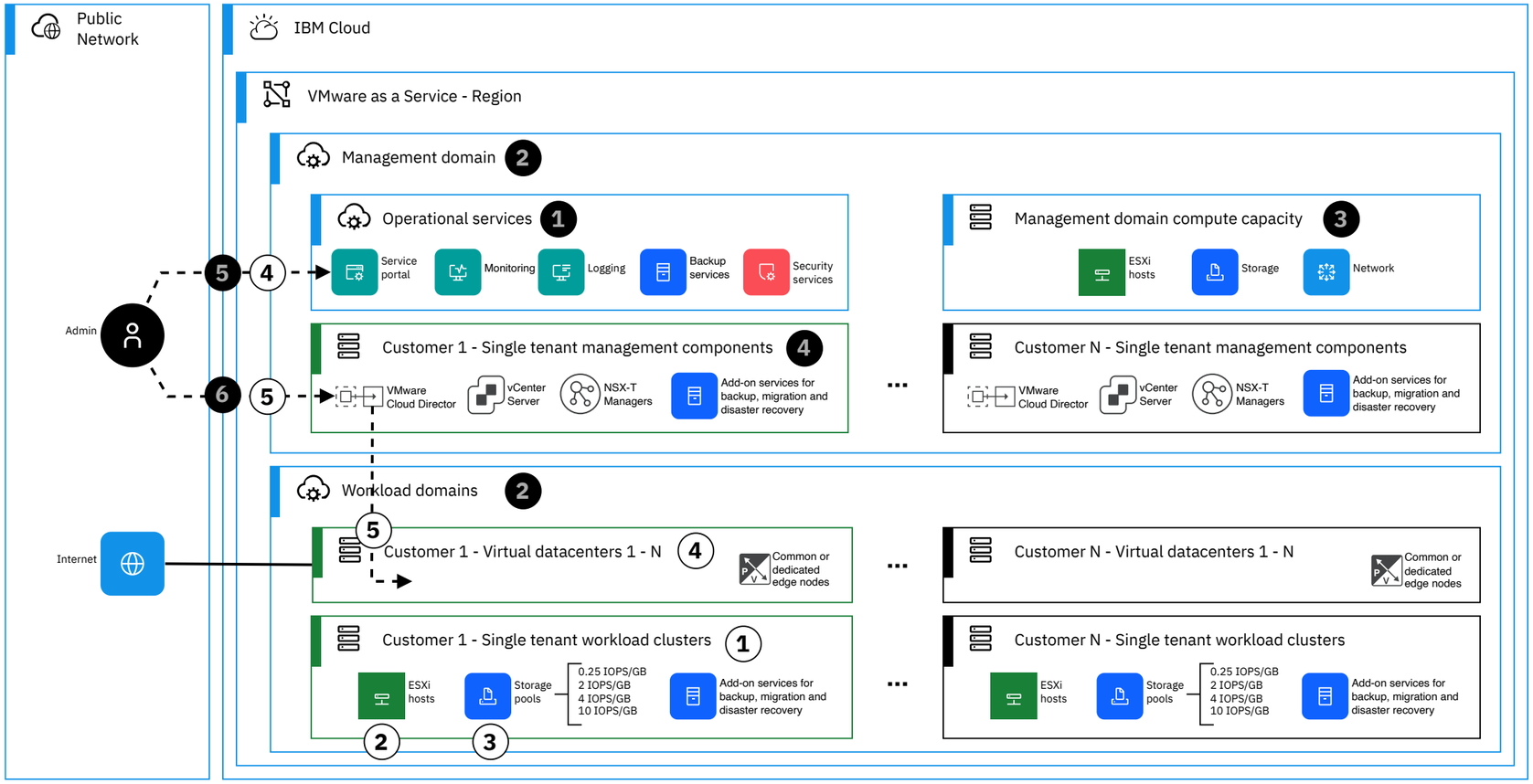
IBM Cloud

Printed 2022-10-27

Reference architecture for VMware as a Service - Single tenant

IBM Cloud® managed VMware as a Service (VMWaaS) delivers a VMware Cloud Director platform running on dedicated IBM Cloud® Bare Metal Servers. Each single tenant instance provides dedicated management plane and dedicated compute to where you can deploy one or more secure and isolated virtual data centers through the VMware Console. IBM Cloud® monitors, patches and maintains the underlying VMware environment and hardware.



