VERITAS

# High Availability for Oracle Databases in the Public Cloud

Optimizing availability, security, and resiliency for Oracle databases.

White Paper | August 2023

VERITAS ALTA™

## Executive Summary

Most business-critical applications rely on a robust database management system to deliver a smooth and predictable end user experience. Oracle is one of the leading enterprise database management systems on the market, and Oracle Real Application Clusters (RAC) can provide better availability for your databases. However, there are some significant limitations with Oracle RAC that may hinder your ability to modernize your IT services with the freedom of architecture your business needs to be innovative and flexible.

Veritas Alta™ Enterprise Resiliency is an Oracle-certified solution that provides advanced storage management and high availability for Oracle databases, maximizing your application up-time and optimizing performance—on-premises and in the public cloud. Veritas Alta Enterprise Resiliency also helps safeguard your Oracle databases from the threat of ransomware attacks and data corruption, with advanced security and disaster recovery features that help keep Oracle databases highly resilient. Replacing Oracle RAC with Veritas Alta Enterprise Resiliency results in several key benefits that can improve operations for your business-critical databases:

- **Public cloud integration:** As a platform-agnostic solution, Veritas Alta Enterprise Resiliency enables you to run Oracle databases in any public cloud in a highly available single-instance configuration that delivers close to the same availability as RAC, at a reduced cost.
- **Performance and resiliency:** Accelerate database performance on-premises and in the public cloud with intelligent caching, resiliency, and disaster recovery options that can ensure zero data loss and near-zero recovery times.
- **Data security and integrity:** Veritas Alta Enterprise Resiliency's secure filesystem provides data immutability for Oracle databases that protects against ransomware attacks and data corruption. Additionally, Veritas Alta Enterprise Resiliency volume encryption protects your data against unauthorized access, and reduces risks associated with data exfiltration.

This solution brief will provide an overview of how Veritas Alta Enterprise Resiliency delivers a secure, resilient, and highly available foundation for Oracle single-instance databases that can be a compelling alternative to RAC—on-premises and in the public cloud. It will also provide deployment recommendations, and will include guidance on how to convert your Oracle databases from RAC to a single-instance configuration.

## Solution Value

As a proven market leader in application high availability, Veritas Alta Enterprise Resiliency is a multi-faceted solution for Oracle that delivers extensive functionality to enhance database security, availability, and resiliency as a single software-defined solution.

> *Veritas Alta Enterprise Resiliency adds significant value for Oracle single-instance databases by providing high availability similar to RAC, with less complexity and a much lower cost—with the flexibility to run in any public cloud.*

Veritas Alta Enterprise Resiliency delivers a full spectrum of functionality for Oracle databases that help ensure your IT services deliver a smooth and predictable end user experience.

- **Fast Failover:** Offers high availability, automation, and significant cost savings for Oracle single-instance databases when compared to Oracle RAC. Fast Failover can be configured in any public cloud environment, giving you the uptime you need in the cloud, with freedom of architecture that optimizes your costs and flexibility.

- **Security and ransomware protection:** Veritas Alta Enterprise Resiliency's SecureFS feature enables data immutability for Oracle databases by automating the creation of WORM files and checkpoints that cannot be modified. Checkpoints can be used to quickly recover your database in the event of a ransomware attack. Additionally, volume encryption ensures that your databases are protected against unauthorized data access, and limits the risk of data exposed due to exfiltration.
- **Disaster recovery and resiliency:** Veritas Alta Enterprise Resiliency manages and automates disaster recovery for Oracle databases in a variety of topologies that can be configured to achieve zero data loss (zero RPO) and very low recovery times (near-zero RTO). Veritas Alta Enterprise Resiliency's Global Cluster option orchestrates site-to-site service failover and replication—on premises and in all major public cloud platforms.

