



Author: Marc Staimer

T E C H N I C A L P A P E R

# **Warning:** Azure Stack & AWS Outposts Aren't Suitable for On-Prem Critical Cloud Workloads

In-Depth Analysis of Why Azure Stack & AWS Outposts Fail to Address Enterprise & Government Requirements

**Warning: Azure Stack & AWS Outposts Aren't Suitable for On-Prem Critical Cloud Workloads**

---

**Introduction**

The value of public clouds is no longer a major question for most IT organizations. Public clouds and their services have become increasingly ubiquitous, production-proven, and the first choice for new application development. The big exceptions are Enterprises and other large IT organizations such as governments that have data sovereignty, performance requirements or tightly linked applications on-prem that prevent them from moving to the public cloud.

Here's why so many find public clouds from AWS, Azure, Google, and Oracle so appealing:

**Public Cloud's Real Value**

- **Converts capital expenditures (CapEx) into operating expenditures (OpEx).** IT organizations only pay for what they use instead of taking on the risk of building out infrastructure for peak usage that they might or might not use. The public cloud thus reduces or in some cases, such as Oracle Cloud Infrastructure, eliminates idle time cost. Cloud cost is typically fine grain measuring the resources used in hours, minutes, and, in some cases, seconds. It is the truest application of the old adage "**time-is-money**". This results in more efficient utilization and potentially lower costs when usage is dynamically variable. The pay-per-use model clearly demonstrates the value of speed. Completing tasks faster equates to lower cost.
- **Provides significantly better elasticity.** Unlike on-prem infrastructure (occasionally referred to as a private cloud), it's highly unlikely an application or project will consume all of a public cloud's resources. Those resources are often available automatically or at a moment's notice. More importantly, the resources can be scaled down as demand drops, thereby reducing cost. Although resources can be scaled down in conventional VMware & generic hardware vendor type private cloud, it does not reduce costs because the infrastructure itself does not change and the time to complete jobs goes up.
- **Has the resources always available for devops/devsecops without notice, at low cost, and as a result, accelerate time-to-project-completion.** This is not the case for on-prem infrastructure. It can often be difficult to exasperating and time-consuming to scrounge together the resources for unexpected projects even when fully virtualized. The drive for infrastructure efficiencies on-prem means unplanned resource requirements go unmet or encounter significant delays.
- **Empowers IT organization's agility** to spin up and down applications, try new services, innovate marketing programs, and experiment without having to invest in resources up front and long-term. On-prem infrastructure is the opposite.
- **Enables IT organizations to get out of the business of managing data center infrastructure.** This reduces the stress and strain on IT resources while empowering a redirect to more strategic utilization such as cost reduction projects, new applications, or services that drive innovation and revenue growth.
- **Are generally more secure than private clouds.** Public clouds are hardened through years of encountering and preventing hacking attempts. They commonly recruit and attract top-notch security professionals for this task. They're more likely to be timely on security vulnerability patching. In addition, they do not suffer from perimeter complacency, i.e. if it's behind the firewall, it's secure.
- This proven value has made public clouds both highly attractive and widely used.



Public clouds have been and continue to be an incredible boon to many IT organizations. However, for some Enterprises and other large IT organizations such as governments moving to the cloud is not an option for the reasons mentioned above. In fact, while organizations leverage the public cloud to build new cloud-native applications, approximately 20% of Enterprise apps are in the cloud according to [McKinsey & Company](#).

**Public Cloud Issues For Enterprises and Governments**

The majority of public clouds cannot deliver mission/business-critical infrastructure, databases, and services for enterprise-class applications. Mission/business-critical applications are the lifeblood of

Enterprises and government agencies. Mission/business-critical applications demand and are highly dependent on mission/business-critical databases and hardware infrastructure. An application can't really be mission/business-critical if the underlying database software and hardware infrastructure are not. By definition, mission/business-critical systems must deliver high availability (HA) with no single point of failure (SPOF) to ensure 99.95% SLAs or better uptime including planned and unplanned outages. In addition, it must deliver performance and capacity scalability to meet or exceed SLA requirements 99.95% of the time.

### Mission/Business-Critical

#### Mission/Business Critical Defined

A mission/business critical database, application, or system means that it's necessary for the success of the organization, an operation, or business. The loss of a mission/business critical application for any reason is rapid, substantial, and often catastrophic. It is not hard to imagine the outage consequences and costs for a banking system, electrical power grid management system, nuclear power plant control system, air traffic control system, pharmaceutical quality control system, emergency responder system, online transaction processing, or high frequency trading system. These are just some examples of mission/business critical systems where their loss has catastrophic consequences. There are many more. When mission/business critical systems fail, are interrupted, or suffer an outage, the results are generally disastrous. The organization is likely to see a loss of customer satisfaction, customers, revenue, profits, and productivity. In addition, their hard earned reputation can suffer, requiring years to rebuild.

The difference between a mission-critical and business-critical system is nuanced. It correlates to the adverse impact of an outage. Loss of a mission-critical system results in the failure of a specific outcome. Using the previous examples that could mean the loss of electrical power, a person's life, a transaction, etc. Loss of a business-critical system results in an economic loss. The two are related and tend to be two sides of the same coin, but not necessarily so.

- Customers lose or have limited control over their physical and cyber data security. Security revolves around what the public cloud service provider delivers. If more security is required or warranted than what is offered, it may be excessively costly or not possible. A single IT organization's needs can be too costly for the public cloud service provider to deliver.
- Many public clouds cannot or do not offer the database performance, reliability, availability, and scalability demanded by mission/business-critical applications. Latencies are too high; IOPS are too low; throughput is too narrow; reliability, availability, and scalability are too unsatisfactory. In other words, applications in the cloud do not meet the mission/business-critical requirements of Enterprises.
- The public cloud service provider cannot or will not provide data sovereignty because of limited data center locations. When they do not have a cloud data center in a specific sovereign location, it compromises data sovereignty. A public cloud service provider may be willing to build a data center for a national government but is unlikely to build one for large multi-national Enterprises, local, or state governments. This is a non-starter in several countries and regions around the world.
- As regulators and the lawyers have made crystal clear, compliance is not legally outsourceable. By not controlling the data center infrastructure, IT organizations may not be able to meet their compliance requirements. Failure to comply is not the legal responsibility of the public cloud services provider. In the current worldwide environment of personally, identifiable information (PII) privacy laws and regulations, compliance is the enterprise's legal responsibility and non-compliance is quite expensive and financially irresponsible.

These issues have put the public cloud benefits and value out-of-reach for many Enterprises and governmental organizations. Delivering agile, flexible, performant, and pay-per-use cloud services with the mission/business criticality demanded as an on-prem cloud offering has simply been weakly addressed by most cloud services providers.



Attempts by AWS, Azure, and Google to provide this solution are half baked, at best. Azure Stack Hub, in particular, is a partial solution that fails miserably on multiple levels. This report examines why on-prem cloud offerings from AWS, Azure, and Google Cloud Platform (GCP), fail to meet Enterprise mission/business-critical requirements.

It then examines how Oracle's latest "Cloud@Customer" services such as Autonomous Database on Exadata Cloud@Customer and Dedicated Region Cloud@Customer solve these fundamental problems.

*Table of Contents*

**Introduction ..... 2**

- Public Cloud’s Real Value ..... 2
- Public Cloud Issues For Enterprises and Governments ..... 2
- Mission/Business-Critical ..... 3

**How AWS Outposts, Azure Stack, and GCP Anthos On-Prem Cloud Offerings Fail ..... 5**

- AWS Outposts ..... 5
  - Cloud IaaS, PaaS, SaaS, DBaaS, 3<sup>rd</sup> Party Apps, Cloud Services, Data Behind Firewall ..... 5*
  - Simplicity ..... 6*
  - Mission/Business-Critical ..... 7*
  - Data Sovereignty/Data Residency ..... 8*
  - Reduced TCO ..... 8*
  - AWS Outposts Summary ..... 9*
- Microsoft Azure Stack (a.k.a. Azure Stack Hub, Azure Stack Edge, and to a lesser degree Azure Stack HCI) .....10
  - Cloud IaaS, PaaS, SaaS, DBaaS, 3<sup>rd</sup> Party Apps, Cloud Services, Data Behind Firewall ..... 10*
  - Simplicity ..... 10*
  - Mission/Business Critical ..... 11*
  - Data Sovereignty/Data Residency ..... 13*
  - Reduced TCO ..... 13*
  - Azure Stack Summary ..... 13*
- Google Cloud Platform (GCP) Anthos .....14
  - GCP Anthos Summary ..... 14*