Technical specifications for Single Tenant instances

- VMware stack is managed by IBM Cloud
- Dedicated hosts and multiple host profiles
- Multiple performance options for attached Network File Storage
- Monthly charges
- Public and private networking
- Multiple networking edge type options
- (Future) vSAN
- (Future) Client-managed keys - Bring Your Own Key (BYOK)
- (Future) Add-on third-party services for backup, migration, and storage

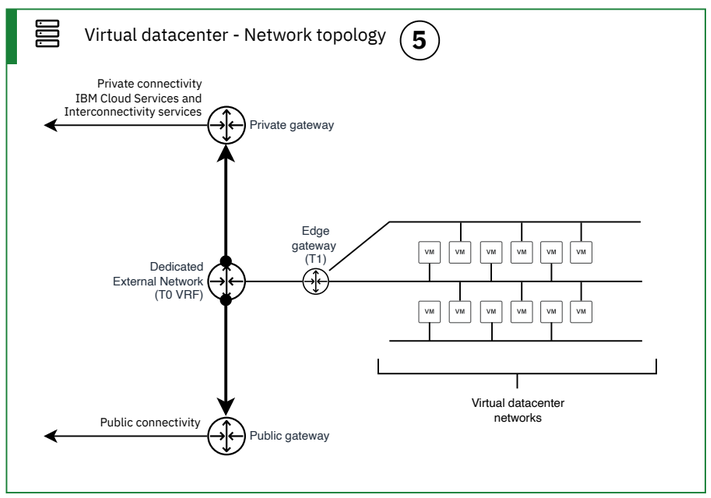
Service portal

You can manage the lifecycle of virtual data centers by using the VMware as a Service offering. The following functions are supported when you use the VMware as a Service console or public API:

- VMware site creation
- VMware site deletion
- VMware site capacity elasticity
- Virtual data center creation
- Virtual data center deletion

1. VMware as a Service is a IBM Cloud managed service where IBM Cloud monitors, patches and maintains the VMware environment and underlying hardware.
2. The solution separates management and workload domains logically and also physically.
3. Management workloads are hosted on a highly resilient management clusters, separate from your workload clusters and managed by IBM Cloud.
4. In the single tenant instance, the VMware management appliances are dedicated to your instance only, and are not shared between other customers.
5. Service portal is used to manage the lifecycle of the VMware as a Service instance (VMware site).
6. Virtual data centers are managed though VMware Console (VMware Cloud Director). A virtual data center contains your virtual data center networks and virtual machines.

