Solution Showcase

Oracle ZDLRA: Fiduciary-class Data Recovery for Financial Services Organizations

Date: November 2016 **Authors:** Jason Buffington, Principal Analyst; and Mark Peters, Practice Director & Senior Analyst

Abstract: In financial services, data *is* the business; therefore, timely and accurate data recovery is equivalent to timely and accurate business resumption. Oracle Zero Data Loss Recovery Appliance (ZDLRA) is a purpose-built Oracle Database recovery appliance offering "fiduciary-class" data recovery, which is designed to meet the stringent data and business recovery demands of this particular industry.

The Specific Data Recovery Needs of the Financial Services Industry

For decades, IT professionals and risk management officers in the financial services industry have relied upon the same general-purpose backup and recovery solutions as other industries. However financial services businesses are often held to a higher standard, which is both heavily regulated and has stringent data availability/accuracy requirements—in financial services, some of the latter are self-imposed for competitive advantage, but most are a result of the *fiduciary* responsibilities (whether to investors, customers, regulators, or the government) that are simply part of being in the finance business.[1,2] While the old adage "if it ain't broke, don't fix it" is often used when the status quo is "good enough," the truth is that traditional backup and recovery technologies are often insufficient for the heightened demands of the financial services industry (where, for instance, heavy fines can be levied if regulators' demands for data regarding specific transactions cannot be delivered rapidly). What's specific about the financial services industry from a data protection and recoverability perspective is the myriad issues that it must address:

- Market situation and vulnerabilities: Data security is top of mind these days.[3] From rampant attacks of crypto-ransomware, through failed backups and restores causing downtime outages that can cost millions of dollars per hour, to lost transactions that can never be recovered, it is clear that *data protection matters* in financial services.
- Regulatory environment: Governance and compliance requirements span an array of acronyms (FACTA, SOX, SEC, among many), but all demand 100% data accuracy and recoverability; indeed, new OCC guidelines that come into force in January 2017 impose stringent and enforceable *recovery* goals for large financial organizations.[4]
- The essential business of handling money: Almost every I/O transaction (within a computer) is a monetary transaction (between two parties that supposedly trust each other). A lost I/O transaction is quite literally a lost financial

[1] Note: Limited elements of this ESG Solution Showcase have been adapted from an ESG Blog, *Better Business Protection – Fiduciary Class Data Protection*, published November 2016 and written by the same authors.
[2] The Merriam-Webster Dictionary defines "fiduciary" as "*relating to or involving trust (such as the trust between a customer and a professional).*"
[3] Cybersecurity is the most-cited IT priority this year by a wide margin, per ESG's Research Report, *2016 IT Spending Intentions Survey*, Feb 2016.
[4] Source: OCC Bulleting 2016-30: Enforceable Guidelines for Recovery Planning: Final Guidelines, September 2016. Full details here.

transaction, so *data loss of any kind is unacceptable*. Moreover, even a moment of downtime—the lack of availability of data/applications—is a moment when trust between the parties is violated, thereby undermining long-term confidence (a key element within "fiduciary responsibility").

Underlying most of these mission-critical applications is a transactional database (very often from Oracle in the finance industry). If every I/O directly equates to money, then business success is relying on an organization's business processes, which are in turn dependent on the IT systems, which are entrusted to the organization's *fiduciary* care…and therefore their operation and protection demands demonstrable best approaches and efforts.

But what about the data itself? In many industries, an acceptable focus is just *backup*, with less focus on *recovery* (meaning that variable recovery times and even some amount of data loss—e.g., a few pixels of a video, a late order dispatch, one less mailer, or a test rerun—is acceptable). While data protection remains crucial in the financial services industry, the focus must be more weighted to data recovery and availability, as it directly translates to, for example, the ability to trade, provide accurate account details, price stocks, and so on. Any impact to data availability can generate immediate and significant adverse business impacts—significantly more so than in most other industries. Something better than typical "one size fits all" data protection and recovery toolsets is needed because such platforms are not optimized for zero downtime and zero data loss, nor to specifically deduplicate transactional databases, rather than plain files.