**New Oracle Cloud@Customer Services ..... 15**

- Oracle Autonomous Database on Exadata Cloud@Customer .....16
  - Oracle Database ..... 16*
  - Oracle Exadata X8M ..... 17*
  - Cloud IaaS, PaaS, SaaS, DBaaS, 3<sup>rd</sup> Party Apps, Cloud Services, Data Behind Firewall ..... 17*
  - Simplicity ..... 18*
  - Mission/Business-Critical ..... 18*
  - Data Sovereignty/Data Residency ..... 18*
  - Reduced TCO ..... 18*
  - The Oracle Autonomous Database on Exadata Cloud@Customer Summary ..... 19*
- Oracle Dedicated Region Cloud@Customer .....19
  - Cloud IaaS, PaaS, SaaS, database cloud service, 3<sup>rd</sup> Party Apps, Cloud Services, Data Behind Firewall ..... 20*
  - Simplicity ..... 21*
  - Mission/Business-Critical ..... 21*
  - Data Sovereignty/Data Residency ..... 21*
  - Reduced TCO ..... 21*
  - Oracle Dedicated Region Cloud@Customer Summary ..... 22*

**Conclusion ..... 22**

**For More Information on the Oracle Cloud@Customer Services ..... 23**

## How AWS Outposts, Azure Stack, and GCP Anthos On-Prem Cloud Offerings Fail

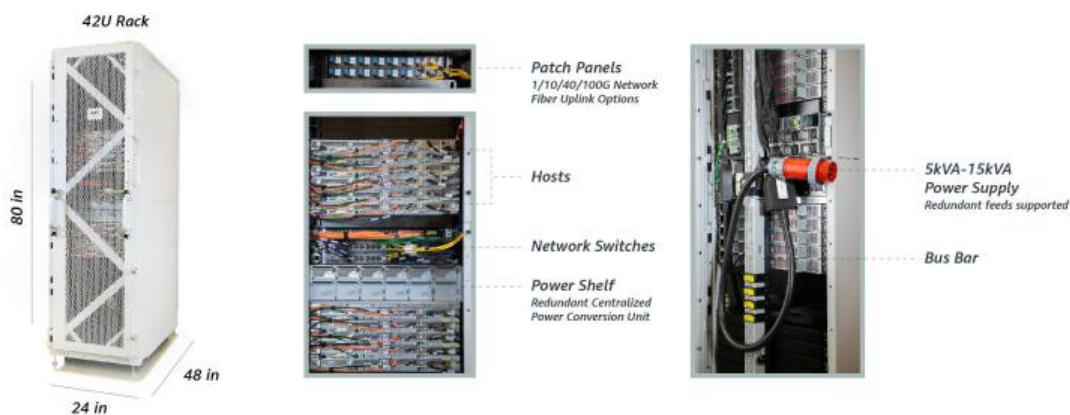
Enterprise and government cloud requirements are many and frequently nuanced. However, most can be boiled down to the following:

- Bring the cloud and cloud services on-prem behind their firewall.
- Simplicity – it's got to be simple, easy, intuitive and automated.
- Mission/business-critical.
- Data sovereignty, data residency, legal, and regulatory compliance.
- Reduced total cost of ownership (TCO) over traditional on-prem systems.

AWS, Azure, and GCP have very different approaches in their less than successful attempts to satisfy these requirements with their on-prem cloud solutions. They just flop in different ways. A deeper dive shows how.

### AWS Outposts

AWS Outposts is the AWS system that brings AWS cloud hardware and services to customers' data centers. AWS delivers and installs Outposts fully assembled in a 42 RU standard rack. Outposts has two variations. The first variation enables users to use the native AWS APIs, tools, and some services.



Outposts' primary purpose is to provide Infrastructure-as-a-Service (IaaS) tools to build and run AWS native applications on-prem. It provides a consistent AWS on-prem and cloud experience. A second variation of Outposts is an extension of the existing AWS VMware Cloud service that allows users to run VMware private cloud software on Outposts. The VMware variant becomes available in the second half of 2020.

Outposts is architected for workloads that need low latency access, local data processing, or local data storage. The infrastructure for Outposts is delivered, installed, monitored, patched, and updated by AWS. AWS accomplishes this by connecting Outposts to AWS regions for management and control plane services. AWS Outposts became available at the end of 2019, and, as of August 2020, is still not completely rolled out. AWS has plans to add services over time. The problem is that despite current and future promised cloud services, it fails to address most Enterprise and government cloud concerns, issues and requirements.

### Cloud IaaS, PaaS, SaaS, DBaaS, 3<sup>rd</sup> Party Apps, Cloud Services, Data Behind Firewall

AWS Outposts can be completely separated from the AWS public cloud except for backups of snapshots. Backups are sent to S3 object storage in a local AWS region. Although backups are encrypted via customer managed AWS KMS (key management system) keys, the backup data is not on-prem, thereby compromising data sovereignty.

Like many on-prem cloud offerings, AWS Outposts provides a limited subset of AWS public cloud features and services. They include:

- **EC2** – Compute instances.
  - **General purpose** (M5/M5d) instances that balance compute, memory, and network resources for general-purpose workloads.
  - **Compute optimized** (C5/C5d) instances for high performance compute-intensive workloads.

- **Memory optimized** (R5/R5d) instances for fast performance workloads that process large data sets in memory.
- **Graphics optimized** (G4dn) instances help accelerate machine learning inference and graphics-intensive workloads.
- **I/O optimized** (I3en) instances use Non-Volatile Memory Express (NVMe) SSD storage for low latency, high random I/O performance, and high sequential disk throughput.
- **ECS** – Container service.
- **EKS** – Kubernetes service.
- **EMR** – MapReduce service.
- **RDS** – Relational database service, limited to open source databases at this time.
  - **MySQL.**
  - **PostgreSQL.**
- **EBS** – Elastic block storage.
- **S3** – Object storage 2<sup>nd</sup> half 2020.
- **VMware Outposts variant.**

That’s just seven of AWS’ vast swath of cloud services made available on Outposts including S3 coming later in 2020. Users cannot run most AWS public cloud databases including RDS Aurora, Oracle, Microsoft SQL Server, and MariaDB. They also cannot use AWS public cloud database services such as Amazon Redshift, Amazon DynamoDB, Amazon ElastiCache for Redis, Amazon ElastiCache for Memcached, Amazon DocumentDB, Amazon Keyspaces, Amazon Neptune, Amazon Timestream, and Amazon Quantum Ledger DB. They can only use RDS MySQL and PostgreSQL...period. AWS is promising MariaDB and Microsoft SQL Server down the road, but no timeframes yet.

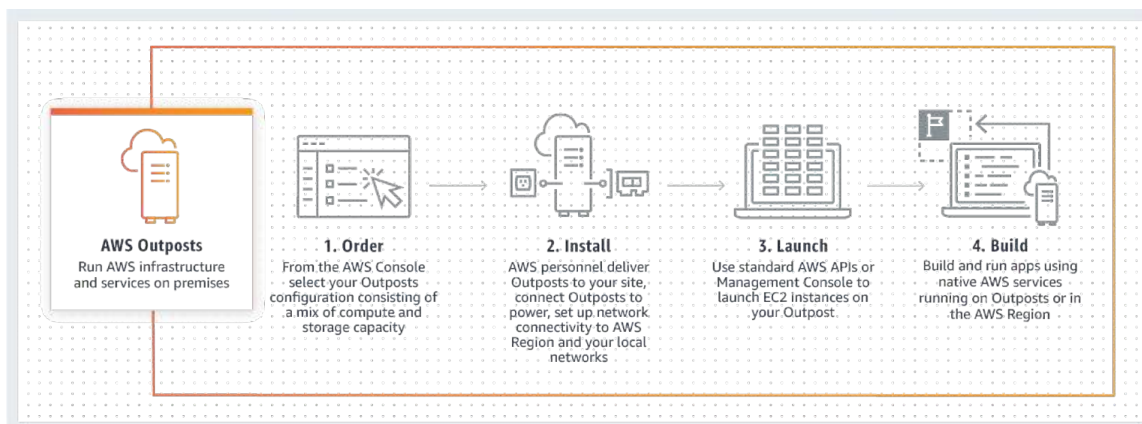
The primary focus of AWS Outposts is for development environments that enable IT organizations to develop applications that run in both the AWS public cloud and on Outposts without change. Amazon positions AWS Outposts as Enterprise class in keeping data resident to meet data sovereignty requirements. However, backup snapshots are kept in S3 in the AWS public cloud, **not** on-prem. The control and management plane is completely in the AWS public cloud, not on-prem. Therefore, for customers looking to meet data sovereignty requirements, AWS is not the answer. This is where Outposts fails to meet its first Enterprise and government requirement.

Another area AWS Outposts fails to deliver (as of the 3<sup>rd</sup> quarter of 2020) are SaaS applications from either AWS—doesn’t have any—or third-party independent software vendors (ISVs). There are none. So, it follows that there are also no mission/business-critical applications available on Outposts at this time. None. No ERP, CRM, eCommerce, nada. That means Outpost users must develop and write their own or choose another vendor.

Conclusion: AWS Outposts has no SaaS of its own and no third-party apps, once again failing another Enterprise and government requirement.

### Simplicity

AWS delivers and installs Outposts fully assembled in a 42 RU standard rack. The process is similar to most self-serve AWS processes. It’s a straightforward process per the AWS website; albeit, it requires the customer to figure out what they need based on documentation, but with little direct help from AWS.