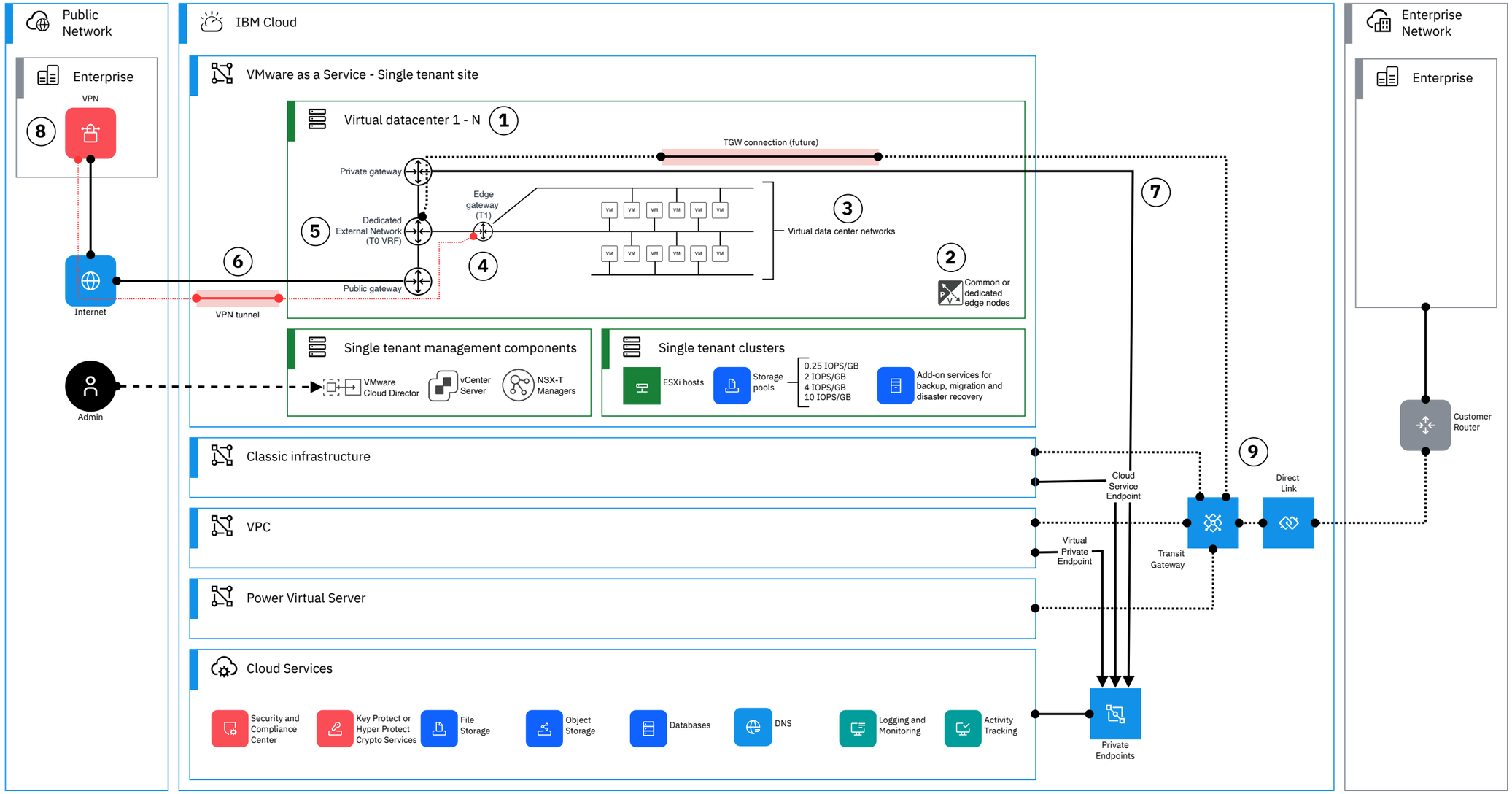
1. In the VMWare as a Service - Single tenant instance, you can deploy a cluster consisting of two or more hosts, and one or more NFS shares with variable performance options.
2. VMware deployments are sized based on the CPU, memory, and storage that are required to run the targeted workload. VMware deployments are elastic and you can resize them at any time.
3. For the attached Network File Storage, you can choose from the following storage performance tiers: 0.25 IOPS/GB, 2 IOPS/GB, 4 IOPS/GB or 10 IOPS/GB. *) vSAN is in the roadmap.
4. After the instance has been provisioned, you can create one or more virtual data centers though the Service portal or order add-on services (future). Virtual data centers consume the compute and storage resources from your dedicated cluster.
5. Virtual data centers are managed though VMware Console (VMware Cloud Director). You can create and configure your virtual data center networks, import and create VMs, and use the add-on services (future) though the VMware Console.



Printed 2022-10-27

Network architecture for VMware as a Service - Single tenant

IBM Cloud® managed VMware as a Service (VMWaaS) delivers a VMware Cloud Director platform running on dedicated IBM Cloud® Bare Metal Servers. Each single tenant instance provides dedicated management plane and dedicated compute to where you can deploy one or more secure and isolated virtual data centers through the VMware Console. IBM Cloud® monitors, patches and maintains the underlying VMware environment and hardware.



