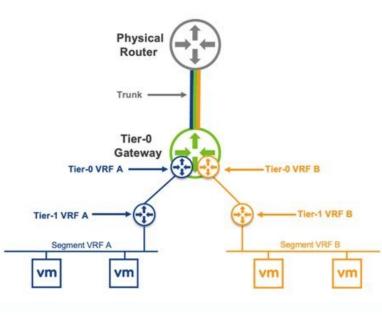
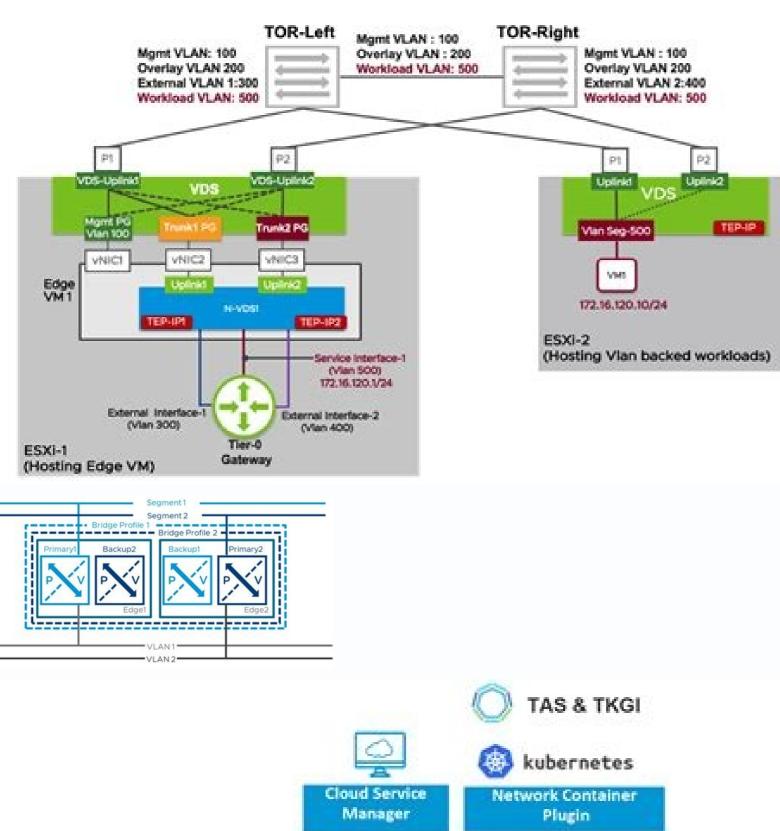
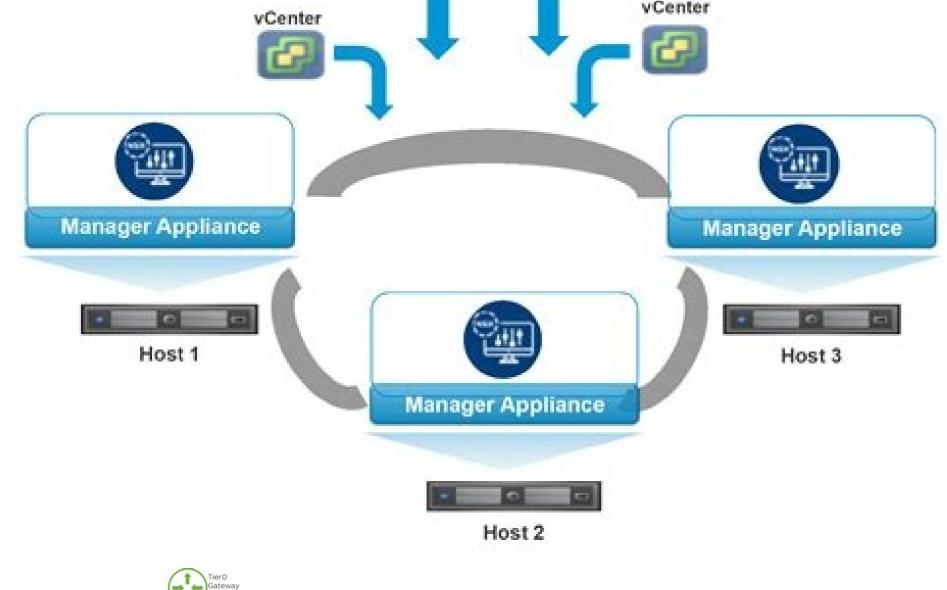
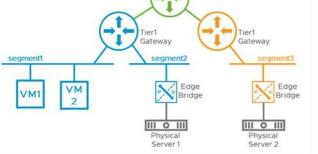
Vmware nsx- t reference design guide. pdf











Vmware nsx-t reference design guide. Vmware nsx-t multi-locations reference design guide. Vmware nsx-t reference design guide 2.5. Vmware nsx-t reference design guide.pdf.