Outposts comes with most of the public AWS cloud APIs and development tools. However, the RDS database as a service (DBaaS) is anything but simple. AWS is responsible for basic database tasks including maintaining, patching, and upgrading the database like most DBaaS. However, it leaves the vast majority of database administration to the customer. That includes indexing, re-indexing, tuning, performance optimizing, troubleshooting, root cause analysis, scaling, which necessitates extensive sharding, and restores from outages, which are labor-intensive and painstakingly slow. And, there are no built-in RDS developer tools at this time making development far more labor-intensive than it needs to be. The hardware is generic with no optimization for RDS databases or any other.

Conclusion: AWS Outposts is overly complex, failing yet another Enterprise and government requirement.

#### Mission/Business-Critical

Amazon says that AWS Outposts is designed for the Enterprise and government organizations, and yet it does not meet the criteria for mission/business-critical. Outposts has HA with centralized redundant power conversion units, active components including top of rack switches and hot spare hosts. However, it has no built-in business continuity or instant recoveries from power outages, rack failures, data center disasters, or site failures.

There are optional daily automatic backups and RDS replicas that can be provided by DBAs. Those data protection processes do NOT provide business continuity in the event of an outage. Outages other than a redundant component failure will result in downtime regardless of (HA) configuration. In addition, the backups (snapshots) are stored in an S3 AWS public cloud region. The backup data is in the cloud, not on-prem. That increases downtime and means the backup data is not behind the IT organization's firewall. RDS restores will take more time since they require human intervention to assure proper restoration from the correct point-in-time and that it is functioning correctly. There is additionally no built-in malware protection. Restorations from a system or complete rack failure is from another Outpost or AWS region in the same account. Disaster recovery (DS) is from an AWS public cloud region. Of note is that RDS on AWS Outposts can only replicate to one availability zone (AZ).

For RDS, the most demanding application on AWS Outposts, CPUs scale up to a maximum of 48 and 96 vCPUs — not very scalable. CPU scaling is manual, not elastic or serverless. It's disruptive and requires downtime. Downtime is not tolerated in Enterprises and government accounts. It must be scheduled for a weekend or late at night, adding cost. That means Outposts cannot react on-demand or automatically to unexpected spikes in RDS database vCPU requirements.

AWS Outposts performance is not easy to discern from Amazon documentation. It takes a bit of digging. One performance metric Amazon has mentioned in passing and on their website is RDS database I/O latency performance at single digit milliseconds (ms). That depends on the use of I/O optimized NVMe SSD EC2 instances. Max EBS 16 KiB IOPS is 80,000 (roughly 160,000 8 KiB IOPS). Max EBS throughput is 2.375 Gbps. Those performance specs are four to five generations behind current Enterprise and government database performance requirements. To put that in perspective, if optimistically, that single digit milliseconds of latency is more than 50 times slower than the Oracle Databases running on Exadata Cloud@Customer and Oracle Dedicated Region Cloud@Customer. Assuming Outposts' maximum EBS configured throughput and IOPS per RDS, its throughput ranges from approximately 9.5% of a minimum configuration for Oracle Exadata Cloud@Customer or Dedicated Region Cloud@Customer running either the Oracle Database or Oracle Autonomous Database, to less than 1% in a max configuration. IOPS also trail badly delivering a high of 28% to a low of 1.3% compared to Oracle on-prem cloud offerings. We will cover this in more detail later in this document. Put simply, Amazon's definition of mission/business-critical database performance is aimed at much smaller databases and IT organizations than Oracle. Keep in mind that cloud operations are charged by time. In the case of AWS RDS, it's coarse grain by the hour. Time is money. The faster Exadata Cloud@Customer ends up costing much less than the slower AWS Outposts.

AWS Outposts support is completely from Amazon. That's desirable for Enterprise and government IT organizations, providing one-throat-to-choke support. However, like most AWS services, getting a person on the phone is difficult. Unless IT organizations are willing to pay large sums of money, support is mostly handled through chat windows or emails. That is not what most Enterprises and government IT organizations expect and require. AWS has gotten measurably better, but still lags when it comes to support. Few of these IT organizations have much tolerance for providing their cheeks upon which Amazon learns to shave.

One soul crushing mission/business-critical problem for AWS Outposts is operational disruption. There will be planned downtime especially when it comes to the RDS MySQL and PostgreSQL databases. Neither MySQL nor PostgreSQL have real-time failover clusters. That means patches and updates are disruptive, requiring scheduled downtime. Adding CPUs or vCPUs to a database is also disruptive, causing more planned downtime. Their business continuity is also disruptive. Recoveries and restores from outages using backups and replicas take



time. And depending on the outage and where the Outposts and databases are recovered from, a lot of time. Both planned and unplanned downtime is a huge issue for Enterprises and governments. Some applications cannot go down. This is why these IT organizations demand contractual SLAs for availability, performance, and manageability (API error rates). Amazon provides no SLAs for AWS Outposts. They only provide availability SLAs for their AWS public cloud based only on unplanned downtime, not planned downtime and there are many caveats.

Conclusion: AWS Outposts just does not meet the definition of mission/business-critical cloud services.

#### Data Sovereignty/Data Residency

AWS Outposts for the most part can meet data sovereignty and data residency requirements—if there are no snapshots, replicas, clones, or backups to S3 in the AWS public cloud. That will only be possible if and when AWS provides S3 on Outposts later in 2020. Otherwise, users will not be able to back up their applications or data without third-party data protection systems if they want to keep all their data in their data centers.

Conclusion: AWS Outposts struggles to meet data sovereignty and data residency requirements.

#### Reduced TCO

Amazon asserts that AWS Outposts has a lower TCO than on-prem systems. Based on their performance numbers, that is unlikely. Cloud pricing is tied to time. Time is tied to performance and AWS performance is mediocre at best. When taking all costs into consideration, and not just pricing, the TCO for AWS Outposts appears to be higher, not lower than Oracle Cloud@Customer services.

AWS Outposts pricing (not costs) is based on three-year contractual commitments to cover the costs of implementing and managing the hardware and software infrastructure. Amazon offers three different pricing models tied to the specific hardware configuration:

- No upfront payment. Just monthly payments for renting the infrastructure for 3 years.
- Partial upfront payment plus monthly payments for 3 years.
- All upfront payment without monthly infrastructure payments for 3 years.
- There are additional charges as well:
  - Elastic Block Store tier charge per GB per month.
  - Operating systems charges per month.
  - Data transfer charges.
  - Egress charges from S3 storage per month.
  - RDS vCPU per **hour** charges – billed monthly.

There are several other costs that must be taken into consideration including:

- Scheduled downtime for planned disruptions – increased personnel costs.
  - Patching and updating.
  - Scaling up or down CPUs for applications or RDS.
- Trained personnel costs.



- Must have administrators and developers knowledgeable and trained in AWS tools, APIs, configurations, idiosyncrasies, etc.
- Third-party data protection systems to keep snapshot or backup data on-prem to meet compliance, data residency, and data sovereignty requirements. Including costs for:
  - Data protection software subscription costs.
  - Hardware to run the data protection software.
  - Storage for the backed up or snapshot data.
  - Maintenance and support on the hardware.
  - Tech refresh for the hardware.
  - Trained administrators.
- Performance costs.
  - Amazon charges per vCPU hour.
  - The relatively slow performance of Outposts means longer runtimes for RDS database jobs.
  - More time equals more cost. Time is money in clouds.

Conclusion: When all costs are considered, it is far more likely AWS Outposts will have higher TCO than on-prem systems.

[AWS Outposts Summary](#)

AWS Outposts is positioned as an Enterprise cloud on-prem system. Yet it fails to meet most Enterprise and government cloud on-prem requirements. AWS Outposts in reality is a first-generation effort by Amazon that is best suited for AWS application development on-prem. It's Amazon's attempt at entering the on-prem world without making a full commitment. This is analogous to getting engaged for 9 years and never getting married. Amazon is learning what works and what doesn't for Enterprises and government IT organizations. Customers will have to decide if they want to pay the price to educate AWS.

Enterprises & Government Requirements	AWS
	Outposts
Behind Firewall	Limited
IaaS	✓
PaaS	∅
Native SaaS Cloud Apps	∅
3rd Party SaaS Cloud Apps	∅
DBaaS	✓
Data	Mixed
Cloud Services	7
Simplicity	∅
Mission/Business Critical	∅
Business Continuity	∅
Data protection & DR	✓
Top notch performance	∅
Scalability	∅
SLAs	∅
Availability	∅
Performance	∅
Manageability (API errors)	∅
Data Sovereignty/Data Residency	Partial
Reduced TCO	∅



**Microsoft Azure Stack (a.k.a. Azure Stack Hub, Azure Stack Edge, and to a lesser degree Azure Stack HCI)**

Azure Stack is, by Microsoft's own description, an extension of the Azure public cloud based on the same tools and software but deployed in customers' data centers. Available since 2016, it has not evolved much since the introduction. As of Q4 2020, it meets just a small subset of Enterprise and government cloud concerns, issues, and requirements.