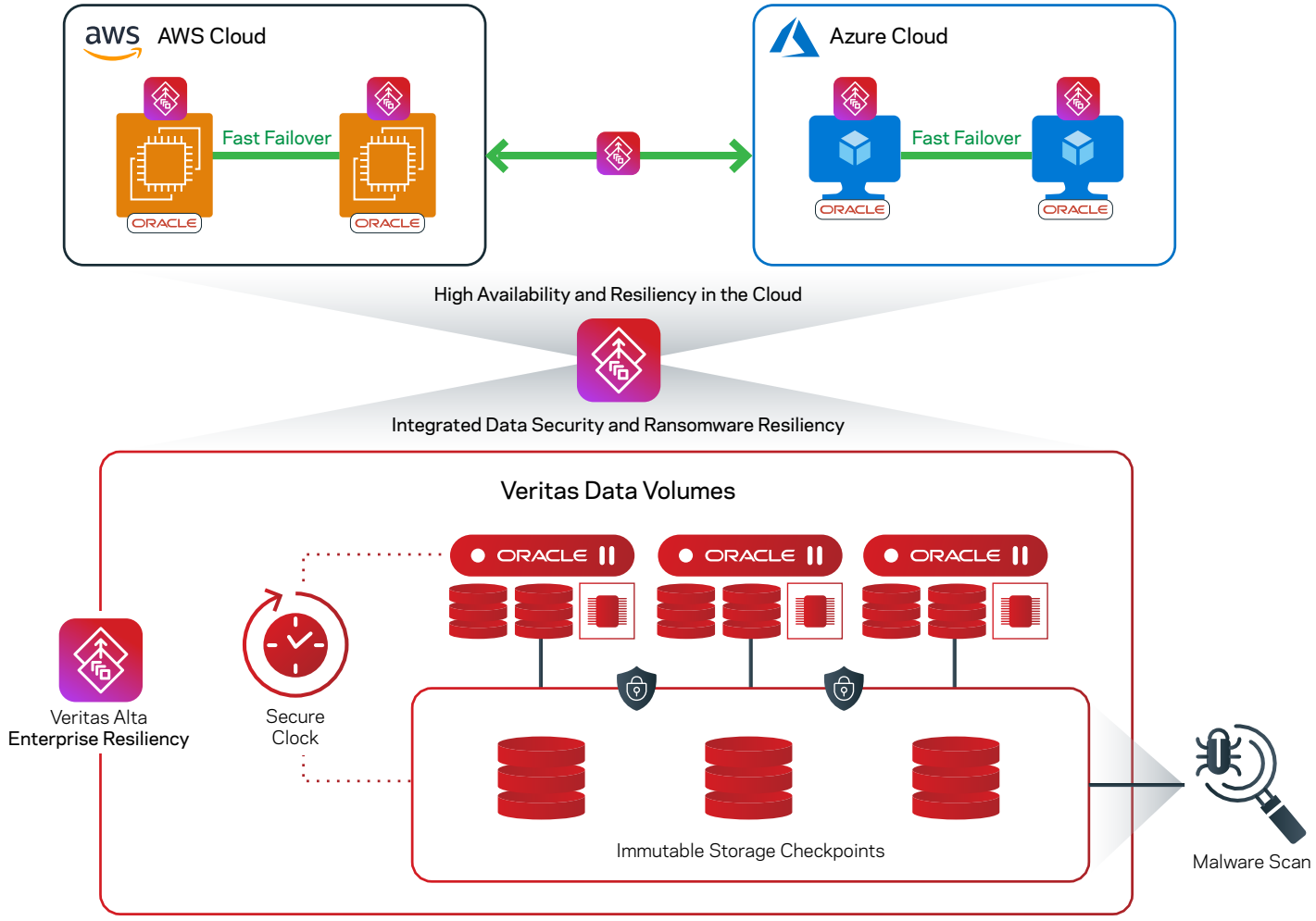



*Figure 1. Veritas Alta Enterprise Resiliency provides a highly available, secure, and resilient foundation for Oracle databases*

Modern business-critical applications demand availability and uptime—a requirement with direct implications for the underlying databases, operating systems, and storage management systems. Many organizations are cost-sensitive, and for some applications, a few seconds of downtime is acceptable. In these situations, the fast failover of a single-instance Oracle database using Veritas Alta Enterprise Resiliency provides a compelling alternative solution that offers fast failover while avoiding the considerable complexity, cost, and application tuning required by Oracle RAC. As a platform-agnostic solution, Veritas Alta Enterprise Resiliency provides fast failover for your Oracle single-instance databases, while giving you the flexibility to run in any public cloud environment—which is not supported with Oracle RAC.

### Solution Components

Veritas Alta Enterprise Resiliency is a proven platform for running Oracle databases that has evolved to include several advanced features not available natively in Oracle. Veritas Alta Enterprise Resiliency for Oracle includes the following components:

- **Veritas File System (vxfs):** An extent-based POSIX-compliant journaling file system capable of managing large volumes of data, designed to provide high performance and availability for applications. vxfs is fully supported in the cloud and has several advanced features that provide key security, performance, and resiliency benefits for Oracle databases.
- **Veritas Volume Manager (vxvm):** A storage management utility that manages physical disks as logical data volumes that are presented to an operating system as a storage device on which you can create file systems. vxvm volumes can be encrypted to help protect your Oracle databases against unauthorized access.
- **Cluster File System (CFS):** On-premises and cloud-native multi-access block storage services depend on a cluster file system to support parallel access to data by multiple compute instances. CFS is a feature of the vxfs that provides highly available, parallel access for Oracle databases deployed in a fast failover configuration. CFS provides better lock management than NFS-based storage services, and makes failover more reliable.
- **Flexible Storage Sharing (FSS):** A feature of CFS that allows you to create parallel access storage volumes on-premises and in the cloud. FSS allows logical volumes to be created using block storage, enabling a common storage namespace without requiring physically shared storage. Using FSS, Oracle single-instance databases can be made highly available by eliminating slow storage operations that would otherwise be required. FSS is transparent to file systems and applications, and can be implemented using on-premises block storage and most cloud-native block storage services.
- **Veritas Volume Replicator (VVR):** Enables platform-independent disaster recovery by intelligently managing replication for Oracle databases. VVR has several advanced features, including Adaptive Sync which improves sustained throughput for latency-sensitive applications by automatically switching from synchronous to asynchronous mode and vice versa based on latency. VVR can replicate Oracle databases between cloud zones, regions, from on-premises data centers to the cloud, and between different cloud providers. When integrated with the Veritas Alta Enterprise Resiliency Global Cluster option, VVR provides optimized data replication between geographically dispersed sites.
- **Veritas InfoScale Operations Manager (VIOM):** VIOM is a platform- and vendor-agnostic centralized management console for Veritas Alta™ Shared Storage that also provides some visibility into other third-party infrastructure. VIOM is used for monitoring, visualization, and management of system and storage resources. VIOM is also a reporting engine and can generate multiple reports, including a risk analysis report that can summarize issues that may arise within an environment that could reduce high availability and disaster recovery readiness.
- **Oracle Enterprise Manager plug-in:** Provides integration with Oracle Enterprise Manager (OEM), so you can efficiently manage Veritas Alta Enterprise Resiliency storage and clusters through OEM.

## Oracle in the Cloud

The public cloud has become a mainstream option for running business-critical workloads. With several cloud service providers available to choose from, it is important to have the flexibility to work with the cloud service provider that best suits your business requirements. If you're considering moving to the cloud and are using RAC in your on-premises environment, the lack of cloud provider support with RAC means that you may need to consider other solutions to provide high availability and resiliency for your Oracle database when migrating to a public cloud service.

