White Paper

The Security Benefits of a Fully Managed Database Service: Oracle Autonomous Database

Sponsored by: Oracle Corp.

Carl W. Olofson
March 2020

IN THIS WHITE PAPER

In this white paper, we consider the important role of security features such as detection and protection of privacy-related and other sensitive data, detection of improper or suspicious access, and control of database access in a comprehensive way. We also look at timely patching of database management system (DBMS) software, especially where security patches are involved. Patching is done on an infrequent basis in most datacenters, exposing the database to risk in the delay. This white paper discusses that risk and related factors involving database unavailability. It also looks at other security concerns and how they may be addressed through technology.

One might think that moving to a managed database service in the cloud would solve the availability problem, but these services may still require interaction between the customer and the service provider, resulting in database unavailability during the patching process. Handling most security issues remains the user's responsibility, but without proper tools and features, this can be problematic at best. The Oracle Autonomous Database Cloud Service, by contrast, overcomes these issues, providing timely patching without downtime for continuous availability but with maximum security and a range of capabilities that enable users to properly monitor and secure their data.

SITUATION OVERVIEW

The Patching Issue

Computer software is never in a steady state. It requires constant improvement and updating. Some of this effort has to do with shifting usage models or the correction of previously undetected problems, but a great deal has to do with countering vulnerabilities that may be found and exploited by bad actors. This is especially important for databases, where breaches result in significant liability for the enterprise. These updates are applied through patching.

What Is Patching?

A patch is a piece of code that is inserted into existing software to alter its behavior. It may represent a fix to a known problem, a much-requested enhancement, or the removal of a security vulnerability. Applying a patch to a database server normally requires taking it offline to modify the code and then bringing it up again.

Why Is Patching Such a Problem?

If a delay in patching exposes the enterprise to potential hacking, why isn't a patch done right away? Because patching requires both downtime and staff time, it must be scheduled for off-hours. Even at night, however, taking the database offline is going to inconvenience someone, and in the case of a 24 x 7 availability requirement, an offline option is not possible. The alternative is to set up a second database server, load the software, apply the patches, test the patched system, and then swap servers. This approach usually results in brief interruption as one server is quiesced, the last transactions are passed over to the other system, and then the other system comes online. So patching causes extra staff effort, interrupts other work, and disrupts the operations schedule. These activities can represent considerable cost. Most users have many database instances, and the total staff time cost can be calculated at roughly an hour per instance. Even if the patch itself only takes 15 minutes, the process of taking the system offline, applying the patch, verifying the patch, and bringing the system back online can take an hour altogether. And that doesn't even take into account the operational disruption as systems administrators and other operations staff must work around this activity. This is why patches are not usually applied as they come in but instead are batched up and applied in bunches at some scheduled time.

What Are the Risks of Delayed Patching?

When patches are not applied in a timely manner, problems that have been fixed in the current code base are not addressed, improvements are not available and, most importantly, known vulnerabilities are still present, exposing the database to potential hacking. Such delays also create problems. How many DBAs get that sinking feeling when they call in with a problem, and the first question the support engineer asks is, "What is your patch level?" If it's not current, the advice may be to get up to the current patch level and then call back if the problem persists. The security risk is particularly significant. Once patches are issued to address a vulnerability, that vulnerability becomes widely known and hackers are looking for databases that have not yet been patched. So the danger of delayed patching is considerable.

Cloud Service Patching

Moving to the cloud can address the problem of timely patching, yet this is not necessarily a perfect fix. In many cases where a public cloud service is involved, the user may operate under a "shared responsibility model" that places physical responsibility for the system, including its security, in the hands of the managed cloud provider but leaves responsibility for the state of the software, including patching, in the hands of the user. Here, once again, the patching effort must be done by staff and results in downtime.

Even some managed cloud database providers that offer full software support for the database server may need to schedule patching with the user because the patching operation causes an interruption in service. This alone could compel some users to batch up patches rather than have them applied as they come in.

What's Required to Address the Patching Issue?

The only way to ensure the timely application of patches is to use a service that offers a nondisruptive patching process. This obviates the need to delay or batch up patches and ensures that the database servers are running with the latest version, including the fixes for all known security vulnerabilities. The critical nature of this capability should be obvious.