**Cloud IaaS, PaaS, SaaS, DBaaS, 3<sup>rd</sup> Party Apps, Cloud Services, Data Behind Firewall**

Azure Stack can be completely separated from the Azure public cloud; although, it's not really meant to be. This is because the Azure Stack Hub supports a much-reduced set of Azure Cloud services.

Azure Stack offers only a subset of features and services available in the Azure public cloud:

- Only a subset of VM sizes.
- Auto scale is not supported.
- 256-bit AES encryption is not supported.
- Customer-managed encryption keys are not supported.
- Storage replication for DR is not supported.
- Native Azure SaaS is not supported.
- 3<sup>rd</sup> party SaaS is not supported.
- DBaaS has limited support, not the same as the Azure public cloud service

A big reason Azure Stack features and services are much reduced is that the core Azure Stack software is frozen-in-time. It's not the same software running in the Azure public cloud, making version control management and compatibility difficult and nightmarish.

Azure Stack supports specific versions of Azure PowerShell and Azure service APIs. In reality, not all Azure applications can be deployed on Azure Stack. Microsoft specifically encourages customers to use supported application versions to ensure that they can be deployed in the Azure Stack Hub, Azure Stack Edge, and Azure Stack HCI.

Azure Stack's primary focus is for development environments. Developers can create applications locally then run on the Azure Stack and/or in the Azure public cloud. This is where Azure Stack begins to fall short in meeting Enterprise and government requirements.

Microsoft positions Azure Stack as "well-suited" for Enterprises, governments, users, and applications with strict compliance requirements. But here's the contradiction, there are no software as a service (SaaS) applications from Microsoft or third-party independent software vendors (ISVs) available on Azure Stack. Even the database as a service (DBaaS) is a functionally challenged version of Azure SQL.

Conclusion: There are "zero" mission/business-critical class applications by definition, available today on Azure Stack in any of its forms.

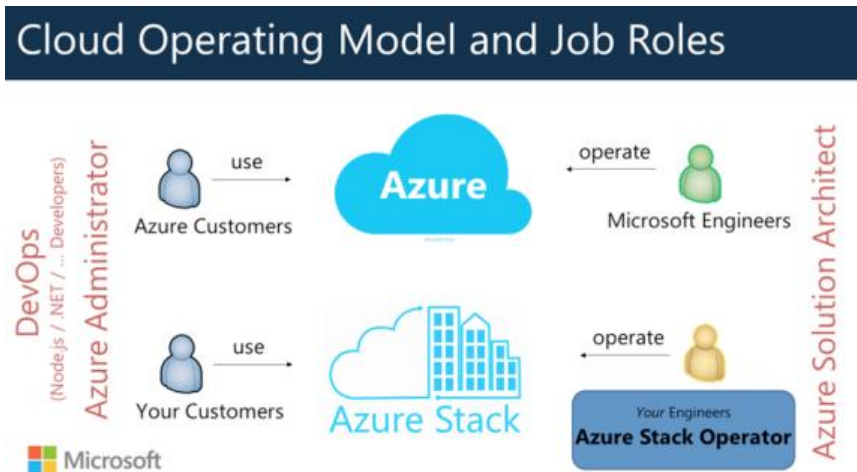
**Simplicity**

Azure Stack is deployed as an appliance with specific server and storage hardware components defined by Microsoft but assembled and delivered by third-party Azure partners such as HPE, Dell, Huawei, Cisco and others. This means customers call a hardware vendor for technical support and Microsoft for software support, which inevitably leads to increased stress and raised blood pressure rates. It provides most of the Azure public cloud tools, but a very limited set of its services that can run inside the customer's own premises or co-location datacenters. Azure Stack provides an IaaS and PaaS hardware abstraction layer through Resource Providers (RPs). RPs customize, configure, and control the hardware underlying both the Azure public cloud and Azure Stack. This is conceptually similar to a hypervisor. The Azure Resource Manager (ARM) calls on RPs to provide access to physical and virtual hardware services, automates deploying infrastructure, applications, and services (cloud orchestration).



That may on the surface sound okay. But a slightly deeper look shows that the Azure Stack is not even close to a fully managed service. Microsoft requires at least one dedicated Azure Stack Operator on-prem to

operate, plan, integrate, package/offer cloud resources and requested services on the Azure Stack infrastructure. Instead of reducing complexity and administrative personnel, it increases them and the associated costs. The Azure Stack customer is expected to carry the full payroll burden of this dedicated Azure Stack Operator. Costs that can run in excess of \$250,000 per year all-in. And realistically, most enterprises and governments can't rely on a single Azure Stack operator especially if they are running three shifts. That means at least two to three are required at a minimum, raising costs to as much as \$750,000 per year before paying for the actual cloud service. This isn't something that Microsoft highlights in its Azure Stack promotional videos.



Azure Stack SQL RP is actually an example of introducing additional complexity instead of achieving a state of simplicity. The Azure Stack SQL RP enables the Hub administrator or users to create and use SQL databases. However, those databases are not the same as those in Azure public cloud. The database functionality is reduced. They also have different processes for implementing, operating, and managing that are much more labor-intensive. The customer must first create a VM instance. Then they must create a SQL Server instance (either Azure Stack IaaS VMs or on non-Azure stack server VMs.) The SQL RP does not automatically do this, and the SQL Server instances must be allocated exclusively to the RP. SQL Server "Always On" databases must be configured separately in three different VMs across separate physical servers. There are also limitations in connecting on-prem database applications to the SQL Server databases running in the Azure Stack. It's labor-intensive and error prone. There is no database as a service (DBaaS) with Azure Stack.

Conclusion: Azure Stack is a complex assortment of parts, like a kit car more than a fully engineered high performance automobile.

#### Mission/Business Critical

Azure Stack is not close to meeting the criteria for mission/business-critical. Consider that Azure Stack has no built-in business continuity or instant recoveries from power outages, rack failures, data center disasters, or site failures. Downtime is inevitable when there's an outage even in a high availability (HA) configuration. Microsoft's documentation recommends placing VMs in availability set (VM redundancy) across multiple fault domains (single node in the Azure Stack Hub scale unit). When a physical server fails, VMs from that fault domain are restarted on other fault domains; however, there will be downtime. This is because as the VMs come back online they have to be rebalanced to maintain that HA. Microsoft provides Azure Stack with no service level agreements (SLAs) or service level objectives (SLOs) at this time. Third-party data protection software is limited because Azure Stack is a sealed system with permissions and network locked down.

The answer for Microsoft Azure Stack data protection in general and database data protection specifically, is limited, falling considerably short of meeting mission/business-critical requirements. For infrastructure backups, Microsoft offers Infrastructure Backup Service (full backups only). They also staunchly recommend Microsoft Azure Backup (MAB) as a VM, for file backups to Azure storage (full and incremental). For DR, Microsoft advocates Azure Site Recovery Service to replicate VMs to Azure Storage (full and incremental) asynchronously on outbound port HTTPS 443. Keep in mind that when the hardware infrastructure fails,

and it will fail, Azure Stack customers depend on the hardware partner to try and restore their environments using cloud recovery. The key takeaway is that every Azure Stack recovery and restore requires downtime. Performance of Azure Stack is difficult to pin down because it depends on the third-party vendor's hardware configuration. Published performance specs are extremely limited. Dell is the only vendor that has [published](#) some specifically configured Azure Stack HCI info (see Table 1).

Cluster Resources	Dell EMC AX-640 without Intel Optane DCPMM	Dell EMC AX-640 with Intel Optane DCPMM
Number of nodes	4	4
CPU	2 x Intel 6248 CPU @ 2.50 GHz (3.90 GHz with TurboBoost)	2 x Intel 6248 CPU @ 2.50 GHz (3.90 GHz with TurboBoost)
Memory	384 GB RAM	384 GB RAM
Drives	10 x 2.5 in. 1.92 TB Intel S4510 RI SATA SSD (76 TB)	10 x 2.5 in. 1.92 TB Intel S4510 RI SATA SSD (76 TB)
NICs	Mellanox ConnectX-5 EX Dual Port 100 GbE	Mellanox ConnectX-5 EX Dual Port 100 GbE
Persistent memory	None	<b>12 x 128 GB (1.5 TB) Intel Optane PM / node</b>
<b>VMFleet Storage Load generation tool testing</b>		
Transactional 100% Reads 4KB	2,103,412 IOPS 1.5-millisecond (ms) avg read latency	~ 3 million IOPS 700 microsecond (µs) avg read latency
Throughput Sequential Reads 512KB	11 GB/s	23 GB/s

Table 1: Dell EMC Azure Stack HCI Performance Results

Neither Microsoft nor any of its partners have published any Azure Stack Hub, Azure SQL, and SQL Server performance results at this time. It's important to recognize that Azure Stack Hub is not Azure Stack HCI. Azure Stack HCI is more of a Nutanix or VMware VxRail hyperconverged infrastructure alternative that is managed via the Azure public cloud. It enables VMs to move more easily between on-prem and the Azure public cloud, backs up Azure Stack HCI to the Azure public cloud, and can use the Azure public cloud as a DR site. It is not a managed service although customers can subscribe to the software. The scalability limitations appear to be four nodes, similar to VMware's VxRail, versus 16 nodes for Azure Stack Hub. Scalability for either falls short of Enterprise and government expectations. As for performance, consider that Oracle Autonomous Database on Exadata Cloud@Customer and on Dedicated Region Cloud@Customer is 37 to 79 times faster – much lower latency – than the published Azure Stack HCI numbers. Remember, Azure Stack Hub, the primary Azure Stack offering, does not support Intel® Optane™ Persistent Memory supported in Oracle Autonomous Database on Exadata Cloud@Customer and in Dedicated Region Cloud@Customer. That lack of support results in significantly higher latencies. As stated previously, time is money. Cloud charges are based on vCPU usage. Azure Stack throughput is as much 99.85% less and the IOPS as much as 87.5% less than Oracle's Cloud@Customer offerings. More on this later.