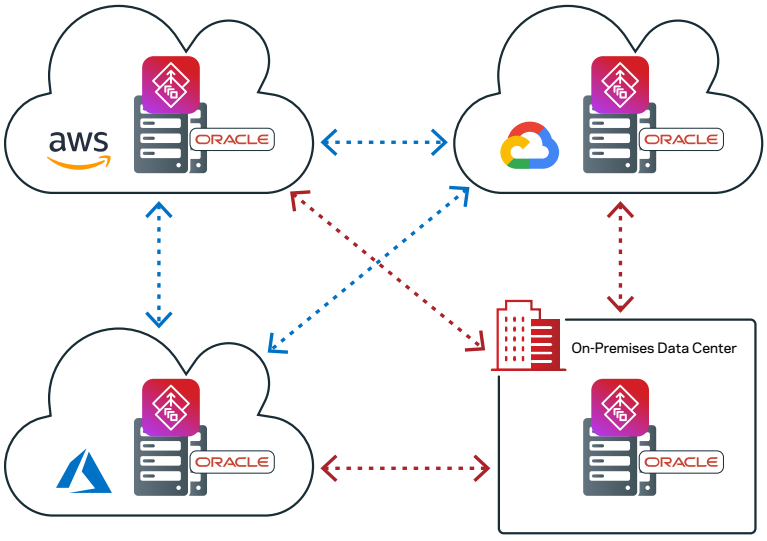



*Figure 2. Veritas Alta Enterprise Resiliency provides advanced resiliency for Oracle in the public cloud*

Veritas Alta Enterprise Resiliency's fast failover for Oracle single-instance databases can be configured in any public cloud platform, giving you the ability to provide high availability for your database in the cloud, without being locked into a single cloud provider.

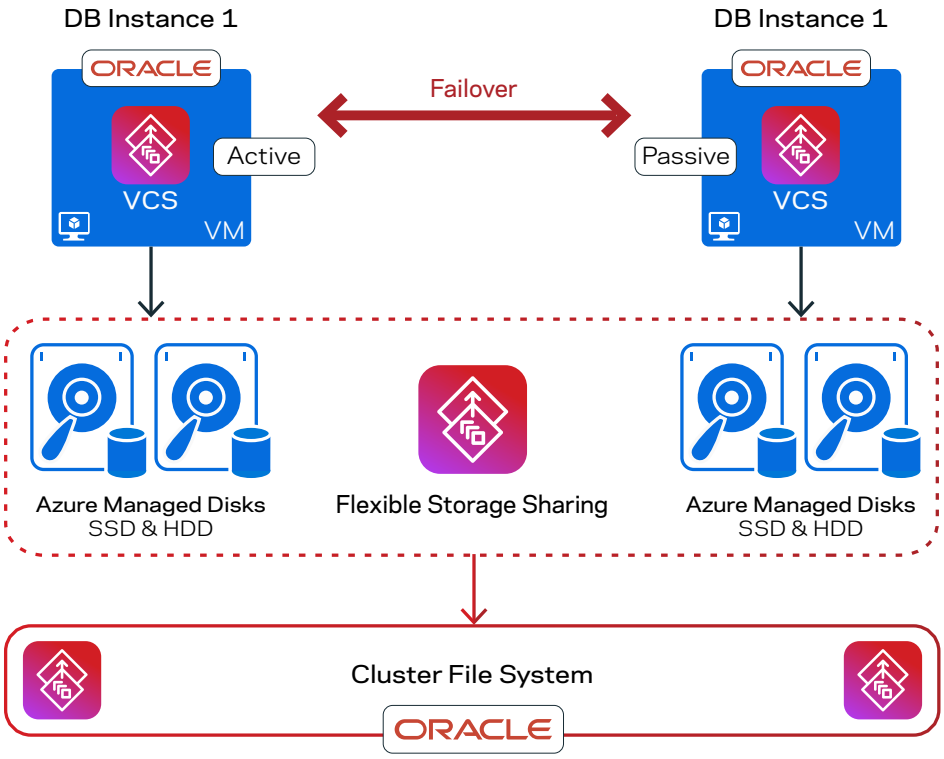



*Figure 3. Veritas Alta Enterprise Resiliency's fast failover solution for Oracle single-instance databases in the public cloud*

### Fast Failover for Single-Instance Databases

The Fast Failover solution consists of an active Oracle database instance accompanied by a passive system that is ready to take over if the active system fails. If the active system fails, the Oracle Database is restarted on the passive system (among other operations). This process makes database recovery very fast, as the storage is concurrently mounted on both systems, thus eliminating the slow storage operations required to start the Oracle database on the passive node.

Figure 3 is an example of how Veritas Alta Enterprise Resiliency fast failover works with an Oracle single-instance database in the public cloud. In this example, an Oracle single-instance database is shown deployed in Microsoft Azure with Veritas Alta Enterprise Resiliency providing parallel access storage for the database using block storage provided by Azure managed disks.

Veritas Alta Enterprise Resiliency can be deployed using cloud marketplaces, which helps simplify the deployment experience and reduces the time to value. Solution templates are available in the AWS Marketplace (AWS CloudFormation Template), the Azure Marketplace (Azure ARM Template), and the Google Cloud Platform Marketplace (Deployment Manager Template).

### Disaster Recovery and Resiliency

Ensuring that your applications can be made resilient and recovered with no data loss and minimal downtime is a key requirement for many business-critical applications. While Oracle provides some native options for backup, recovery, and resiliency, achieving zero data loss over any distance and a near-zero RTO requires additional configuration and tools.

Veritas Alta Enterprise Resiliency can support zero data loss for Oracle databases using what's known as a bunker configuration (shown in Figure 3). This configuration incorporates a bunker site into a standard primary/DR configuration, which is used to store logs that are being synchronously replicated from the primary site. This configuration does not require synchronous replication between the primary and DR sites, which is difficult to achieve and limits your options for geographic distribution of your Oracle databases to protect against localized outages. Veritas Alta Enterprise Resiliency delivers geographically dispersed resiliency for Oracle databases with zero data loss over any distance, and automated failover that enables near-zero recovery times.