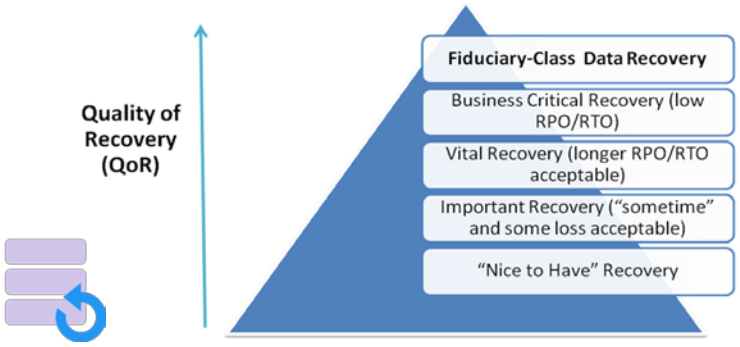
Said another way, financial services is an industry where the confluence of having to deliver 100% across three vectors—being digital, being secure, and being available—creates a demand for IT offerings to deliver against this extremely high level of "digital trust" that simply didn't exist until recently.

'Fiduciary-class' Data Recovery

While data backups are performed regularly in just about all IT organizations, all too often IT professionals mistakenly assume that they can magically go from there to *business* recovery. "Backup" gets a lot of the attention, but it is always "recovery" that ultimately matters. Acknowledging that not all applications and workloads are equal, we need to also define different levels of recovery, especially to add a new tier that delivers on the "digital trust" demands; after all, the mere setting of Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs)—or at least anything other than "instant with no loss"—inherently assumes that there will be *some* delay, and maybe even *some* unrecovered data. While that may work for some types of data and some industries, it does not work for mission-critical applications in financial services, which need a new "ultra-level" of data—that is, *business*—recovery.

These distinctions should also be applied to some other industries, but it makes sense that the idea and term "fiduciary-class data recovery" would first be introduced in reference to the mission-critical databases that power the financial industry, many of which run on Oracle Database, as the highest tier of the "quality of recovery" hierarchy (see Figure 1).

FIGURE 1. An Expanded Hierarchy of Recovery



Source: Oracle, 2016

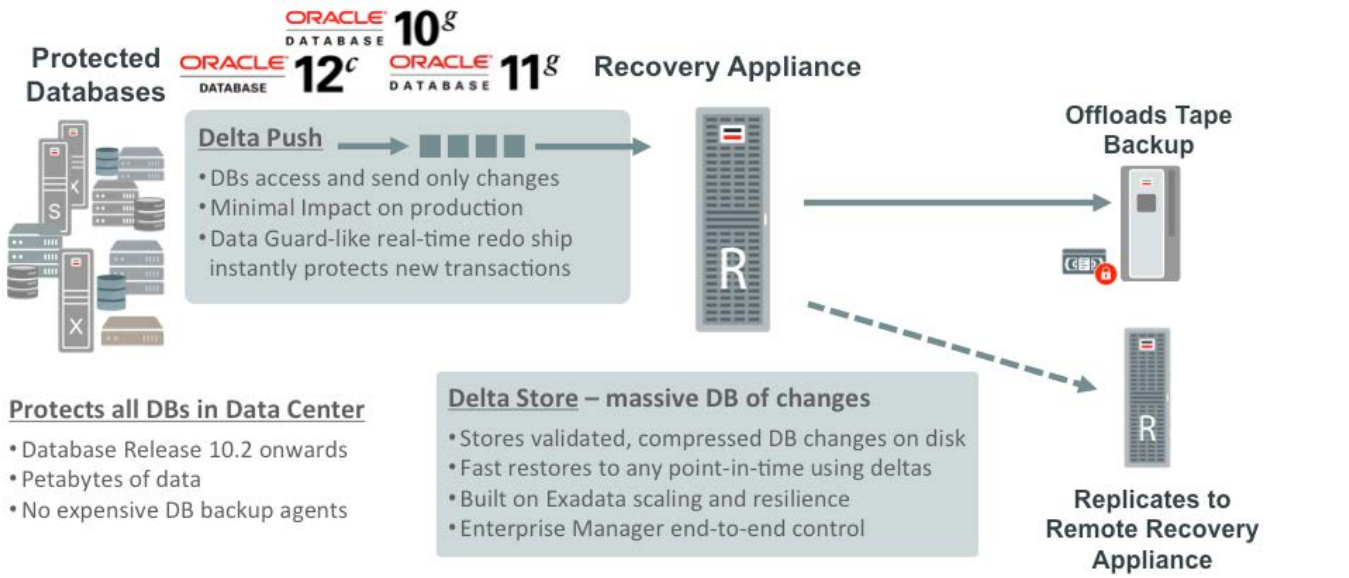
Fiduciary-class data recovery should be thought of as a prerequisite for the financial services industry (an industry often inextricably identified with the term "fiduciary responsibility") because terms like "mission-critical [data recovery]" merely state an attribute of the data and a desire, whereas "fiduciary-class data recovery" represents an ability to fulfill on the trust and expectations that—respectively—the users and providers of the data have.