Support is another major mission/business-critical issue. Azure Stack is an on-prem system delivered by a third-party partner who also takes the first call for support. This complicates support. Microsoft calls out specific coordinated escalation and resolution procedures between Microsoft and the hardware partner. Those procedures still increase the time to find the root cause of problems and the ultimate resolution. Maintenance updates and patches including Windows Server security, non-security, and features, are also disruptive. Although updates/patches occur once a month, they are not automatic. The Azure Stack operator gets an alert in the admin panel and then must download the patches, which depending on the size can take a while. The Azure Stack RP applies the updates/patches to all affected components with viewable status as they're applied.

The problem is, once again, operational disruption. Per Microsoft, patching requires planned downtime: "these maintenance operations can affect existing tenant workloads and cause new tenant operations (for example, creating, reconfiguring, or deleting VMs) to fail, while other operations such as backup may also be unavailable." That means the Azure Stack operator must take the system offline for a period of time and that period of time can be relatively lengthy, according to the latest Microsoft release notes: "The 2002 update has had the following expected runtimes in our internal testing — 4 nodes: 15-42 hours; 8 nodes: 20-50 hours; 12 nodes: 20-60 hours; 16 nodes: 25-70 hours." (Note: 16 server nodes is the maximum Azure Stack Hub configuration, so it has limited scalability.) There is no rolling update capability. In addition, those downtime numbers do not include the updates provided by hardware vendors for the underlying infrastructure such as firmware, microcode, and driver updates/patches. The Azure Stack operator has to interface separately with the hardware manufacturers processes for those updates and patches.

Conclusion: With complicated, labor-intensive, time-consuming, and disruptive procedures causing downtime for long periods of time — as much as three days offline, Microsoft Azure Stack does not meet the Enterprise and government requirements for mission/business-critical infrastructure.

#### Data Sovereignty/Data Residency

Azure Stack can meet data sovereignty and data residency requirements if it is completely disconnected from the Azure public cloud. Doing so requires that customers provide their own Microsoft SQL Server licenses that are not managed by Microsoft or cloud-based pay-per-use licensing.

Conclusion: Meeting data sovereignty and data residency requirements with Microsoft Azure Stack is difficult.

#### Reduced TCO

Azure Stack is supposed to reduce an IT organization's costs, but reality shows that it raises TCO. That's because the mixed cost model of pay-per-use cloud pricing for the Azure Stack, plus hardware capital expenditures (CapEx), hardware support, and maintenance fees beyond standard warranties, is complex and only part of the TCO equation. Other rarely calculated costs include:

- Multiple Dedicated Azure Stack operators. For Enterprises and governments, there always needs to be more than one operator in case of illness, vacations, employee exits, or terminations.
- Tech refresh. Tech refresh takes extensive budget planning, bids, bake-offs, people, manual labor, time — always more than expected, professional services, and money — also always more than expected.
- Patching and updating, especially since it is disruptive, requires downtime, which means it has to be planned and scheduled well in advance, usually performed on a weekend with multiple IT personnel. That costs time and money.
- vCPU runtime costs for databases and applications. Even when running with Intel® Optane™ Persistent Memory on [Dell EMC infrastructure](#), Azure Stack still has relatively high latencies and low IOPS numbers. That means databases take longer to respond to queries. Azure Stack jobs are charged by the second. Running on Dell EMC infrastructure, Azure Stack runs approximately 39x to 79x slower than either Oracle Autonomous Database on Exadata Cloud@Customer or Oracle Dedicated Region Cloud@Customer (19µs). Time is money, meaning jobs in Azure Stack will have approximately 39 to 79 times higher fees.
- Requires a costly Enterprise support plan.

Conclusion: Azure Stack does not lower TCO — it increases it.

#### Azure Stack Summary

Azure Stack is primarily a platform for IT organizations to develop applications on-prem using the same tools they use in the Azure public cloud. This enables applications to be developed on-prem and run in the cloud or vice versa. Azure Stack does not fully address the concerns, issues, and needs of the Enterprise and governments. It is far more of a D.I.Y cloud kit than a fully managed cloud instance on a customer's premises.

Enterprises & Government Requirements	Microsoft
	Azure Stack
Behind Firewall	Limited
IaaS	✓
PaaS	✓
Native SaaS Cloud Apps	∅
3rd Party SaaS Cloud Apps	∅
DBaaS	Reduced
Data	Mixed
Cloud Services	7
Simplicity	∅
Mission/Business Critical	∅
Business Continuity	∅
Data protection & DR	✓
Top notch performance	∅
Scalability	∅
SLAs	∅
Availability	∅
Performance	∅
Manageability (API errors)	∅
Data Sovereignty/Data Residency	Partial
Reduced TCO	∅



### Google Cloud Platform (GCP) Anthos

GCP is by far the weakest offering compared to AWS Outposts and Azure Stack, and of course, way behind Oracle’s cloud on-prem solution. Google delivers Anthos, a multi-cloud Kubernetes container orchestration stack. It’s an amalgamation of three things:

1. Google Kubernetes Engine or GKE.
2. GKE on-prem.
3. Anthos configuration management console, a single pane of glass for managing policies and security across Kubernetes container implementations.

Anthos is not an on-prem public cloud software stack such as AWS Outposts, Azure Stack or Oracle Exadata Cloud@Customer. It’s not an on-prem cloud at all. Anthos doesn't extend GCP services into on-prem infrastructure. Anthos does not move the cloud behind the customer’s firewall. It’s chiefly an orchestration and management product / tool that enables applications to be developed and deployed using the Kubernetes service model in containers on-prem, in the Google public cloud, in both, and in other clouds. Customers can also deploy a variety of Anthos plugins to run services such as serverless functions.

Although it is hardware-agnostic, running on the majority of x86 servers in the market, there is no service to manage the underlying infrastructure. There is no cloud infrastructure at all on-prem. It is not an on-prem service.

### GCP Anthos Summary

Of the Enterprise or government cloud issues, the only one Anthos addresses is simplicity. There is nothing in Anthos that meets mission/business criticality, performance, reliability, scalability, automation, data sovereignty/data residency, regulatory compliance, or lowering TCO. It doesn’t address any one of these issues. In data center terms, GCP Anthos is a “no-op” for enterprise and government IT organizations.

Enterprises & Government Requirements	GCP
	Anthos
Behind Firewall	Limited
IaaS	∅
PaaS	✓
Native SaaS Cloud Apps	∅
3rd Party SaaS Cloud Apps	∅
DBaaS	∅
Data	∅
Cloud Services	∅
Simplicity	✓
Mission/Business Critical	∅
Business Continuity	∅
Data protection & DR	✓
Top notch performance	∅
Scalability	∅
SLAs	∅
Availability	∅
Performance	∅
Manageability (API errors)	∅
Data Sovereignty/Data Residency	∅
Reduced TCO	∅



### New Oracle Cloud@Customer Services

At 12PM Pacific Daylight Time (PDT) 8 July 2020, Larry Ellison, Oracle Chairman and CTO, announced two services that represent a massive paradigm shift for bringing the public cloud on-prem behind the customer’s firewall:

1. Oracle Autonomous Database on Exadata Cloud@Customer.
2. Oracle Dedicated Region Cloud @ Customer.

These announcements fundamentally redefine what it means to put the public cloud in the customer’s own data center behind the customer’s firewall. For the first time, there are services that completely resolve Enterprise and government IT organization’s concerns and issues for using the public cloud. These announcements are not coming out of left field. Oracle has been building up both its portfolio of public cloud services and data centers to offer these services for several years.

In public cloud data centers alone, Oracle had 16 as of September 2019. As of 5 August 2020, Oracle has 25 around the world. That’s the same number as AWS. Oracle is building out more data centers and is scheduled to have 36 in operation by the middle of 2021, which will be nine more than AWS is scheduled to have. Oracle is determined to build out at least two Cloud Regions in almost every country it operates. The US, Canada, EU, South Korea, Japan, India, and Australia already have two Cloud Regions. Upcoming second Cloud Regions include the UK, Brazil, UAE, and Saudi Arabia. The rationale is to guarantee data sovereignty and data residency in those countries for business continuity and DR.