Other Security Issues

System-Level Security

Managing security at the network, OS, VM, and container level can be tricky at best. Coordinating security definitions across all these levels requires tools that make such settings straightforward to define and modify. While the mechanics of the network, OS, VM, and container-level security are the responsibility of the cloud service provider, how they are set is up to the user. Tools that are inconsistent in operation, or difficult to use, make that job so much harder.

Protecting Sensitive Data and Ensuring Compliance

Some sensitive data is relatively easy to identify and protect; data that is formally defined for that purpose under some law, regulation, or contract can be discovered and defined appropriately, to prevent unauthorized access. Personally identifiable information (PII), on the other hand, is trickier, especially with the range of emerging privacy regulations, including GDPR, HIPAA, CCPA, and hundreds of other data privacy regulations. In some cases, protecting specific field data is not enough. It is necessary to prevent access to combinations of data that could compromise a person's identity as well. Proper tooling can ensure that those efforts can be done efficiently and consistently.

Sometimes, elements of PII may be embedded in a text field or may be labeled in an obscure or confusing way. Tools that can detect such PII are vital to ensuring that the enterprise remains in compliance, and out of legal trouble.

Obviously, when database applications change, they need to be tested against realistic data — data of the same volume, range of values, and distribution of values. But using real data is out of the question because to do so would enable developers and testers to see it. So a sophisticated data masking approach is called for, one that can produce useful test data that exercises the application just as the real data, but with no elements that could compromise real sensitive data.

Protection from the Cloud Service Vendor

Wait … what? Do we need to be protected from the cloud service vendor? Well, technically, yes; because any access to sensitive data by an unauthorized person can be considered a violation. So although the cloud service vendor may need to be able to see and manipulate the database operational settings, and even the schema, the vendor should not have access to the data itself.

Protection from Malign Access

A constant concern is that of suspicious activity, which may indicate either an external attack or improper access by an internal user. Although there are numerous tools available that can perform database log analysis and identify such activity, it is always up to the data management team to take action, usually well after the fact. What's needed is a database system that can respond immediately when a potential breach is detected while keeping DBAs in the loop. Such detection would include suspicious patterns of access both at the time of access and later (through log analysis, for more sophisticated kinds of breaches).

Oracle Autonomous Database

Oracle Autonomous Database is a managed cloud database service. It is offered on the Oracle Cloud. For customers that need to keep the data in the datacenter, for either legal or operational reasons, Oracle also offers Oracle Exadata Cloud at Customer, which is a physical system that is managed remotely by the Oracle Cloud team yet is situated locally in the customer's datacenter.

A Full Cloud Database Service

As a full cloud service, Oracle Autonomous Database is delivered in a way that ensures all operational chores are taken on by the Oracle Cloud team. Upgrades and patches are applied as a matter of course. The system is also self-tuning, using machine learning algorithms to improve performance by tuning on a continuous basis. The system is designed for transparent rolling upgrades, which means that patches can be applied as they come in and without any interruption of service. This also means the user does not need to think about scheduling the patch or worry about downtime.

Automatic Patching

Oracle's Approach to Patching

Oracle applies all security patches immediately and others on a scheduled basis. Patching is done on a rolling basis, which eliminates downtime, ensuring that the database is continuously available. Oracle can do this because the hardware is configured for nonstop operation, and the software provides a smooth cutover from server to server. Oracle's long history of server clustering for uninterrupted operation — most notably in Real Application Clusters (RAC) introduced in 2001 — has made this possible. The flexibility afforded by the self-tuning functions of the Oracle Autonomous Database software ensures smooth performance throughout. This technology is the result of decades of research and development at Oracle and first rose to prominence with the self-managing features of Oracle9i. The patching and patch testing processes take place behind the scenes, so the effect is to make the patch process seem virtually undetectable by the user. Contrast this with the manual and error-prone processes of other patching methods.