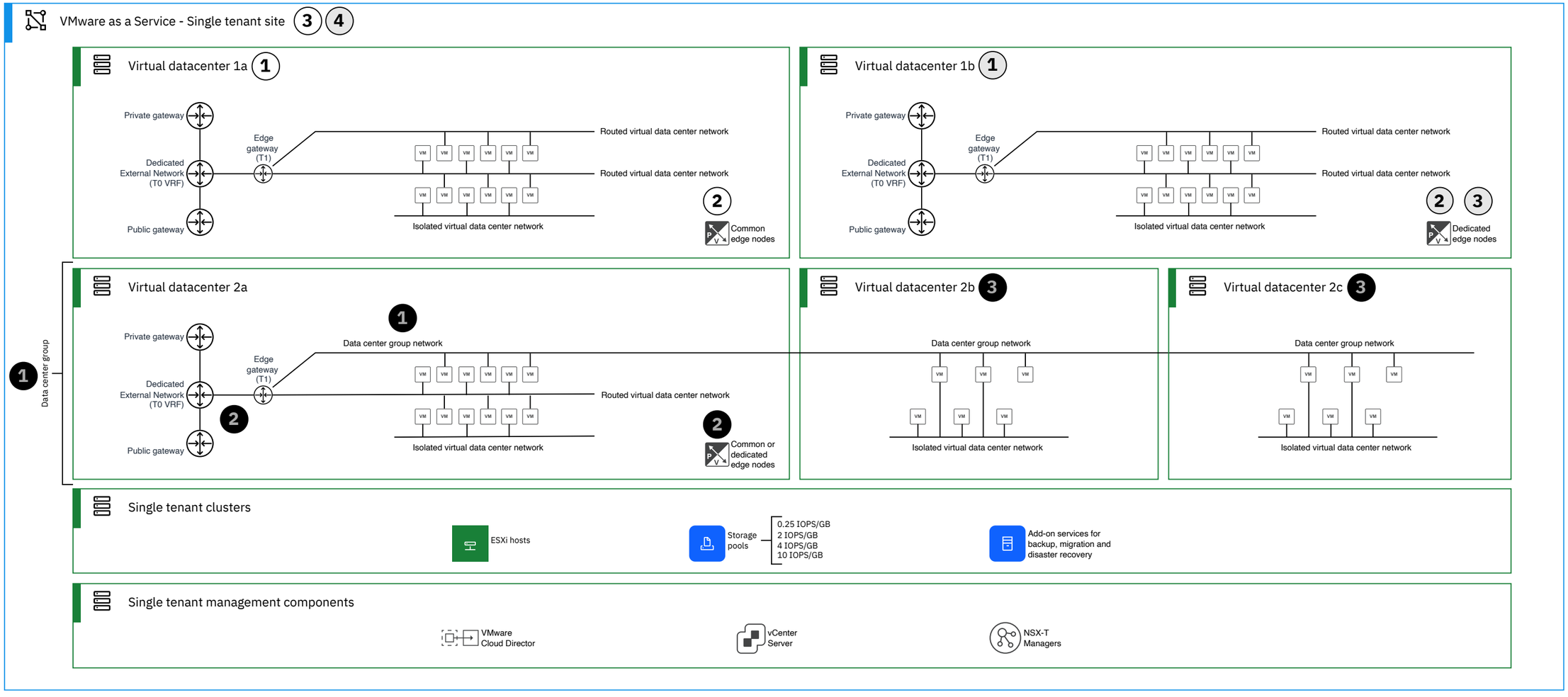
1. You can create one or more virtual data centers in the single tenant clusters. Networking uses NSX-T Tier 1 and Tier 0 gateways, which are hosted in the NSX-T edge nodes deployed on your workload domain.
2. You can select between common or dedicated edge nodes per virtual data center. Edge node virtual machines are deployed on your dedicated cluster. Common edge nodes are good for low and moderate bandwidth needs, and dedicated edge nodes can be used for high bandwidth use cases.
3. Virtual data center networks are created inside each virtual data center and by default they are visible only within that virtual data center. You may optionally share virtual data center networks with other virtual data centers inside your Singe Tenant Site.
4. Edge gateway (NSX-T Tier 1) is the default gateway for the routed virtual data center networks. You can optionally create isolated networks, which are not attached to the edge gateway. You can create firewall and NAT rules as well as configure VPN services on the edge gateway.
5. Dedicated external network (NSX-T Tier 0 VRF) is created for each virtual data center, which has private and public connectivity.
6. Public connectivity is provided though an interface connected to Public Gateway and IBM Cloud frontend routers. Public IP addresses are provided by IBM Cloud. Each virtual data center is provides a default number of public IPs and you can order more if needed.
7. Private connectivity to IBM Cloud Services is provided through an interface connected to Private Gateway and IBM Cloud backend routers. Connectivity to IBM Cloud services can be established through Cloud Services Endpoints.
8. VPN tunnels (policy based IPsec or L2VPN) can be established between virtual data center and on-premises though IBM Cloud public network and Internet.
9. Interconnectivity (future) to VPCs, Classic infrastructure, Power Virtual Servers or Direct Links is provided through TGW connection to IBM Cloud Transit Gateway. BGP is used as the routing protocol to exchange routing information between the Virtual data center and Transit Gateway.

