The “What is an Autonomous Database” section is intended to be common for each of the three Oracle Autonomous Database White Papers that focus on Self-Driving, Self-Securing and Self-Repairing attributes.

[iii] IDC Perspective, “Oracle’s Autonomous Database: AI-Based Automation for Database Management and Operations”, Feb. 2018

[iv] Verizon - 2018 Data Breach Investigation Report

[v] Cybersecurity Ventures 2018 - https://cybersecurityventures.com/jobs/

[vi] ISC2 Global Information Security Workforce Study 2017 https://iamcybersafe.org/gisws/

[vii] Ponemon “Today’s State of Vulnerability Response” 2018

[viii] 0Patch. “Security Patching is Hard” 2017

[ix] Oracle RAC is also an integral part of Oracle Maximum Availability Architecture (Oracle MAA)

[x] Verizon Data Breach Investigation Report 2017 – Appendix D “The Patch Process Leftovers”

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

Oracle Autonomous Database
August 2020