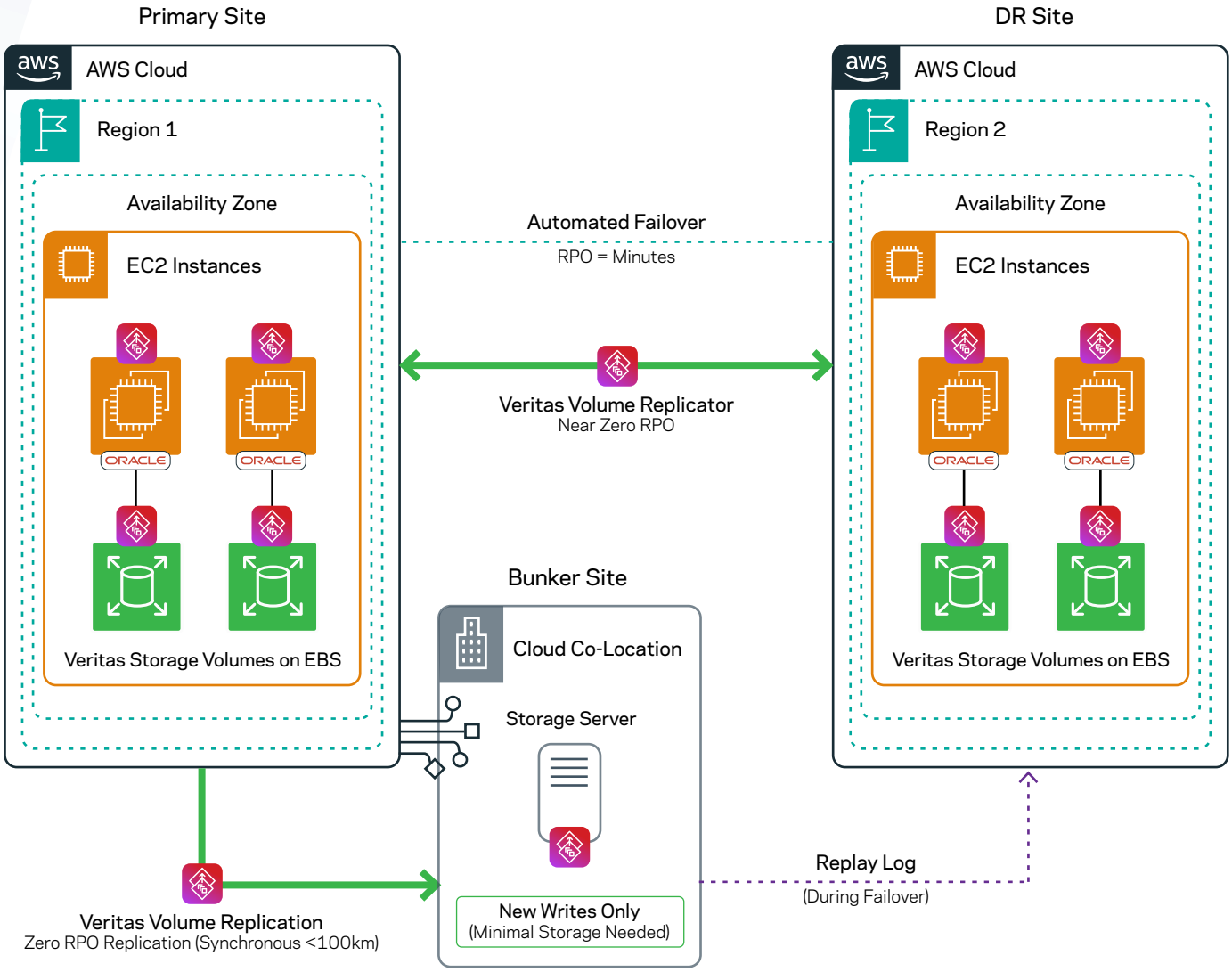



*Figure 4. Veritas Alta Enterprise Resiliency's bunker configuration provides advanced resiliency for Oracle databases*

## Performance and Optimization

Veritas Alta Enterprise Resiliency's SmartIO feature enables intelligent granular caching at the application level, and includes a plug-in designed specifically for Oracle databases. With SmartIO, you can cache reads on fast storage and enable storage Quality of Service (QoS) for mission-critical applications. SmartIO can be customized to maximize application performance by allowing you to pin specific Oracle tablespaces to the cache, giving you the granularity to tune database performance at the tablespace level.

Veritas Alta Enterprise Resiliency can also improve the overall performance of Oracle databases by providing extensions to the Oracle Disk Manager (ODM), a database accelerator technology that enables online transaction processing (OLTP) performance equal to raw disk partitions, but with the manageability benefits of a file system. The Veritas Alta Enterprise Resiliency extensions for ODM were co-developed

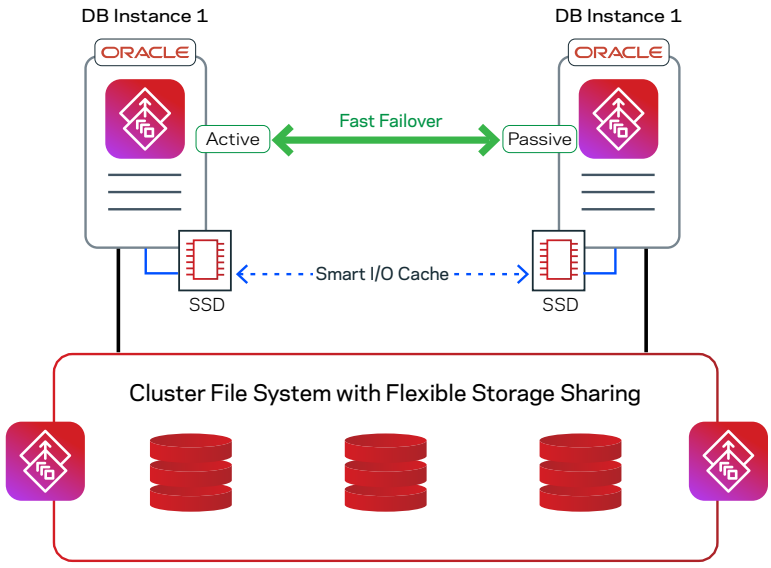



*Figure 5. Veritas Alta Enterprise Resiliency fast failover with SmartIO enabled improves performance for Oracle single instance databases*

with Oracle for the purpose of improving database performance by enhancing file management and disk I/O throughput. With advanced I/O optimization, users can improve database throughput for I/O-intensive workloads. Other key benefits of using ODM include:

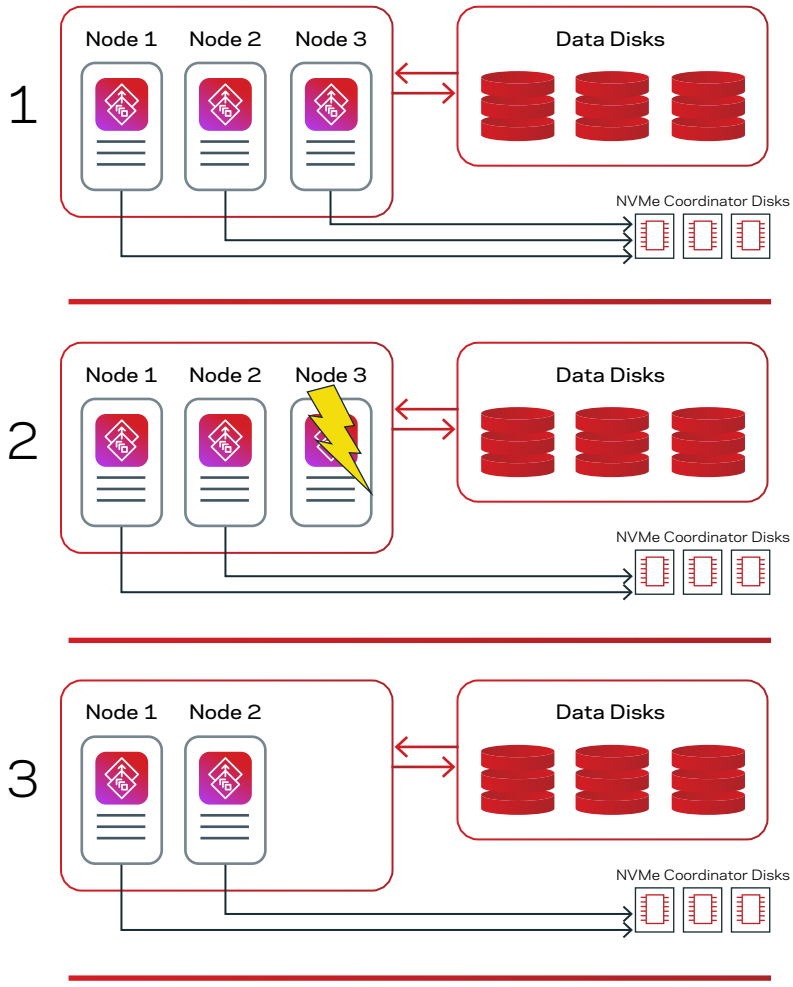
- Reduced system overhead with an improved file system layout
- Kernel-level process that delivers asynchronous I/O for files and raw devices
- Complete transparency for end users

### Ensuring Data Integrity

When multiple systems/nodes have access to data via shared storage, the integrity of the data depends on internode communication, ensuring that each node is aware when other nodes are writing data. When the coordination between the nodes fails, it results in a *split-brain condition*—a situation where two servers try to independently control the storage, potentially resulting in application failure or even corruption of critical data, which can then require days to recover.

Veritas Alta Enterprise Resiliency's integrated I/O fencing solution ensures data integrity by preventing data corruption. Without I/O fencing, it is not possible to determine which node(s) are valid members of the cluster, and subsequent write operations will compromise data integrity. I/O fencing ensures that errant nodes are *fenced* and do not have access to the shared storage, while the eligible node(s) continue to have access to the data, virtually eliminating the risk of data corruption.

Fencing is done using industry-standard SCSI-3 persistent group reservation technology, as well as other non-SCSI-3 fencing technology. In public cloud environments where SCSI-3 persistent group reservation compatible disks are not available, I/O fencing is configured using NVMe devices or coordination point servers. Fencing in the public cloud using NVMe disks is a simple yet highly reliable solution for ensuring data integrity. Veritas Alta Enterprise Resiliency fencing with NVMe disks adds an additional layer of security for your data, as you can block access to the disks to prevent unauthorized access, and you can prevent disks from being attached to other compute instances without proper authority.




1) The cluster is operating nominally.
2) Node 3 loses communication with the rest of the cluster. It Loses its registration on the coordinator disks.
3) Node 3 is ejected from the cluster. Writes from Nodes 3 are no longer permitted.

*Figure 6. Veritas Alta Enterprise Resiliency I/O fencing ensures data integrity*

## Securing Oracle Workloads

Malware and data corruption are common factors that can lead to unplanned downtime and other scenarios that can negatively affect your IT services. Protecting your databases from these threats requires a solution designed for enterprise workloads that natively provides security and encryption functionality for your data, without compromising performance and usability. Veritas Alta Enterprise Resiliency offers filesystem security designed to protect your databases against ransomware attacks and data corruption, as well as volume encryption that ensures your data is protected against unauthorized access.

### Ransomware Resiliency

Veritas Alta Enterprise Resiliency's secure filesystem SecureFS enables files and file system checkpoints to be immutable. The WORM functionality available in Veritas Alta Enterprise Resiliency ensures that files and file system checkpoints can only be read but not modified or deleted for a given retention period. After the retention period has expired, the file can then be modified or deleted. There is also a less restrictive WORM option—called SoftWORM—where the root user is given the ability to reduce retention times on files or checkpoints. By running your Oracle databases on an Veritas Alta Enterprise Resiliency secure file system, you can protect your databases against ransomware attacks and data corruption with an easy to use solution that requires minimal overhead.