IBM Cloud

Printed 2022-10-27

Virtual data center network architectures

IBM Cloud® managed VMware as a Service (VMWaaS) delivers a VMware Cloud Director platform running on dedicated IBM Cloud® Bare Metal Servers. You can deploy one or more secure and isolated virtual data centers through the VMware Console with embedded flexible networking services using either cost effective common edge nodes or dedicated edge nodes for higher bandwidth needs. Optionally, you can also share networks between virtual data centers.



1. Virtual data center defines the logical isolation to host various user or application groups within your single tenant site or instance. You can have a virtual data center 1a (or multiple of this type) and it has its networks inside the virtual data center.
2. You can use either the common or dedicated edge nodes to host virtual data center Dedicated External Network (Tier 0 VRF) and Edge Gateway (Tier 1). This allows you to optimise and scale network performance and throughput per virtual data center. Using common edge nodes provide you a low compute overhead and cost effective solution for low and moderate bandwidth needs.
3. Note that the scope of virtual data centers and networks is this single tenant site. Also each virtual data center and its networking is configured individually.

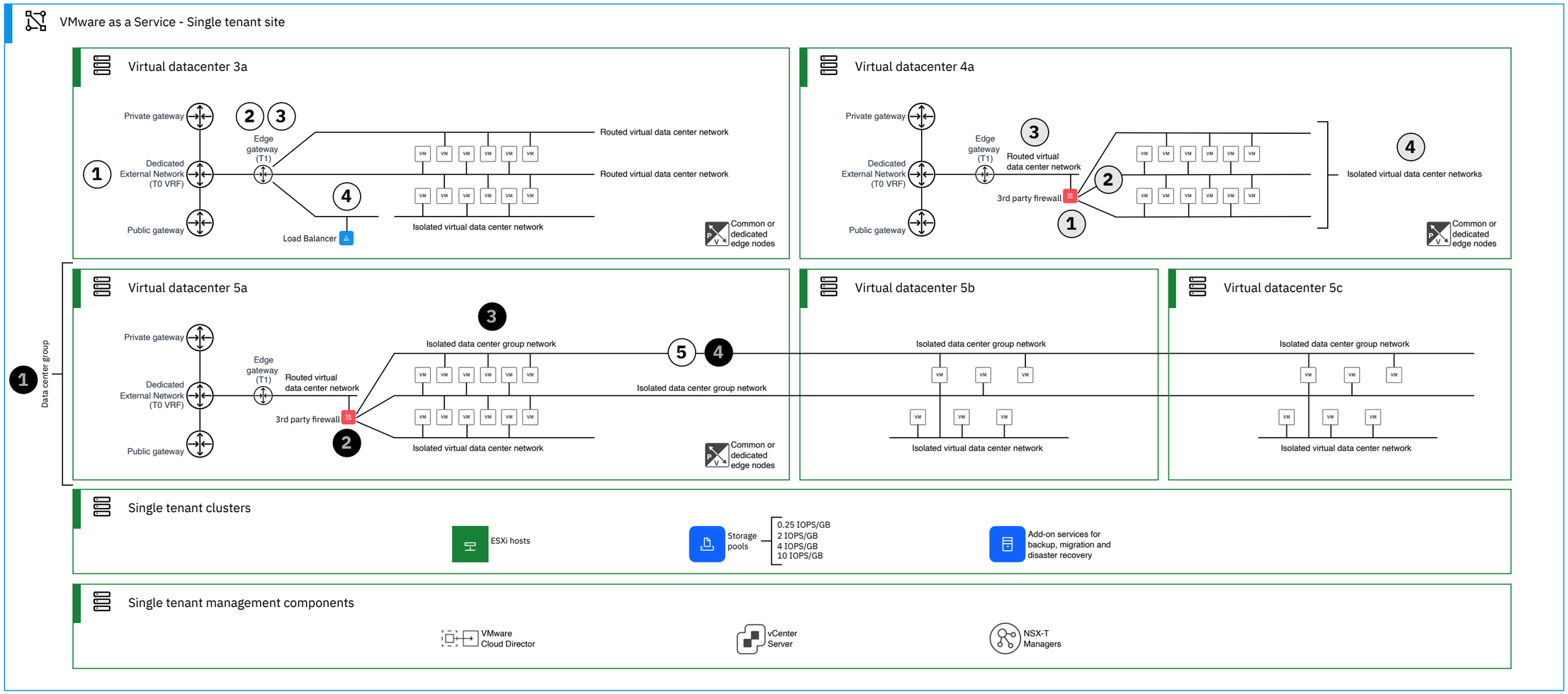
1. You can have another virtual data center 1b (or multiple of this type). The Dedicated External Network (Tier 0 VRF) and Edge Gateway (Tier 1) of this virtual data center are hosted on the dedicated edge nodes.
2. Dedicated edge nodes provide the same network architecture as common edge nodes, but they are be used to provide dedicated compute capacity (virtual machines) for the virtual datacenter's networking to provide high bandwidth for your workloads. This allows you to optimise and scale network performance and throughput per virtual data center.