With those facts as background, the latest Oracle Cloud@Customer announcements demonstrate Oracle’s push to solve the Enterprise and governmental issues with moving to public clouds while changing the on-prem cloud game completely. A detailed look at each announcement shows how.

## Oracle Autonomous Database on Exadata Cloud@Customer

This is the third iteration of Oracle Exadata Cloud@Customer<sup>1</sup> and by far the most advanced. Oracle Autonomous Database on Exadata Cloud@Customer is specifically architected to put mission/business-critical databases behind the customer's firewall while providing the best of public cloud elasticity on demand and pay-for-what-your-use charges. It is designed specifically for customers that want to move their Oracle Databases to the cloud but have to keep them on-prem because of sovereignty laws, industry regulations, corporate policies, security requirements, network latency, application performance, or because it's impractical to move their databases away from other tightly coupled on-prem IT infrastructure.

The Oracle Autonomous Database on Exadata Cloud@Customer combines the incomparable automation of the Oracle Autonomous Database with the unparalleled performance of the Exadata X8M as the consummate on-prem managed database cloud.

There are several reasons why the Oracle Autonomous Database on Exadata Cloud@Customer is so far ahead of everyone else when it comes to databases on-prem, the Enterprise, government, and other large IT organizations. It starts with the world market leader in databases as per Gartner<sup>2</sup> and DB-Engines<sup>3</sup>.

### Oracle Database

- Only Autonomous Database available today.
- First and most complete converged<sup>4</sup> database on the market with the vast majority of database types and data models using the same or different data. No ETLs are required.
  - *Relational*
  - *OLTP*
  - *OLAP*
  - *Data Warehouse*
  - *Object*
  - *XML*
  - *Key Value*
  - *JSON*
  - *Document*
  - *Time Series*
  - *Graphic*
  - *Spatial*
  - *Blockchain*
  - *IoT*
- Only Enterprise-class database with built-in machine learning algorithms ready to plug and play without programming language.

<sup>1</sup> Exadata Cloud@Customer was first made generally available and in production in 2016.

<sup>2</sup> [2019 Gartner Magic Quadrant for Operational Database Management Systems](#)

<sup>3</sup> [db-engines ranking](#)

<sup>4</sup> IBM DB2, SAP 4/HANA, and Microsoft Azure SQL claim multi-model/modal databases. But the number of types tend to be limited, or are performance constrained, and do not have the container database (CDB)/pluggable database architecture of Oracle. For a cloud database service, to get the performance or multi-tenancy, it generally means the customer must have multiple separate database instances without a common set of data. It frequently still requires ETLs again between databases. Most databases are a singular specialized type of database. That means each database requires its own specialized skills, knowledge, training, and expertise. Some have two in OLTP and data warehouses as part of the "hybrid transactional and analytical platform" specification. The Oracle Database incorporates every major database type into a single converged multi-tenant database with no data silos or separate database architectures to implement, operate, manage, and maintain.



Classification	Regression	Feature Extraction
Naive Bayes Logistic Regression (GLM) Decision Tree Random Forest Neural Network Support Vector Machine (SVM) Explicit Semantic Analysis	Linear Model Generalized Linear Model (GLM) Support Vector Machine (SVM) Stepwise Linear Regression Neural Network LASSO	Principal Comp Analysis (PCA) Non-negative Matrix Factorization Singular Value Decomposition (SVD) Explicit Semantic Analysis (ESA)
Clustering	Attribute Importance	Text Analysis
Hierarchical K-Means Hierarchical O-Cluster Expectation Maximization (EM)	Min Description Length Princippal Comp Analysis (PCA) Unsupervised Pair-Wise KL DIV CUR Decomposition for Row & AI	Sentiment Analysis Algorithms Support Text Tokenization & Theme Extraction Explicit Semantic Analysis (ESA) for Document Similarity
Time Series	SQL Analytics	Statistical Functions
Forecasting - Exponential Smoothing Includes Popular Models e.g. Holt-Winters w/trends, seasonality, irregularity, missing data	SQL Windows, Patterns, Aggregates	Basic Statistics: min, max, median, stdev, t-test, F-test, Pearson's, Chi-Sq, Anova, etc.
Anomaly Detection	Association Rules	R Packages
1-Class SVM	APriori / Market Basket  Predictive Queries Predict, Cluster, Detect, Features	3rd party R Packages through Embedded Execution Spark Mlib Algorithm Integration

The Oracle Autonomous Database on both Cloud@Customer offerings applies far-reaching administration services automation on top of the very latest Oracle Database software. It uses the very best Oracle Database practices with policy engines, decision trees, and advanced machine learning algorithms to automate the vast majority of manual database tasks including; provisioning, clustering, tuning, indexing, re-indexing, elastic resource scaling up and down, patching, upgrading, business continuity, data protection, disaster recovery, and security. The DBA no longer needs be an expert in database administration and can focus on applications using the database and developing new applications and services instead.

In addition, Oracle Autonomous Database leverages many of the most advanced, popular, industry-leading, production-proven, capabilities built into Oracle Database, such as:

- Real Application Clusters or RAC, nothing comparable available on the market for business continuity;
- Autonomous Data Guard (ADG) – automates the creation, operation, patching, backup, recovery for near instantaneous failover in the event of a total system or site outage between two active systems;
- Flashback enables reversing human errors by selectively and efficiently undoing the effects of a mistake in about as long as it took to make it;
- Recovery Manager (RMAN), the built-in database backup, recovery, and restore that sets the standard;
- Oracle Database Vault implements powerful security controls within Oracle Database 19c that restrict access to application data by privileged database users; and
- Multi-tenant Container Databases (CDB) with Pluggable Databases (PDB) of the same or different types.

#### Oracle Exadata X8M

Oracle Exadata X8M is the fastest, most powerful database machine currently available on planet earth. Nothing else is close no matter the database or hardware used. In Cloud@Customer configurations, it delivers read **latencies ≤ 19 μs**; up to **12 million 8KiB read IOPS**; and up to **300 GBps throughput**. Speed translates into reduced vCPU usage. And, for cloud services in the public cloud or on-prem, fees are based on vCPU usage per second. Time is definitively money in the cloud. Faster performance means less time for operations, and, of course, less money.

A closer look clearly illustrates how Oracle Autonomous Database on Exadata Cloud@Customer resolves those Enterprise and government IT organization's issues and concerns.

#### Cloud IaaS, PaaS, SaaS, DBaaS, 3<sup>rd</sup> Party Apps, Cloud Services, Data Behind Firewall

The Oracle Autonomous Database on Exadata Cloud@Customer is an on-prem cloud database service specifically for the Oracle Autonomous Database and the Exadata X8M infrastructure.

It does not provide PaaS or SaaS services at this time. However, the Autonomous Database capabilities mean that DBAs no longer have to manage the database—no provisioning, tuning, indexing, re-indexing, scaling, patching, backing up, etc. Getting a database up and running is as simple as picking the type of database (transaction processing or data warehousing), the capacity required, performance needed, and it's set. The rest is done autonomously. That frees up DBAs to work on strategic projects instead of on pedantic manual tasks. DBAs can then use the vast array of tools ready-to-use in the Oracle Database to

develop applications that create value from data in new ways, including machine learning algorithms, real-time analytics, graph analytics, documents, IoT, blockchain, and more.

Conclusion: By design, Oracle Autonomous Database on Exadata Cloud@Customer supports moving Oracle Databases to on-prem cloud infrastructure while automating DBA tasks.

#### Simplicity

The entire system is configured, installed, implemented and managed by Oracle in the customer's data center. Setting up a database is as simple as choosing the database type, OCPUs (vCPUs), and capacity. One click. That's it.

Conclusion: Doesn't get any simpler than that.

#### Mission/Business-Critical

The Oracle Autonomous Database on Exadata Cloud@Customer is designed from the ground up for mission/business-critical applications. It is the definitive market leader in performance, availability, flexibility, reliability, operability, and manageability. Oracle uniquely provides SLAs on performance, availability, and manageability.

Performance as previously noted, is the fastest and most scalable anywhere for any kind of database. Period. The performance of Oracle Autonomous Database on Exadata Cloud@Customer is typically up to two orders of magnitude better than its competitors for equivalent configurations.

Consider that it comes with built in automated HA, business continuity, disaster recovery, backup, and more. HA from Oracle Real Application Clusters (RAC). Should a node in the RAC fail for any reason, the system will detect the issue and reconfigure in three seconds or less. In other words, no noticeable outage. If there is a complete system or site failure, Oracle Autonomous Data Guard, set up with a single click, will fail over automatically to a second Oracle Autonomous Database on Exadata Cloud@Customer on the customer's site, a second site, or to a Oracle Cloud Infrastructure region. Backups via Oracle RMAN are automatic.

Patching and upgrades are done online automatically and autonomously for the databases, operating systems, and all hardware infrastructure without disruption or DBA intervention. Everything is done by a combination of the algorithms and Oracle. Rolling patching and upgrades occur on a per RAC node basis. The database is self-healing. In fact, it will detect and correct most problems without the DBA even being aware that a problem occurred.

Scaling is automated, elastic, on-demand, and fine grain pay-per-use to the second. No human intervention is required.