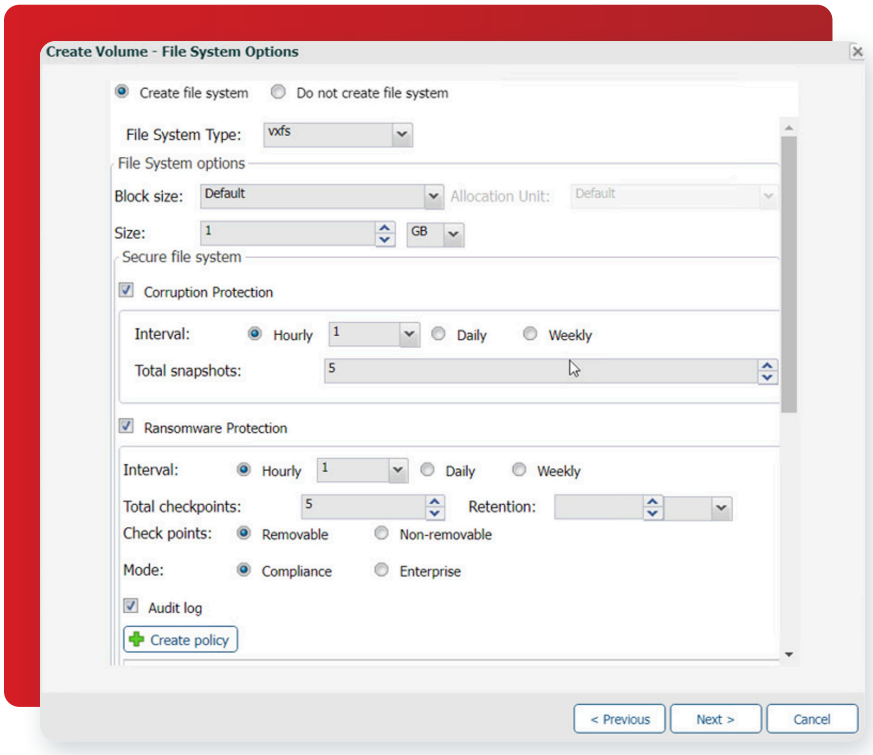



*Figure 7. Veritas Alta Enterprise Resiliency's SecureFS protects your Oracle databases against corruption and ransomware attacks*

Veritas Alta Enterprise Resiliency's secure file and checkpoint option is a space efficient, quick, and easy to use solution to protect your primary data against ransomware attacks. Immutable checkpoints are created automatically and can be rolled back very quickly to reduce downtime in the event of malware infiltration. Some of the key benefits include:

- **Immutable checkpoint:** Designates file system checkpoints as non-modifiable to protect primary data against ransomware attacks, with no impact on recoverability
- **Audit logging:** Ensures there is a proper record of events related to unauthorized modifications within the file system
- **Data resiliency:** Supports file- or volume-level recovery, as well as database-level recovery

The secure file system functionality is customizable, which gives you the flexibility to design templates specifically for Oracle workloads. As an example, you can place the Oracle datafiles and online redo logs on a secure file system with checkpoints created automatically every two hours, and the archive logs can be designated as WORM with a retention interval of 24 hours or longer, depending on operational standards.

Veritas Alta Enterprise Resiliency also gives you the flexibility to integrate custom scripts into the data management process to provide additional functionality and data services for Oracle databases. Veritas Alta Enterprise Resiliency volumes and database checkpoints can be scanned by a third-party anti-malware solution to ensure there is no known ransomware present, and to remove any threats if ransomware is identified.

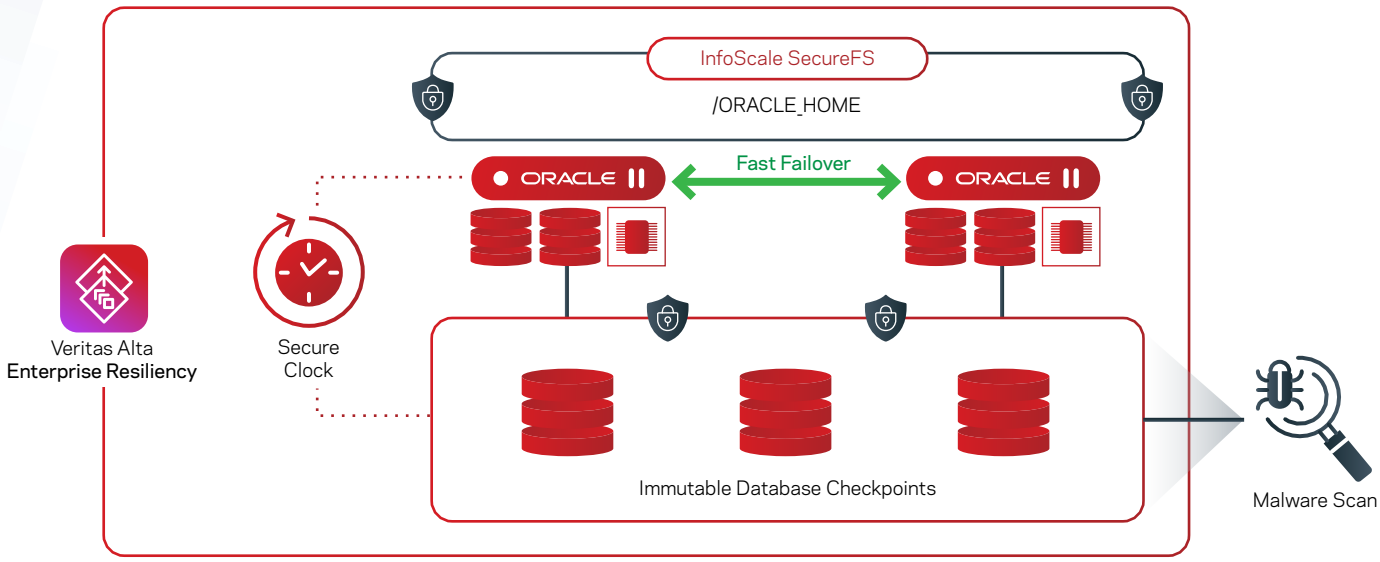



*Figure 8. Veritas Alta Enterprise Resiliency's SecureFS helps protect your databases against ransomware attacks*

### Secure Clock

While secure files and file system checkpoints ensure that your data is secure and unchangeable, it is equally important to manage data retention settings to eliminate attempts at expiring data and subverting immutability. Veritas Alta Enterprise Resiliency's secure clock ensures that there is a method of keeping track of time on your systems that guarantees the filesystem's retention periods cannot be subverted. If a secure clock mechanism were not present, it is possible that a retention period could be expired by simply changing the system clock to some point in the future.