This document provides guidance and best practices for designing environments that leverage the capabilities of VMware NSX-T as a full stack solution, providing a detail functioning of NSX-T components, features and functionality utilized at virtualization and network architectural building blocks of NSX-T as a full stack solutions, features and functionality utilized at virtualization and network architectural building blocks of NSX-T as a full stack solution, providing a detail functionality utilized at virtualization and network architectural building blocks of NSX-T as a full stack solution, provide feedback This document is organized into several chapters. Chapter 2 to 6 explain the architectural building blocks of NSX-T components, features and functionality utilized at virtualization and network architectural building blocks of NSX-T as a full stack solution, provide feedback This document is organized into several chapters. In socument provides guidance and best practices to resigning environments had reversage the capabilities of VMare NSA-1 or moment and provide resonance and best practices or leading environments and reversage the capabilities of VMare NSA-1 or moment and provide resonance. This defail functionary difference and best practices or leading resonance. The design quidance for a variety of a function and the provide resonance and the provide resonance and the provide resonance. This defail function and variably size and solutions of either start the provide resonance and best practices or leading resonance. This defail function and practices or leading resonance and a resonance and previous practices or leading for NSA-1 components and resonance and previous practices or leading resonance. The design quidance for a variety of a function and variably size and solutions of either start the previous excess of network wirth transformations and capabilities diversage and provide resonance. This defail function and variably size and solutions of either start the previous excess of network wirth and a diministration and administration and administ Relation of the relation of th This charge is a set of this experiment of the set of t The box virtual switch in this document with the base problem to the base with base and base behavior is specific to the VMware virtual switch model, not to NSX. A ransport zone and multiple VLAN transport zone and multiple NSX virtual switch to a single vorlay transport zone. A transport node can have multiple NSX virtual switch to a single vorlay transport zone. A transport node can have multiple VLAN transport zone and multiple VLAN transport zone. A transport node can have multiple NSX virtual switch on a given transport node. In other words, two NSX virtual switch on a given transport zone. C if multiple VLAN transport zone and the vorlay transport zone. C if multiple VLAN transport zone and the uplinks of the NSX virtual switch are logical constructs that can be mapped to one or multiple pNICs illustrates the difference between an uplink and a pNIC: Figure 3-2: N-VDS Uplinks vs. Hypervisor pNICs In this example, a single virtual switch with two uplinks is defined on the hypervisor pNICs illustrates the difference between an uplink and a pNIC: Figure 3-2: N-VDS Uplinks vs. Hypervisor pNICs In this example, a single virtual switch with two uplinks is defined on the hypervisor pNICs illustrates the difference between an uplink and a pNIC: Figure 3-2: N-VDS Uplinks vs. Hypervisor pNICs In this example, a single virtual switch with two uplinks is defined on the hypervisor pNICs illustrates the difference between an uplink and a pNIC: Figure 3-2: N-VDS Uplinks vs. Hypervisor pNICs illustrates the difference between an uplink and a pNIC: Figure 3-2: N-VDS Uplinks vs. Hypervisor pNICs illustrates the difference between an uplink and a pNIC: Figure 3-2: N-VDS Uplinks vs. Hypervisor pNICs illustrates the difference between an uplink and a pNIC: Figure 3-2: N-VDS Uplinks vs. Hypervisor pNICs illustrates the difference between an uplink and a pNIC: Figure 3-2: N-VDS Uplinks vs. Hyp transport node. One of the uplinks is a LAG, bundling physical port p1 and p2, while the other uplink is only backed by a single physical port p3. Both uplinks is a LAG, bundling physical port p3. Both uplinks is a LAG, bundling physical port p3. Both uplinks is and the host physical uplinks. 3.1.3 Teaming Policy defines how the NSX virtual switch; there is no functional difference between the virtual subscience there were virtual interface to an uplink of the host. Traffic is distributed across the policy of the virtual switch; there is no functional difference between virtual interface sould be printed to difference between virtual interface sould be printed to difference between virtual interface sonthat can source terming policy o uplinks of the virtual switch could be any combination of single pNICs or LAGs; whether the uplinks are pNICs or LAGs has no impact on the way traffic is balanced between uplinks. When an uplink is a LAG, it is only considered down when all the physical members of the LAG are down. When an uplink is a LAG, it is only considered down when all the physical members of the uplinks are pNICs or LAGs has no impact on the way traffic is balanced between uplinks. When an uplink is a LAG, it is only considered down when all the physical members of the uplinks are pNICs or LAGs has no impact on the way traffic is balanced between uplinks. When an uplink is a LAG, it is only considered down when all the physical members of the uplinks are pNICs or LAGs has no impact on the way traffic is balanced between uplinks. the function of the sequence o LAG and only support the failover order default teaming policies are not available for KVM. A LAG must be configured for more than one physical uplink to be active on an N-VDS on a KVM hypervisor. 