3. There are multiple size options for the dedicated edge nodes: medium, large and extra large following NSX edge transport node sizes.
4. Note that the scope of virtual data centers and networks is still this single tenant site.

1. You can optionally create networks are shared between multiple virtual data centers. You can group virtual data centers into data center groups, which can then share networking amongst them. While virtual data center networks are local, data center group networks can span multiple virtual data centers. Both network types can be either routed or isolated within their domain. *) Multi-zone networking is in the roadmap.
2. To provide routing in and out of the data center group, the Dedicated External Network (Tier 0 VRF) and Edge Gateway (Tier 1) in 2a provide the the egress connections. These can be hosted on the selected edge node type (common or dedicated) to provide a the suitable solution for your bandwidth needs.
3. You can have other virtual data centers, like virtual data centers 2b and 2c, which can see the shared networks and attach their workloads to these. They can then use the shared external networking connectivity provided by virtual data center 2a. These virtual data centers can also have local virtual data center networks.

Printed 2022-10-27

Firewalling and load balancing inside virtual data center

IBM Cloud® managed VMware as a Service (VMWaaS) delivers a VMware Cloud Director platform running on dedicated IBM Cloud® Bare Metal Servers. You can deploy one or more secure and isolated virtual data centers through the VMware Console with embedded flexible networking services using either cost effective common edge nodes or dedicated edge nodes for higher bandwidth needs. Optionally, you can also share networks between virtual data centers.



