



Responsibility Matrix: Bring Your Own Cloud (BYOC) - Managed Service

This matrix outlines specific responsibilities for operating in a Bring Your Own Cloud* (BYOC) deployment. For application-specific requirements, please refer to the relevant responsibility matrix.

Process / Task / Responsibility	NetApp Instaclustr	Customer
Cloud Provider Account		
Configure cloud provider account according to NetApp provided BYOC setup guide for nominated cloud provider(s)		X
Configuration of cloud provider account backup storage following setup guide		X
Structure cloud account to meet NetApp Instaclustr permissions and data sensitivity requirements		X
Create, modify, configure, and delete clusters and associated resources in the NetApp Instaclustr Managed Platform		X
Create, modify, configure, and delete required resources in the cloud provider account as part of cluster creation and modification	X	
Responsible for not modifying any resources or configuration created by NetApp Instaclustr's provisioning system directly in the cloud provider account without first getting agreement of those changes with NetApp including: • Firewall Rules • VPC or VNET Peering Connections • Virtual Machines		X
Monitor and pay cloud infrastructure charges		X



Process / Task / Responsibility	NetApp Instaclustr	Customer
Security		
Responsible for the security of all resources created by NetApp Instaclustr within the customer's cloud provider account (including instances, firewall rules, etc.).	X	
Intrusion detection/prevention to NetApp Instaclustr-managed nodes	X	
Retain exclusive operating system root privileges and console login	X	
Monitor instances for unexpected processes or connections	X	
Responsible for security of all other assets in customer cloud provider account		X
Monitoring cloud account activity for suspicious activity including: - Compromised user accounts/suspicious user activity - Unusual storage/bucket access - Signs of compromised [non-NetApp Instaclustr] hosts - Monitoring all [non-NetApp Instaclustr] assets Compromised user accounts/suspicious user activity Unusual storage/bucket access Signs of compromised [non-NetApp Instaclustr] hosts		X
Monitoring all non-Instaclustr assets		X



Process / Task / Responsibility	NetApp Instaclustr	Customer
Incident Resolution		
Provide 24x7 support for underlying node instances per support level SLA	X	
Assess impact of any incident (including security incident) to customer business as per severity levels defined in the support policy.	X	
Notify customer on detection of incident which may have customer-visible impact, and provide updates on progress and resolution	X	

Note: For PCI enabled clusters, please refer to the additional responsibility matrix:
<https://www.instaclustr.com/support/documentation/useful-information/pci-compliance/>

** Bring Your Own Cloud (BYOC) was previously referred to as Run in Your Own Account (RIYOA).*

NetApp® Instaclustr specializes in open source technologies for enterprises. Our managed platform streamlines data infrastructure management, backed by experts who ensure ongoing performance, scalability, and optimization. This enables companies to focus on building cutting edge applications at lower costs.