Conclusion: There is no doubt by any definition, that the Oracle Autonomous Database on Exadata Cloud@Customer is production-hardened mission/business-critical cloud solution.

#### Data Sovereignty/Data Residency

The Oracle Autonomous Database on Exadata Cloud@Customer default is to always keep the data on-prem to meet all data sovereignty and data residency requirements. This includes Data Guard business continuity, RAC HA, RMAN backups, and DR. All of it can remain within the customer's data center or data centers. The customer has the option to back up to the Oracle public cloud if the regional Oracle Cloud data center meets the organization's data sovereignty requirements.

Conclusion: Oracle Autonomous Database on Exadata Cloud@Customer meets all data sovereignty and data residency requirements.

#### Reduced TCO

The common industry assumption is that Oracle is expensive. Like most common wisdom, there is a grain of truth that often leads to an incorrect conclusion. The fees for Oracle Autonomous Database on Exadata Cloud@Customer are the same as the service offered in their Oracle public cloud based on usage over time. However, since Oracle deploys the hardware behind the customer's firewall on their premises, the customer must make a three-year commitment of at least \$10,000 per month. That's the grain of truth.

Here's where the conventional wisdom conclusion of "expensive" falls apart. As noted earlier, the exceptional performance of Oracle Autonomous Database on Exadata Cloud@Customer means jobs complete much faster than any other database cloud service. They complete as much faster than AWS or Azure ranging from twice as fast to 100 times faster. This means it costs less to run jobs. The autonomous

nature of this service means that DBAs do not have to be as experienced, knowledgeable, or skilled. They no longer have to manage or even operate the database. They spend a lot less time on managing the database, making them far more productive working on revenue-producing or cost-reducing projects.

In addition, the ability to consolidate hundreds to thousands of Oracle Databases of all types into the Oracle Autonomous Database on Exadata Cloud@Customer reduces database costs and storage costs by eliminating database data duplication and storage silos, power, cooling, hardware infrastructure, rack space, cabling, conduit and more.

Conclusion: The common wisdom is wrong. Oracle Autonomous Database on Exadata Cloud@Customer reduces TCO unlike any other cloud database on-prem service.

[The Oracle Autonomous Database on Exadata Cloud@Customer Summary](#)

Oracle Autonomous Database on Exadata Cloud@Customer addresses every Enterprise and government IT organization's issues and concerns with the cloud specifically for databases. Exadata is designed for Enterprise and government IT needs. Consider that for Oracle's first fiscal quarter of 2020 that ended in August, the company reported strong double-digit growth of on-prem Exadata. Revenues were up 15% with their largest backlog ever. This is for a product line that has been in the market for more than 11 years. At a time when on-prem infrastructure is tumbling at NetApp, Dell EMC, IBM, HPE and others, Oracle is taking material market share. In fact, IBM Power Systems in the company's most recent quarter cratered with a 28% year-on-year revenue decline. Exadata clearly solves Enterprise and government IT issues.

When Enterprises and government IT organizations need more than Exadata, such as IaaS, PaaS, SaaS applications, and other major cloud services, that's when Oracle's Dedicated Region Cloud@Customer comes into play.

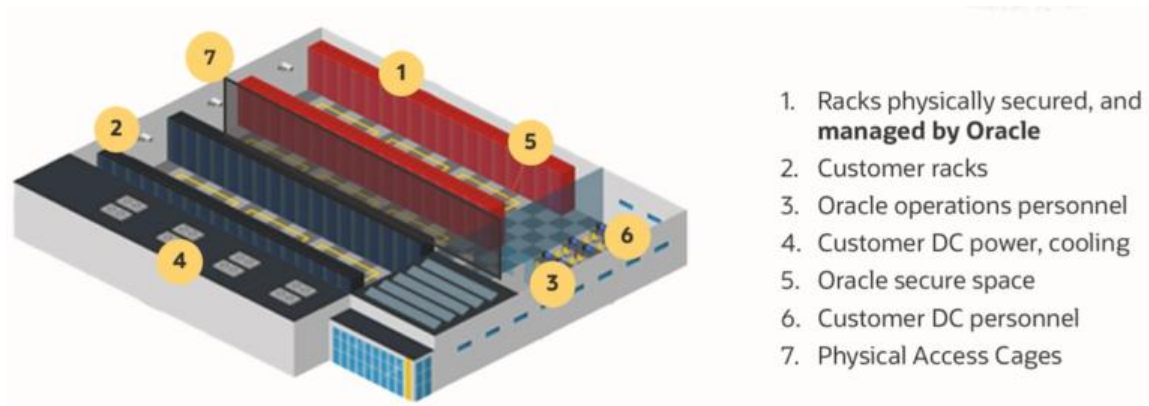
Enterprises & Government Requirements	Oracle
	Autonomous DB Exadata Cloud@Customer
Behind Firewall	✓ (DBaaS & data)
IaaS	∅
PaaS	∅
Native SaaS Cloud Apps	∅
3rd Party SaaS Cloud Apps	∅
DBaaS	✓
Data	✓
Cloud Services	2
Simplicity	✓
Mission/Business Critical	✓
Business Continuity	✓
Data protection & DR	✓
Top notch performance	✓
Scalability	✓
SLAs	✓
Availability	✓
Performance	✓
Manageability (API errors)	✓
Data Sovereignty/Data Residency	✓
Reduced TCO	✓



[Oracle Dedicated Region Cloud@Customer](#)

As much as the Oracle Autonomous Database on Exadata Cloud at Customer redefines database cloud on the customer's premises, Oracle Dedicated Region Cloud@Customer completely redefines hybrid clouds. It takes everything in the Oracle public cloud and duplicates it on-prem. It takes the concept of hybrid clouds and blow it out of the water with a fundamentally new definition.

It's 100% identical to the Oracle public cloud. It includes all of the same services, applications, tools, operating systems, virtualization, Oracle Databases (including the Autonomous Database), security, Oracle SaaS applications, third-party ISV applications, and infrastructure, including Exadata. This is a complete dedicated public cloud in the customer's data center, behind their firewall, fully managed by Oracle. Moreover, just as importantly, pay-per-usage fees and charges, etc. are identical to the Oracle public cloud.



Oracle Dedicated Region Cloud@Customer checks off every issue and concern of Enterprises and government IT organizations.

<b>Partner Ecosystem</b>					
<b>Next Layer Services</b>	Oracle SaaS	Big Data & Analytics	Container Ecosystem	Oracle on Oracle	DevOps
<b>Data Services</b>	Exadata	ATP	ADW	DBaaS	Other Data Management
<b>Core Services</b>	Compute & OS	Storage	Networking	Security	Governance & Management
<b>Regions</b>	<b>Oracle Dedicated Region Cloud @ Customer</b>				
	Infrastructure Orchestration	Software Defined Infrastructure			
	Control Plane HW   SW	Compute	Storage	Network Devices	
	Service Enclave	Customer Enclave			
	<b>Oracle Cloud Infrastructure Racks</b>				
	Space	Power	Cooling	External Connectivity	On-prem Connectivity
	<b>Customer Data Center</b>				

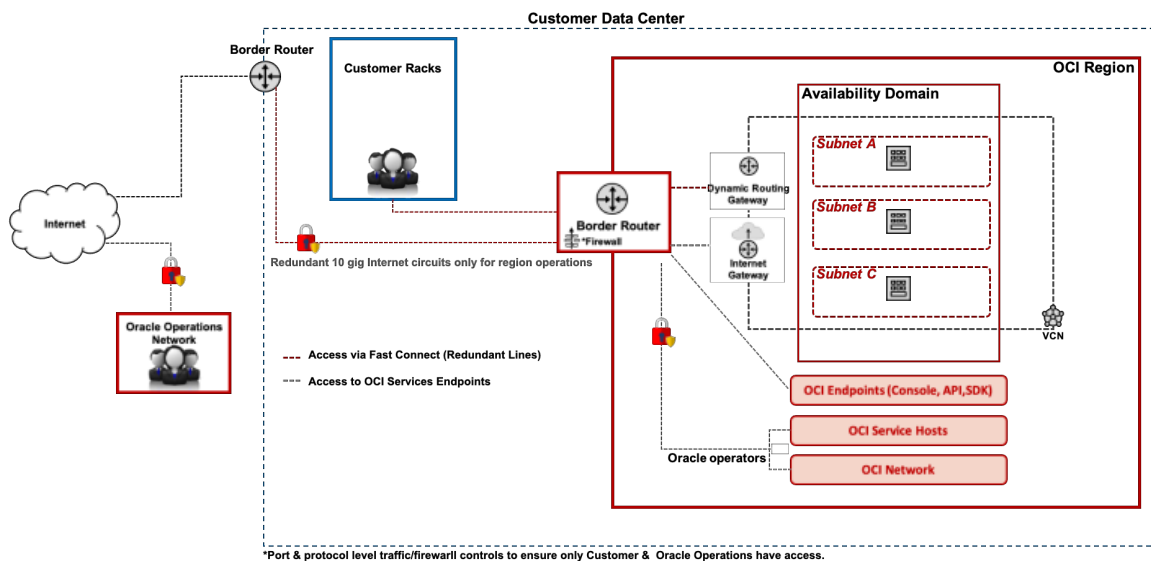
Cloud IaaS, PaaS, SaaS, database cloud service, 3<sup>rd</sup> Party Apps, Cloud Services, Data Behind Firewall

Everything is in the customer's data center. It looks, feels, and acts exactly as the Oracle public cloud. No services, tools, applications, third party, etc. are left out. It's a cut and paste of the Oracle public cloud hosted within the customer's data center.