The Veritas Alta Enterprise Resiliency secure clock involves recording the system time to a file at the system level of the filesystem. This mechanism guarantees that ransomware cannot subvert the secure clock by manipulating the system time.

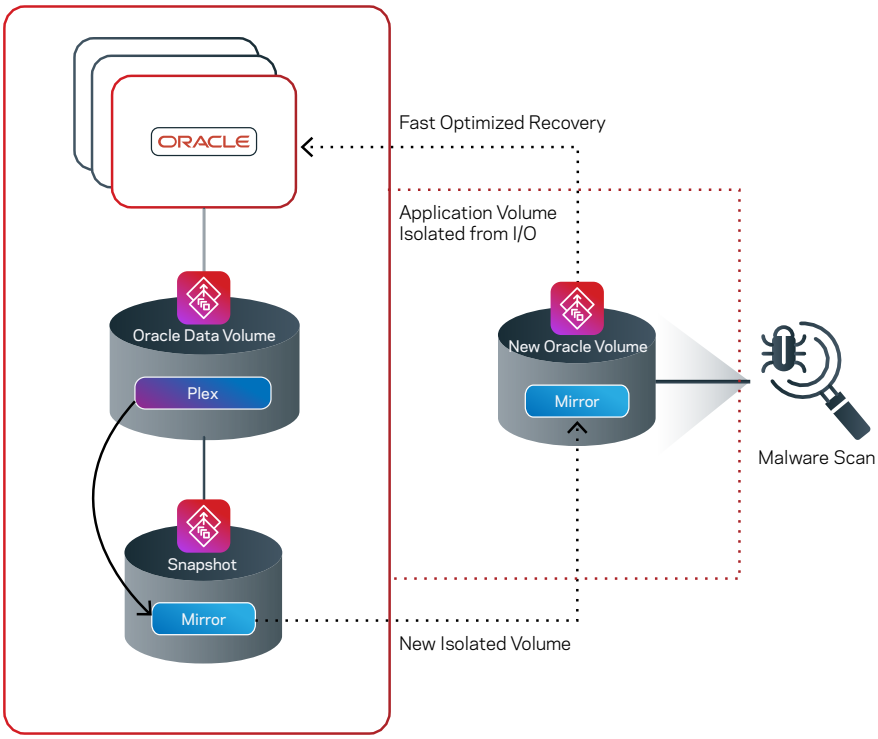



*Figure 9. Data isolation with encrypted volumes*

### Data Isolation

Veritas Alta Enterprise Resiliency can be deployed in a way that provides isolation for production data by mirroring data volumes and isolating them from new I/O—where an anti-malware engine can be used to find and eliminate ransomware.

Veritas Alta Enterprise Resiliency's volume mirroring and optimized snapshots can be accessed independently of the volumes from which they were taken. By creating a volume mirror and detaching the mirror as a new snapshot volume, this effectively isolates a copy of your primary data from new I/O. At this point, you can automate the process of running an anti-malware scanning engine to scan the new snapshot volume, which will detect and eliminate ransomware. Once the snapshot is validated as safe by the anti-malware engine, you can use Veritas Alta Enterprise Resiliency's FastResync option to quickly reassociate the snapshot plex with its original volume in an optimized manner, where only changed data is synchronized. This gives you a fast and reliable way to protect your production databases from ransomware attacks with a very low RPO.

### Data Encryption

All volumes on Linux and Windows systems can be encrypted, which gives you an added layer of security that protects your data against unauthorized access. Veritas Alta Enterprise Resiliency uses AES-256 bit symmetric key encryption and is FIPS 140-2 compliant. Encryption can be enabled automatically when volumes are created to ensure that all I/O going to and from Veritas Alta Enterprise Resiliency volumes is encrypted. If an attacker gains access to your cloud credentials and is able to create snapshots or make unauthorized copies of your databases, Veritas Alta Enterprise Resiliency volume encryption protects you against data exfiltration by ensuring that your data is inaccessible to the attackers.

## Converting from RAC to Single-Instance

Converting your RAC cluster to a single-instance database involves making a copy of the Oracle RAC database and recovering it on another system as a single-instance database. The following files need to be copied on the RAC database using a supported utility, and restored on the single-instance database system:

- **Data files:** Used to store data defined within Oracle tablespaces; each tablespace has one or more datafiles
- **Archive log:** An archived version of the online redo log (which is a circular log of all changes to be made to the database)
- **Control file:** A file that describes the database structure, and identifies all datafiles and log files
- **Parameter file (SPFILE):** Contains database parameters and the location of the control file

The copy operation can be done using Oracle native tools such as RMAN and Data Guard. You can also perform backup and recovery of RAC databases using NetBackup™ and NetBackup appliances, which have features and functionality designed specifically to protect Oracle workloads.

### Procedure Overview using RMAN

Oracle Recovery Manager (RMAN) is an Oracle native utility for performing backup and recovery of Oracle databases. The RMAN executable is automatically installed with the Oracle database software, and the backup process consists of an RMAN client connecting to a target database to perform backup and recovery operations. RMAN activity is recorded in the control file of the target database. The high-level procedure for converting a RAC database to a single-instance database on a Veritas Alta Enterprise Resiliency system using RMAN is as follows:

1. Run a backup of all files noted above
2. Copy the backup files generated in step 1 as well as the pfile to a new system where Veritas Alta Enterprise Resiliency is installed
3. Set the parameter *cluster_database = false* in the pfile on the new system
    a. Remove all parameters related to the 2nd Oracle instance thread
    b. Change the existing control file location to the control file location on the new system where Veritas Alta Enterprise Resiliency is installed and configured
4. Follow the RMAN procedure to restore the backup files to the new system
5. Recover and open the database on the new system where Veritas Alta Enterprise Resiliency is configured