Other Security Features of Oracle Autonomous Database

Oracle Autonomous Database offers five key additional areas of functionality to ensure the security of the database, besides patch management. These are as follows:

- **Encryption.** Oracle offers *always-on* encryption for data at rest and in motion. Data is transferred from storage to processing nodes encrypted. It is even kept encrypted in cache. This function is enabled automatically.
- **Separation of the duties of data management and database administration.** Oracle is using features such as Database Vault and the Pluggable Database Lockdown profiles to isolate database administration (managed by Oracle) from data administration (managed by the Autonomous Database customer).
- **Audit.** Data auditing is automatically configured and enabled and in constant operation. The database system records suspicious patterns of access and includes the flexibility to extend analysis of the collected data to other services or even to on-premises security information and event monitoring systems.
- **Dedicated infrastructure.** Optionally, users may request infrastructure dedicated to the service of their databases only, thereby delivering physical isolation, which is required by some data security regimes.
- **Data Safe.** Data Safe is a unified database security control center that detects risks introduced by users, data, and configurations through continuous monitoring.

Oracle Data Safe

Oracle Data Safe is composed of a comprehensive set of security features for Oracle Cloud Databases, including Oracle Autonomous Database. It includes the following areas of functionality:

- Security assessment
- User assessment
- Activity auditing
- Data discovery
- Data masking

These capabilities are delivered through a single database security control center that allows customers to identify sensitive data and mask it, flags risky users and system configurations, and monitors database activity to quickly discover suspicious attempts to access data. The control center is designed to be easy to use and to save time in performing these critical security tasks. Its design principles include tightly integrated features and reporting, risk dashboards, and extensibility to support new security features. In addition, the control center's security data is physically isolated. Its data masking is designed to provide full protection of PII using over 50 predefined masking formats and a range of mathematically based masking transformations.

FUTURE OUTLOOK

IDC believes that most enterprise data will move to the cloud in five to seven years and that, as this happens, the security of that data will be improved. Still, capabilities such as those of the Oracle Autonomous Database may prove to be key to the decision as to which RDBMS to entrust with valuable and sensitive enterprise data going forward. The volumes and changeability of that data will continue to grow rapidly, and the challenges in identifying data for protection and establishing methods that ensure such protection without impeding database performance will continue apace.

CHALLENGES/OPPORTUNITIES

Moving data to the cloud eliminates most of the common methods of illicit data access, including poorly configured servers and "backdoor" passwords that often exist in enterprise datacenters. Oracle Autonomous Database covers much more ground in securing data. But bad guys are clever, and unforeseen methods are bound to occur. Even as competitors look to catch up with the security methods outlined in this document, new threats will loom over both Oracle and Oracle's competitors in the area of database security that will require vigilance, creativity, and foresight to overcome.

CONCLUSION

Database security is threatened by several factors, some of which involve application design and development but others that involve the database management system. When vulnerabilities are found by the DBMS developer, patches are issued to correct these vulnerabilities. Delays in applying such patches leave databases open to attack. Such delays can occur because of the cost, risk, and operational disruption involved in applying patches manually.

Oracle's approach to this problem with the Oracle Autonomous Database allows for the timely and automatic application of security patches without the risk of manual work (because it is automated) and

without operational disruption. This may involve moving the data to the Oracle Cloud or keeping the data in the local datacenter using the Oracle Cloud at Customer offering. In either case, Oracle Data Safe should be a key element of the overall data security plan.

The benefits of this service to the customer with respect to database security include the following:

- Elimination of the cost and risk associated with manually applying security patches
- Timely, automated application of security patches, ensuring that the latest updates have been applied against all known vulnerabilities
- Data Safe, which enables a comprehensive way to manage database security
- Other features that enhance database security, including encryption of data both in motion and at rest, automatic and continuous activity auditing, and Database Vault, which ensures that only those personnel who actually work with the data can see the data

Considering these benefits, IDC recommends that users do the following:

- Ask the question, "How often do we apply security patches, and how many known vulnerabilities threaten our data?"
- Calculate the labor and operational cost of applying security patches — including disruption and the risk of human error — to determine how much the current practice is costing the enterprise.
- Other questions to ask are, "Do we know where all our sensitive data is, who can see it, and whether it is putting us at risk?" and "Are we confident that we can detect and defeat inappropriate data access?"
- Consider a system that applies security procedures automatically, managed by a professional team of experts, as well as a comprehensive data security management facility as an alternative to the current security methods.
- Evaluate the potential benefits of Oracle Autonomous Database in ensuring database security is taken to the maximum.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com