As an HCI solution on bare metal servers, there are minimum node hardware and network requirements for installing and running Harvester.

A three-node cluster is required to fully realize the multi-node features of Harvester. The first node that is added to the cluster is by default the management node. When the cluster has three or more nodes, the two nodes added after the first are automatically promoted to management nodes to form a high availability (HA) cluster.

Certain versions of Harvester support the deployment of single-node clusters. Such clusters do not support high availability, multiple replicas, and live migration.

Hardware Requirements

Harvester nodes have the following hardware requirements and recommendations for installation and testing.

Hardware	Development/Testing	Production
CPU	ARM64 or x86_64 (with hardware-assisted virtualization); 8 cores minimum	ARM64 or x86_64 (with hardware-assisted virtualization); 16 cores minimum
Memory	32 GB minimum	64 GB minimum
Disk capacity	250 GB minimum (180 GB minimum when using multiple disks)	500 GB minimum, 1 TB or more recommended
Disk performance	5,000+ random IOPS per disk (SSD/NVMe); management node storage must meet etcd speed requirements. Only local disks and hardware RAID are supported.	5,000+ random IOPS per disk (SSD/NVMe); management node storage must meet etcd speed requirements. Only local disks and hardware RAID are supported.
Network card count	Management cluster network: 1 NIC required, 2 NICs recommended; VM workload network: 1 NIC required, at least 2 NICs recommended (does not apply to the witness node)	Management cluster network: 1 NIC required, 2 NICs recommended; VM workload network: 1 NIC required, at least 2 NICs recommended (does not apply to the witness node)
Network card speed	1 Gbps Ethernet minimum	10 Gbps Ethernet minimum
Network switch	Port trunking for VLAN support	Port trunking for VLAN support

:::info important

- Mixed-architecture clusters are not supported. Deploy separate clusters to avoid unexpected system behavior.
- For best results, use YES-certified hardware for SUSE Linux Enterprise Server (SLES) 15 SP3 or SP4. Harvester is built on SLE technology and YES-certified hardware has additional validation of driver and system board compatibility. Laptops and nested virtualization are not supported.
- Nested virtualization is not supported on virtual machines running on Harvester.

- Each node must have a unique `product_uuid` (fetched from `/sys/class/dmi/id/product_uuid`) to prevent errors from occurring during VM live migration and other operations. For more information, see Issue #4025.
- Harvester has a built-in management cluster network (`mgmt`). To achieve high availability and the best performance in production environments, use at least two NICs in each node to set up a bonded NIC for the management network (see step 6 in ISO Installation). You can also create custom cluster networks for VM workloads. Each custom cluster network requires at least two additional NICs to set up a bonded NIC in every involved node of the Harvester cluster. The witness node does not require additional NICs. For more information, see Cluster Network.
- During testing, you can use only one NIC for the built-in management cluster network (`mgmt`), and for testing the VM network that is also carried by `mgmt`. High availability and optimal performance are not guaranteed.
- If the disk only meets the minimum required capacity, you may encounter issues related to the free system partition space requirement during upgrades. :::

CPU Specifications

Live Migration functions correctly only if the CPUs of all physical servers in the Harvester cluster have the same specifications. This requirement applies to all operations that rely on Live Migration functionality, such as automatic VM migration when Maintenance Mode is enabled.

Newer CPUs (even those from the same vendor, generation, and family) can have varying capabilities that may be exposed to VM operating systems. To ensure VM stability, Live Migration checks if the CPU capabilities are consistent, and blocks migration attempts when the source and destination are incompatible.

When creating clusters, adding more hosts to a cluster, and replacing hosts, always use CPUs with the same specifications to prevent operational constraints.

Network Requirements

Harvester nodes have the following network requirements for installation.

Port Requirements for Harvester Nodes

Harvester nodes require the following port connections or inbound rules. Typically, all outbound traffic is allowed.

Protocol	Port	Source	Description
TCP	2379	Harvester management nodes	Etcd client port
TCP	2381	Harvester management nodes	Etcd metrics collection
TCP	2380	Harvester management nodes	Etcd peer port
TCP	2382	Harvester management nodes	Etcd client port (HTTP only)
TCP	10010	Harvester management and compute nodes	Containerd

TCP	6443	Harvester management nodes	Kubernetes API
TCP	9345	Harvester management nodes	Kubernetes API
TCP	10252	Harvester management nodes	Kube-controller-manager health checks
TCP	10257	Harvester management nodes	Kube-controller-manager secure port
TCP	10251	Harvester management nodes	Kube-scheduler health checks
TCP	10259	Harvester management nodes	Kube-scheduler secure port
TCP	10250	Harvester management and compute nodes	Kubelet
TCP	10256	Harvester management and compute nodes	Kube-proxy health checks
TCP	10258	Harvester management nodes	cloud-controller-manager
TCP	10260	Harvester management nodes	cloud-controller-manager
TCP	9091	Harvester management and compute nodes	Canal calico-node felix
TCP	9099	Harvester management and compute nodes	Canal CNI health checks
UDP	8472	Harvester management and compute nodes	Canal CNI with VxLAN
TCP	2112	Harvester management nodes	Kube-vip
TCP	6444	Harvester management and compute nodes	RKE2 agent
TCP	10246/10247/10248/10249	Harvester management and compute nodes	Nginx worker process
TCP	8181	Harvester management and compute nodes	Nginx-ingress-controller
TCP	8444	Harvester management and compute nodes	Nginx-ingress-controller
TCP	10245	Harvester management and compute nodes	Nginx-ingress-controller

TCP	80	Harvester management and compute nodes	Nginx
TCP	9796	Harvester management and compute nodes	Node-exporter
TCP	30000-32767	Harvester management and compute nodes	NodePort port range
TCP	22	Harvester management and compute nodes	sshd
UDP	68	Harvester management and compute nodes	Wicked
TCP	3260	Harvester management and compute nodes	iscsid

Port Requirements for Integrating Harvester with Rancher

If you want to integrate Harvester with Rancher, you need to make sure that all Harvester nodes can connect to TCP port **443** of the Rancher load balancer.

When provisioning VMs with Kubernetes clusters from Rancher into Harvester, you need to be able to connect to TCP port **443** of the Rancher load balancer. Otherwise, the cluster won't be manageable by Rancher. For more information, refer to Rancher Architecture.

Port Requirements for K3s or RKE/RKE2 Clusters

For the port requirements for guest clusters deployed inside Harvester VMs, refer to the following links:

- K3s Networking
- RKE Ports
- RKE2 Networking

Time Requirements

A reliable Network Time Protocol (NTP) server is critical for maintaining the correct system time across all nodes in a Kubernetes cluster, especially when running Harvester. Kubernetes relies on etcd, a distributed key-value store, which requires precise time synchronization to ensure data consistency and prevent issues with leader election, log replication, and cluster stability.

Ensuring accurate and consistent time across the cluster is essential for reliability, security, and overall system integrity.