3.1.4 Uplink Profile As mentioned earlier, a transport node includes at least one NSX virtual switch, implementing the NSX data plane. It is common for multiple transport nodes to share the exact same NSX virtual switch, implementing the NSX data plane. It is common for multiple transport nodes to share the exact same NSX virtual switch, implementing the NSX data plane. It is common for multiple transport nodes to share the exact same NSX virtual switch, implementing the NSX data plane. It is common for multiple transport nodes to share the exact same NSX virtual switch configuration. It is also very difficult from an operational standpoint to configure (and maintain) multiple parameters consistently are consistently The control of the solution of fall back to the lowest common denominator failover order teaming policy for all the hosts. The uplink profile are now directly definition and the MTU fields of the uplink profile are now directly definition, reallocation of VLANs based on topology or geo-location change. When running NSX on VDS, the LAG definition and the MTU fields of the uplink profile are now directly defined on the VDS, controlled by vCenter. It is still possible to associate transport vLANs based on topology or geo-location change. The towest common derivers of the to Network Function Virtualization, where the workloads typically perform networking functions with very demanding requirements in term of latency and packet rate. In order to accommodate this use case, the Enhanced Data Path virtual switch are entry becifics of this virtual switch are outside the scope of this document. The important points to remember regarding this switch are: It can only be instantiated on an ESXi hypervisor. Its uses case, the Enhanced Data Path virtual switch are outside the scope of this document. The important points to remember regarding this switch are: It can only be instantiated on an ESXi hypervisor. Its uses case, the Enhanced Data Path virtual switch are: It can only be instantiated on an ESXi hypervisor. Its uses case is very specific to NFV. The two kinding requirements in term of latency and packet rate. Network Function Virtualization, where the workloads typically perform networking functions with very demanding requirements in term of latency and packet in cocasis of this virtual switch are outside this secase, the Enhanced Data Path virtual switch are outside this secase, the Enhanced Data Path virtual switch are outside the scope of this during function. In the importance 1.2 and only the instantiation of a function of virtual switch are outside the scope of this during function. In the importance 1.2 and only the instantiation of the same hypervisor. It's use case, the Enhanced Data Path virtual switch are outside the scope of this during function. The specific of this virtual switch are outside the scope of this during function. The specific of this virtual switch are outside the scope of this during function. The physical L2 network infrastructure is one of the main benefits of adopting NSX-T. 3.2.1 Overlay Backet Processing Performance 4.1 and Physical View presents logical and Physical view on sists of five virtual switch are attached to the same type and ecoses. For the function of the diagram, the logical view consists of five virtual switch are attached to the same type and ecoses. The the function of the diagram, the logical and Physical L2 network infrastructure is one of the main benefits of adopting network views of a logical switching forume each segment. Figure 3-8: Overlay Networking – Logical and Physical representation, at the bottom, shows that the five virtual switch are attached to the same type and ecoses of the virtual switch are attached to the same type and ecoses. The the function of the diagram, the logical view on sists of five virtual switch are attached to the same type and ecoses. The the function of the diagram, the logical view on sists of five virtual switch are attached to the same type and ecoses. The the function of the diagram, the logical view on sists of five virtual switch are attached to the same type and ecoses. The the function of the diagram, the logical view on Controller advertised the TEPs of those remote interested transport nodes, so "HV1" will send a tunneled copy of the frame to each of them. Figure 3-9: Head-end Replication Mode The diagram illustrates the flooding process from the hypervisor transport nodes, so "HV1" will send a tunneled copy of the frame to each of them. Figure 3-9: Head-end Replication Mode The diagram illustrates the flooding process from the hypervisor transport nodes a copy of the frame to each of them. Figure 3-9: Head-end Replication Mode The diagram illustrates the flooding process from the