Therefore, fiduciary-class data recovery is focused on *the ability to recover ongoing transactions*, not just bits and bytes of random data. Thus, this class of recovery enables financial services companies to rapidly restore their Oracle databases to any point in time. From a pragmatic perspective, a fiduciary-class data recovery solution should ideally offer more than just extremely fast recovery from daily or weekly data backups; it should also reduce the risk of data loss exposure for the organization (that is, little to no lost data/transactions), and deliver a scalable, easy-to-use platform that can reduce complexity and thereby human error. It's not that traditional data protection tools categorically cannot be "amped up" to meet most of these qualifications, but often this combination of solution capabilities is best achieved when designed for a specific platform (instead of as a general-purpose utility), such as what Oracle has introduced with its Zero Data Loss Recovery Appliance.

Oracle ZDLRA Delivers Fiduciary-class Data Recovery

Oracle Zero Data Loss Recovery Appliance (the name says a lot) is a purpose-built Oracle Database recovery solution, which is part of Oracle's "Engineered Storage" portfolio. It has been built on and for Oracle Database, and it runs on a scale-out, high availability, no single-point-of-failure architecture platform. Designed as a fiduciary-class data recovery system, it should be thought of differently than conventional backup and recovery offerings. Built specifically for Oracle Database protection, it is unapologetically "best for Oracle" from not only an engineering perspective, but also from an operational perspective (simplifying database protection for both infrastructure and database administrators). As such, it meets all the solution merits described: ultra-rapid point-in-time recovery, zero data loss exposure, real-time recovery status, and end-to-end security and visibility, together with attractive "basics" (scalability and ease of use, since it is run from within Oracle Enterprise Manager), as seen in Figure 2.

FIGURE 2. Oracle's Zero Data Loss Recovery Appliance Overview



Source: Oracle, 2016

The Recovery Appliance leverages an Oracle Database for its catalog and can essentially record millions of transactions from thousands of databases and play them back with a mouse-click—much like how a DVR works for a home theater, which is a very different approach from general-purpose, file-centric backup tools. The fundamental change in how the

data is protected enables users to recover in a minimal amount of time to *any point in time.* In addition, its integration with and awareness of the Oracle Database means it can understand and track system change numbers (SCNs), allowing it to provide real-time recovery status for all databases under management. Put together, the appliance provides database-contextual visibility and insight that assures ZDLRA operators and beneficiaries—the likes of business unit leaders and operations personnel—that their data will be recoverable when it is needed most, eliminating the "unfortunate surprise" (and fiduciary failure) during restoration that a backup is corrupt.[5]

Being specifically designed for recovery, Oracle ZDLRA is therefore ideally suited to help financial services organizations meet a broad range of regulatory requirements; it enables these organizations to literally shift from "*protecting storage volumes on a schedule*" to "*protecting their most critical financial transactions in an ongoing way.*" It also addresses three other key financial services data needs:

1. Confidentiality: When using Oracle's NIST-certified end-to-end Transparent Data Encryption (TDE), data is encrypted within the database and remains encrypted in the backup (without sacrificing storage consumption).
2. Integrity: Achieved via continual database-aware validation/self-healing, strict policy adherence, and regulatory retention times.
3. Availability: Derived from a high availability architecture and built-in replication, together with continuous data protection and rapid recovery.

The Bigger Truth

Data availability, access, and trust are the foundations for all modern financial services. All must be optimized simultaneously to deliver against strong fiduciary responsibility demands and expectations. When it comes to data and applications, "*Yup, we've got that somewhere and we'll get it, or we hope most of it, to you sometime*" is not an acceptable modus operandi for this industry. Because of this, having traditional interval-dependent data protection and recovery—with RPO measured in hours or days and RTO requiring extra processing power from the production database servers— is also not acceptable.

If the IT groups in financial services organizations haven't ensured that every last transaction is adequately protected and suitably recoverable, then those organizations are not protected and responsible from a fiduciary perspective. When a recovery eventually fails—whether in timeliness or completeness—then the trust and confidence that underpins their business will be proven to be misplaced.

A fiduciary-class data recovery offering such as Oracle's Zero Data Loss Recovery Appliance can put such concerns to rest. Purpose-built for recovery of Oracle Database, which is the underpinning of many financial services firms, ZDLRA's unique and specialized approach is something that ought to be considered by any financial IT professionals who are trusted fiduciaries of the business systems and data that they, and therefore their clients and customers, truly trust and rely on.