Conclusion: Oracle Dedicated Region Cloud@Customer is a fully featured public cloud in the customer's data center. Oracle manages, operates, and maintains everything. SLA guarantees and pay-per-use match the Oracle public cloud.

### Simplicity

Oracle Dedicated Region Cloud@Customer is exactly the same as any Oracle public cloud region – called Oracle Cloud Infrastructure or OCI—same architecture, services, operations, SLAs, security, and billing. Everything is customizable based on the workload needs. Same value proposition as OCI. Zero infrastructure for customers to manage. Customers use the services, applications, and tools required and pay only for usage. Oracle determines with the customer how much Oracle Cloud Infrastructure is needed, then builds it out in the customer's data center. The entire process takes approximately 90 days.



Conclusion: Nothing could be simpler. Oracle builds and manages the infrastructure and all services.

### Mission/Business-Critical

Oracle Dedicated Region Cloud@Customer is architected from the ground up to be mission/business-critical. All services, performance, the database cloud, IaaS, PaaS, and SaaS. OCI has the exact same set of services as offered in the Oracle's public cloud regions.

Same performance as the public OCI. Same Oracle Database and Oracle Autonomous Database as the public OCI and Exadata Cloud@Customer. Same Oracle mission/business-critical SaaS applications as the public OCI. Same SLAs for availability, performance, and manageability as the public OCI, same everything.

Customers get new capabilities, upgrades, and security updates the moment they are available in the OCI public regions. Business continuity and DR can be between two distinct Oracle Dedicated Region Cloud@Customer locations or between one and a regional OCI location.

Solution: Oracle Dedicated Region Cloud@Customer is completely mission/business-critical capable.

### Data Sovereignty/Data Residency

Oracle Dedicated Region Cloud@Customer by design is self-contained. If customers need or want to keep the data on-prem completely, they can do so. If they need to keep the data in-country for data sovereignty, they can do that as well even with business continuity and DR. Business continuity, DR, and replication can be to another Oracle Dedicated Region Cloud@Customer or to an OCI region that meets data sovereignty and data residency requirements.

Conclusion: Oracle Dedicated Region Cloud@Customer easily meets data sovereignty and data residency requirements

### Reduced TCO

Oracle Dedicated Region Cloud@Customer is priced the same way as the Oracle public cloud, OCI. Same fees for everything. The way it reduces TCO is similar to how the Oracle Autonomous Database on Exadata Cloud@Customer does—with performance.

Oracle asserts unmatched Oracle Database [performance](#) for workloads running on the Exadata Cloud Service, Database Cloud bare metal, or in a VM with block storage. There is nothing faster or even close for that matter. Faster database performance tightly correlates into faster database application performance

and response times. That reduces vCPU time. Customers are only charged for what they use, thereby reducing costs. Oracle charges based on the number of vCPUs used over time. Less time equals less cost. With automatically finely granular elastic up and down capabilities in Oracle Dedicated Region Cloud@Customer, costs are significantly reduced.

Oracle claims Dedicated Region Cloud@Customer has more than twice the price-performance for compute in general purpose and memory-optimized instances versus AWS. In addition, Oracle claims up to 20 times the performance of block storage at 58% lower cost than AWS EBS. Oracle also asserts much better bare metal price-performance. With I/O-intensive workloads delivering the highest IOPS at a much lower price versus AWS, and HPC workloads providing 44% lower cost with the same performance as AWS.

However, deploying the Oracle Dedicated Region Cloud@Customer requires a 3 years usage commitment or more. There is also a commitment for at least \$500,000 worth of usage per month or \$6 million per year. This service is obviously aimed at Enterprises and large government IT organizations.

Conclusion: Oracle Dedicated Region Cloud@Customer reduces TCO due to performance and full stack economic advantages compared to the alternatives. No other cloud service provider offers a complete cloud stack on-premises, SaaS application suite, or any Autonomous Database capabilities Oracle brings to the table.

#### Oracle Dedicated Region Cloud@Customer Summary

Oracle Dedicated Region Cloud@Customer is the only full stack Cloud on customer premises or hybrid deployment option that is specifically architected for large Enterprise and government IT organizations. It uniquely addresses every issue and concern about using a public cloud that is deployed on the customer's premises.

Enterprises & Government Requirements	Oracle
	Dedicated Region Cloud@Customer
Behind Firewall	✓
IaaS	✓
PaaS	✓
Native SaaS Cloud Apps	✓
3rd Party SaaS Cloud Apps	✓
DBaaS	✓
Data	✓
Cloud Services	≥ 50
Simplicity	✓
Mission/Business Critical	✓
Business Continuity	✓
Data protection & DR	✓
Top notch performance	✓
Scalability	✓
SLAs	✓
Availability	✓
Performance	✓
Manageability (API errors)	✓
Data Sovereignty/Data Residency	✓
Reduced TCO	✓

### Conclusion

Public clouds deliver huge value. The problem is that many Enterprises and governmental IT organizations cannot take advantage of public clouds. They have several mission/business-critical applications that for reasons of legal and regulatory compliance, security, data residency, data sovereignty, and control, they have to run on-prem behind their firewall. And this isn't changing anytime soon. In fact, it won't change this decade.

Most public cloud on-prem solutions are half measures at best meant to enable organizations to be half in and half out of the cloud. They're aimed principally at application development while allowing some cloud services and applications, but not mission/business-critical application deployments. This is why AWS, Azure, and Google Cloud Platform have failed to satisfactorily solve this problem for Enterprise and government IT organizations.

Oracle is the first to address all of their requirements. That's why Oracle has completely changed the game for on-prem public clouds, outmaneuvering AWS, Azure, GCP and all other cloud service providers.

Enterprises & Government Requirements	Oracle		AWS	Microsoft	GCP
	Autonomous DB Exadata Cloud@Customer	Dedicated Region Cloud@Customer	Outposts	Azure Stack	Anthos
Behind Firewall	✓ (DBaaS & data)	✓	Limited	Limited	Limited
IaaS	∅	✓	✓	✓	∅
PaaS	∅	✓	∅	✓	✓
Native SaaS Cloud Apps	∅	✓	∅	∅	∅
3rd Party SaaS Cloud Apps	∅	✓	∅	∅	∅
DBaaS	✓	✓	✓	Reduced	∅
Data	✓	✓	Mixed	Mixed	∅
Cloud Services	2	≥ 50	7	7	∅
Simplicity	✓	✓	∅	∅	✓
Mission/Business Critical	✓	✓	∅	∅	∅
Business Continuity	✓	✓	∅	∅	∅
Data protection & DR	✓	✓	✓	✓	✓
Top notch performance	✓	✓	∅	∅	∅
Scalability	✓	✓	∅	∅	∅
SLAs	✓	✓	∅	∅	∅
Availability	✓	✓	∅	∅	∅
Performance	✓	✓	∅	∅	∅
Manageability (API errors)	✓	✓	∅	∅	∅
Data Sovereignty/Data Residency	✓	✓	Partial	Partial	∅
Reduced TCO	✓	✓	∅	∅	∅

### For More Information on the Oracle Cloud@Customer Services

Go to: [Oracle Autonomous Database on Cloud@Customer](#)

Go to: [Oracle Dedicated Region Cloud@Customer](#)

This technical paper is sponsored by Oracle. **About the author:** Marc Staimer, as President and founder of the 22-year-old DSC in Beaverton, OR, is well known for his in-depth and keen understanding of user problems, especially with storage, networking, applications, cloud services, data protection, and virtualization. Marc has published thousands of technology articles and tips from the user perspective for internationally renowned online trades including many of TechTarget's IT news sites and Network Computing and GigaOM. Marc has additionally delivered hundreds of white papers, webinars, and seminars to many well-known industry giants such as: Cisco, DELL, EMC, Emulex (Avago), HDS, HPE, LSI (Avago), Mellanox, NEC, NetApp, Oracle, QLogic, SanDisk, and Western Digital. He has additionally provided similar services to emerging companies including: Asigra, Cloudfenna, Clustrix, ConduSiv, DH2i, Diablo, FalconStor, Gridstore, ioFABRIC, Nexenta, Neuxpower, NetEx, NoviFlow, Pavilion Data, Permabit, Qumulo, SBDS, StorONE, Tegile, and many more. His speaking engagements are always well attended, often standing room only, because of the pragmatic, immediately useful information provided. Marc can be reached at [marcstaimer@me.com](mailto:marcstaimer@me.com), (503)-312-2167, in Beaverton OR, 97007.