1. Dedicated external network (Tier 0 VRF) provide you routing to private or to public networks. Connectivity is provided through private and public gateways. IBM Cloud provides you the public IPs dedicated for each virtual data center.
2. Edge gateways (Tier 1) provide policy based IPsec VPN tunnels to provide secure routed (L3) connectivity to on-premises networks. L2VPN tunnel provide a way to stretch (L2) your on-premises networks to cloud.
3. Edge gateways provide embedded stateful firewall (FW) services and network address translation (NAT) capabilities. You can enable non-distributed routing for virtual data center networks to isolate and control east-west traffic between networks attached to the same edge gateway.
4. For load balancing services use BYO appliance or use NSX Advanced Load Balancer (future) attached to a network routed through edge gateway.
5. Distributed firewall service is only supported for data center groups. You can create and modify additional distributed firewall rules.

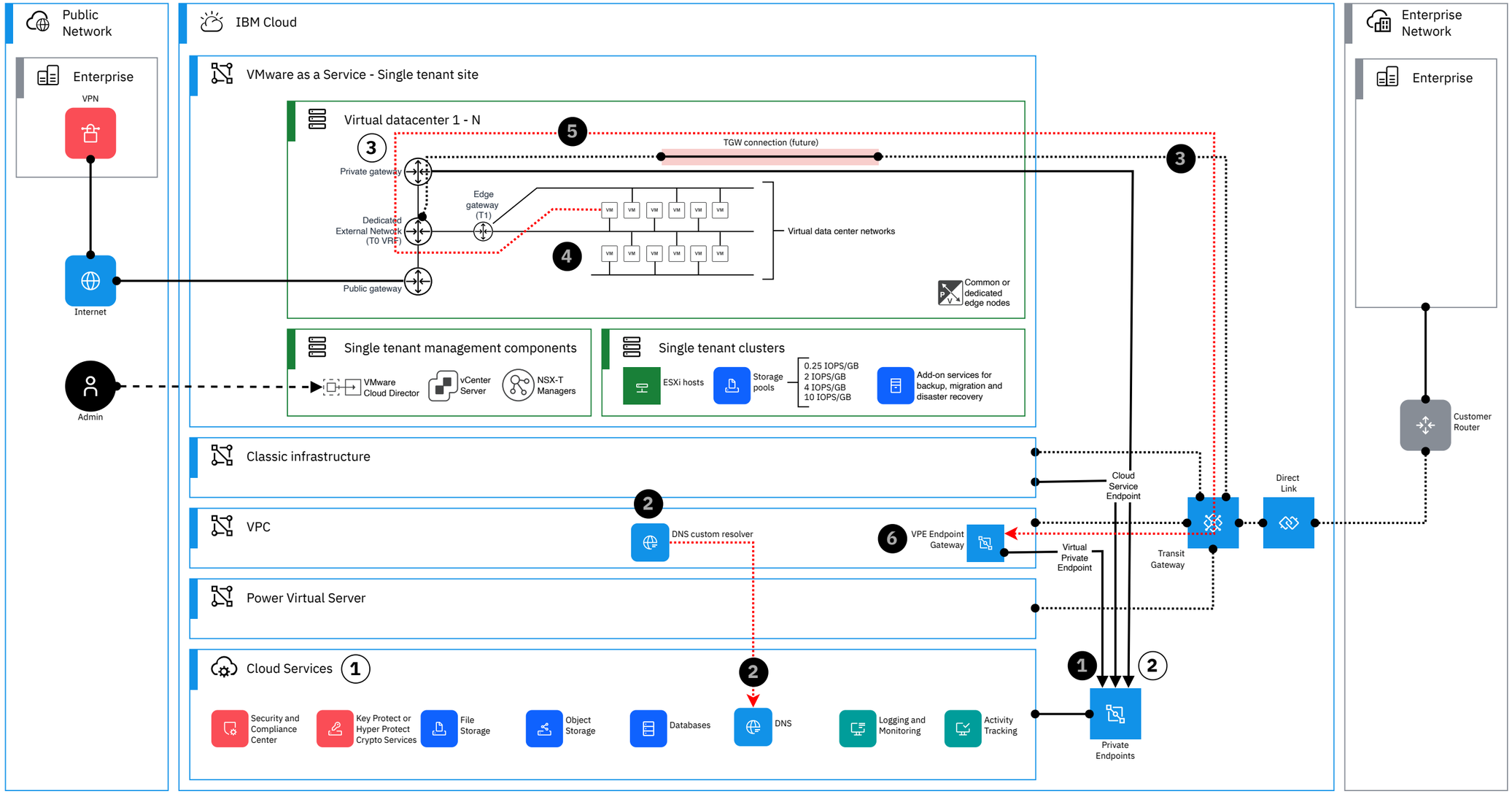
1. You can deploy your own 3rd party firewall into your virtual data center. Deploy the firewall using ova/ovf as a normal virtual machine with the vendor specifications. Obtain a license from the vendor.
2. Deploy the virtual machine with multiple vnics, one for each network segment. Note the needs for clustering, check your vendor specifications for more details.
3. Attach the firewall to a routed virtual data center network and configure static routes accordingly. You can configure public IP addresses for the appliance, contact support to obtain a routed public subnet.
4. Deploy isolated virtual data center networks for your workloads and attach these networks to the firewall. Use the firewall's IP address as the default gateway for your workloads.

