

Upgrade to the Latest OpenStack Version

LEVERAGING TRILIO DATA PROTECTION

New OpenStack versions are released every six months. With that kind of frequency, it grows urgent for IT leaders to identify safe, reliable, and repeatable upgrade paths for OpenStack cloud environments.

Organizations have traditionally resisted making system changes and occasionally bypassed updates in order to avoid interruptions in day-to-day operations. However, older software versions become more susceptible to security and stability risks over time, and businesses miss opportunities for new features that improve performance, scale, and manageability.

With Trilio, customers can dramatically reduce both the risk and timeline associated with this often-costly upgrade process. Trilio data protection makes it easy to backup the existing cloud environment — including valuable workload metadata — and restore it to the upgraded cloud environment, regardless of your preferred distribution.

Trilio **enables a safe upgrade path** and ongoing data protection for organizations managing OpenStack infrastructure.

OPENSTACK RELEASE LIFECYCLE

Since OpenStack operates under a twice-yearly release model, upgrades become a frequent chore. The optimizations of the newer cloud form factors make it challenging to consume the new technology as it becomes available, and older versions are end-of-lived after two years. See the OpenStack release diagram below or visit openstack.org for more information.

SERIES	STATUS	RELEASE DATE	END-OF-LIFE DATE
Train	Development	2019-10-16 (est)	
Stein	Maintained	2019-04-10	
Rocky	Maintained	2018-08-30	
Queens	Maintained	2018-02-28	
Pike	Maintained	2017-08-30	
Ocata	Extended Maintenance	2017-02-22	
Newton	End of Life	2016-10-06	2017-10-25
Mitaka	End of Life	2016-04-07	2017-04-10
Liberty	End of Life	2015-10-15	2016-11-17
Kilo	End of Life	2015-04-30	2016-05-02
Juno	End of Life	2014-10-16	2015-12-07
Icehouse	End of Life	2014-04-17	2015-07-02

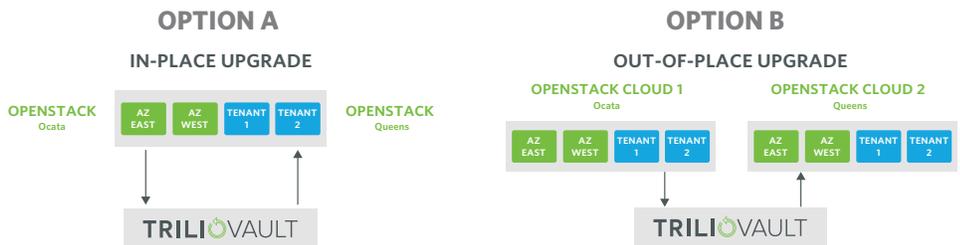
OPTIMAL SOLUTION

TrilioVault offers a highly efficient, reliable, and scalable solution to satisfy the most demanding enterprise needs.

To reduce the risk of data loss during an upgrade, Trilio captures and protects tenant workloads throughout the upgrade procedure. Trilio captures both the application and VM data, as well as the tenant/project metadata itself (network definitions, storage layout, security groups, etc.). Therefore, in the event that the upgrade process encounters failures, operators will be able to rapidly and efficiently recover their environment from a given state at any time.

TrilioVault provides a consistent, safe, and secure upgrade process, regardless of whether an operator is performing an "in-place" or "out-of-place" upgrade.

Trilio enables both **in-place** and **out-of-place upgrades**, enabling you to safely leverage new or existing hardware as needed.



BENEFITS OF UPGRADING OPENSTACK WITH TRILIO

- **Latest Cloud Version Support:** Upgrade to the latest long-term release
- **Simplified Project Management:** Create a predictable timeline for your project completion
- **Cloud and Tenant Data Protection:** Protect your overcloud during upgrade
- **Professional Service Backed:** Confer with Trilio Professional Services experts

THE VALUE OF DATA PROTECTION

Whether it's application or infrastructure, upgrades are certainly not without a degree of risk. Best practices dictate that any architect, engineer, or other member in charge of this environment should protect themselves in the event of:

- Hardware and software failures (manual or programmatically)
- Data loss
- End-of-life (EOL) hardware and software components
- Demanding business compliance requirements and regulations

About Trilio

Trilio is a leader in data protection for OpenStack and KVM environments, and the only provider of OpenStack-native backup and recovery solutions. Since 2013, Trilio has been on a mission to give tenants more control over their ever-changing, growing, complex, and scalable cloud-based architectures. Today, Trilio is trusted by businesses all around the world to protect their clouds in a way that's easily recoverable, and requires little-to-no central IT administration.