### Procedure Overview using Data Guard

Oracle Data Guard is a set of services designed to manage standby databases (which are transactionally consistent copies of the production database) for the purpose of providing disaster recovery for production/primary Oracle databases. Data Guard maintains the standby database(s) by transmitting and applying redo data from the primary database, and it can switch any standby database to production to minimize downtime in the event of a primary database outage. A general outline for how to convert a RAC database to a single-instance database using Data Guard is as follows:

1. Configure standby redo logs on the RAC database; enable archive log mode on the RAC database and set the database initialization parameters.
2. Configure listener entries on the RAC database. Add entries for the RAC and single-instance standby database on all RAC cluster nodes. Also configure TNS entries on all RAC cluster nodes.
3. On the single-instance standby database, create the required directories, configure the listener and TNS entries.
4. Start the single-instance standby database in NOMOUNT mode and verify TNS connectivity for the RAC and single-instance standby databases.
5. Using RMAN, duplicate the RAC database. Verify the standby redo logs on the single-instance standby database.
6. On the single-instance standby database, create the spfile, shutdown the database and start the database in MOUNT mode. Then, start the managed recovery process (MRP).
7. Run a switchover on the RAC database to the new single-instance database.

### Procedure Overview using NetBackup

NetBackup for Oracle delivers enterprise data protection specifically designed to protect Oracle databases. NetBackup's Oracle Intelligent Policies enable RMAN to use NetBackup, which uses the RMAN SBT_LIBRARY parameter to link RMAN with NetBackup's media management functionality. When a NetBackup Oracle Intelligent Policy is executed, NetBackup automatically generates all the files and scripts needed to interface with RMAN. NetBackup-powered appliances add additional functionality to the Oracle backup process by integrating data protection and storage management into a purpose-built appliance optimized for efficiency and security—with a dedicated storage area designed to accommodate Oracle backups using either a *dump and sweep* or incremental merge backup strategy. The high-level procedure to convert a RAC database to a single-instance database on a Veritas Alta Enterprise Resiliency system using NetBackup is as follows:

1. Connect to the RAC database (which is automatically discovered by NetBackup) by providing database login credentials in the NetBackup user interface
2. Create and configure a NetBackup Oracle Intelligent Policy (using the NetBackup policy type "Oracle")
    a. Select your storage target for the policy (such as NetBackup MSDP space-optimized storage)
    b. Configure the backup schedule and type (such as full or incremental)
    c. Define the backup selections for the policy

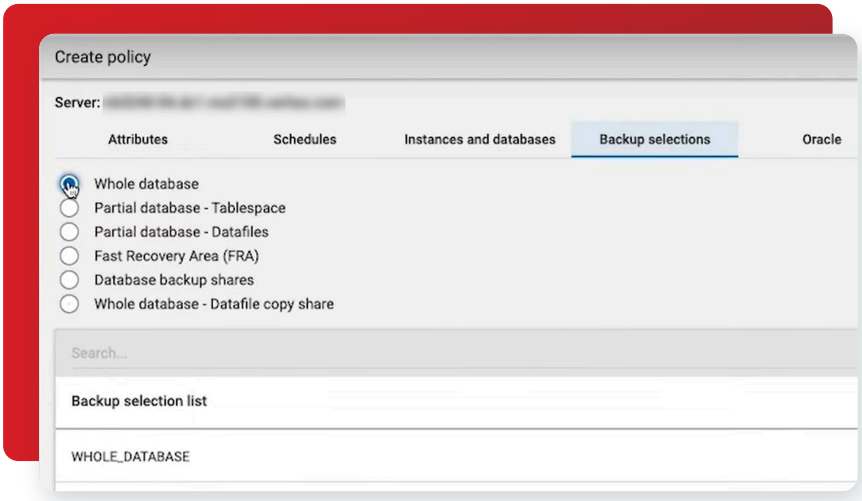



*Figure 10. NetBackup Oracle policy configuration options*

3. Execute the NetBackup Oracle Intelligent Policy to generate a transactionally consistent backup of the Oracle RAC database
4. Perform a database recovery to an alternate system where Veritas Alta Enterprise Resiliency is installed and configured, and Oracle is installed and configured as a single-instance database:
    a. Ensure that you can browse the Oracle backup created in Step 3 using the bplist command on the NetBackup primary server
    b. After setting up the target Oracle single-instance database for alternate NetBackup restores, connect to RMAN to run the recovery commands
        i. Restore the control file on the target system in NOMOUNT mode
        ii. Update the following parameters based on the configuration of the single-instance database on the target system: ORACLE_HOME, ORACLE_SID, ORACLE_USER, TARGET_CONNECT_STR
        iii. Restore the database in MOUNT mode

## Conclusion

Ensuring that your IT services deliver a premier user experience is always top of mind, and the databases that your IT services rely on need a proven enterprise platform to ensure smooth, secure, and resilient operations. Veritas Alta Enterprise Resiliency delivers that secure and resilient foundation for Oracle databases by providing a more flexible solution than Oracle RAC. Veritas Alta Enterprise Resiliency enables you to operate in the public cloud in a highly available single-instance configuration, with similar performance and availability—and reduced costs and complexity—as compared to Oracle RAC. Veritas Alta Enterprise Resiliency provides several key benefits for Oracle databases:

- ✓ **Cloud:** Run Oracle single-instance databases in any public cloud with availability similar to Oracle RAC
- ✓ **Resiliency:** Ensure your databases are highly resilient, with a zero data loss and near-zero recovery time solution that is supported in on-premises, cloud, hybrid-cloud, and multi-cloud environments
- ✓ **Security:** Integrated data immutability and encryption protect your databases against ransomware attacks, data corruption, and unauthorized access

Veritas Alta Enterprise Resiliency is a comprehensive, multi-faceted solution with a proven track record of improving availability and operations for Oracle databases. Veritas Alta Enterprise Resiliency helps you avoid additional costs when compared to native Oracle functionality, with full support to run in any public cloud environment—which is not supported with Oracle RAC. Veritas Alta Enterprise Resiliency provides the foundation you need to run your business-critical Oracle databases in the cloud with maximum flexibility and confidence.

**About Veritas**

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

Copyright © 2023 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo, Veritas Alta, the Veritas Alta logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

V1969 08/23