1. You can use data center groups to provide shared network connectivity for multiple virtual data centers. Use data center group networks for shared networks across virtual data centers.
2. You can deploy a 3rd party firewall on the main virtual data center. Follow the vendor steps for deploying the appliance, specifications and licensing. Deploy the virtual machine with multiple vnics, one for each network segment. Attach the public side to a routed network.
3. Deploy isolated data center group networks for your workloads and attach networks to the firewall. Use the firewall's IP address as the default gateway for your workloads.
4. Distributed firewall service is supported for data center groups as an additional protection. You can create and modify additional distributed firewall rules.

Printed 2022-10-27

Accessing IBM Cloud Services from virtual data center

IBM Cloud® managed VMware as a Service (VMWaaS) delivers a VMware Cloud Director platform running on dedicated IBM Cloud® Bare Metal Servers. You can deploy one or more secure and isolated virtual data centers through the VMware Console. You can access IBM Cloud Services though Cloud Service Endpoints (CSE) using IBM Cloud allocated addresses or (future) using Virtual Private Endpoints (VPE) deployed on your own IP address space through VPC.



1. Provision an IBM Cloud Service though IBM Cloud Portal, CLI or terraform. Preferably select the region where your VMware as a Service Single tenant site is deployed.
2. You can access IBM Cloud Services from your virtual data center using private Cloud Services Endpoints (CSE). CSEs are addressed from private block 166.8.0.0/14. Each service provides private FQDNs, which is resolvable by IBM Cloud private DNS servers 161.26.0.10 and 161.26.0.11.
3. Access to CSE is provided though the private gateways using source NAT.

1. An alternative path (future) to access IBM Cloud Services is to use Virtual Private Endpoints (VPE). A VPE Gateway is provisioned on a subnet on your VPC. Each IBM Cloud Service provides its own FQDN to the service, and FQDN resolvable only inside your VPC.
2. IBM Cloud DNS Services provides a private DNS service for your VPC. The service provides an option to deploy custom resolvers in your VPC subnets with your IP addresses. These custom resolvers are reachable though optional IBM Cloud Interconnectivity Services, like Transit Gateway or Direct Link.
3. To get access to the VPC where DNS custom resolver and the VPE endpoints are provisioned, connect your virtual data center to the Transit Gateway.

4. Configure your gateway, networks and your workloads in the virtual data center to use the IP addresses of the custom resolvers as the DNS servers, You can also use forwarding rules here to point to the required domains for the services.
5. When you have L3 connectivity to the VPC, you can resolve the names and access your IBM Cloud Service endpoint from the virtual data center.
6. You can control access to the VPE using Security Groups and Access Control Lists on the VPC.