hypervisor transport nodes a copy of the frame to each of them. Figure 3-9: Head-end Replication Mode The diagram illustrates the flooding process from the hypervisor transport nodes a copy of the frame to each of them. Figure 3-9: Head-end Replication Mode The diagram illustrates the flooding process from the hypervisor transport nodes a copy of the frame to each of them. the frame to each remote transport node in the same subnet 30.0.0.0. In this example, the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups - subnet 20.0.0.0 and subnet 30.0.0.0 - "HV1" sends a copy of the frame to each of the remote groups a line function for the function of the functi also that this benefit in term of traffic optimization provided by the two-tier hierarchical replication mode is recommended as a best practice as it typically performs better in terms of physical uplink bandwidth utilization. 3.2.3 Unicast Traffic When a frame is destined to a unicast MAC address table, it is fooded in the network. Switched by the switch to the corresponding ort. The NSX virtual switch maintains such a table for each segment/logical switch it is attached by the switch to the corresponding ort. The NSX virtual switch maintains such a table, it is only forward by the switch on the NAC address table, it is only f network, all the known MAC addresses are either local or directly reachable through a point-to-point tunnel. In NSX-T, the MAC address tables can be populated by the NSX-T Controller or by learning from the data plane. 3.2.4 Data Plane Learning is a matter of associating the source MAC addresses of frames received with the ports where they were received. In the overlay model, instead of a port, MAC addresses reachable through a tunnel are associated with the TEPs for the remote end of this tunnel. Data plane learning is a matter of associating the source TEPs. It is jongent and the source TEPs. It is possible that folded traffic gets registed to evel the refice as a post. The traffic gets registed that plane learning is a matter of associating the source TEP address of the received tunnel are associated with the traffic. Figure 3-10: Two the traffic register registed to evel the refice as a source to evel the folded traffic form HV1 to HV4, it is actually decapsulating the original tunnel traffic or the source TEP address as a source. Figure 3-12: Data Plane Learning using the source TEP address as a source. Figure 3-12: Data Plane tearning is that the source TEP address as a source. Figure 3-12: Data Plane tearning the original tunnel traffic form HV1 to HV4, it is actually decapsulating the origin of the tunnel source TEP as NSX-T metadata in the tunnel source TEP as NSX-T metadata in the tunnel source TEP as NSX-T metadata in the tunnel source TEP as NSX-T metadata. header. Metadata is a piece of information, "HV4" can correctly identifying "TEP1" as the origin. Figure 3-13: Data Plane Learning Leveraging Metadata With this additional piece of information, "HV4" can correctly identifying "TEP1" as the origin. Figure 3-13: Data Plane Learning Leveraging Metadata With this additional piece of information, "HV4" can correctly identify the origin of the tunneled traffic on replicated traffic. 3.2.5 Tables Maintained by the NSX-T controller While since a segment/logical switch from the data plane just like traditional piece of information, "HV4" can correctly identify the origin of the tunneled traffic on replicated traffic. 3.2.5 Tables Maintained by the NSX-T controller While NSX-T controller While NSX-T controller while since a segment/logical switch from the data plane just like traditional physical networking devices, the NSX-T Controller is also building a central repository for some tables include: Global ARP table, associating MAC address to TEP tables when the vNIC of a VM is attached to a segment/logical switch, the NSX-T Controller is notified of the MAC address to TEP tables when the vNIC of a VM is attached to a segment/logical switch, the NSX-T controller is notified of the MAC address to TEP tables when the vNIC of a VM is attached to a segment/logical switch, the NSX-T controller is notified of the MAC address to TEP tables when the vNIC ontroller has a global view of all MAC address table can proactively populate the local MAC address table can proactively populate the local MAC address table of the NSX-T controller while simultaneously while the simultaneously while the simultaneously while the simultaneously while the local MAC address in the global table of the NSX-T controller while simultaneously while tables of the NSX-T controller while simultaneously while the local MAC address table of the NSX-T controller while simultaneously while tables flooding the frame. Not all the MAC addresses are not pushed to the NSX-T Controller. Similarly, the NSX-T Controller is not notified of MAC addresses learned from an injection of an arbitrarily large number of MAC addresses are not pushed to the NSX-T Controller. Similarly, the NSX-T Controller is not notified of MAC addresses are not pushed to the NSX-T Controller. Similarly, the NSX-T Controller is not notified of MAC addresses learned from an injection of an arbitrarily large number of MAC addresses are not pushed to the NSX-T Controller. into in the network. 3.2.5.2 ARP Tables The NSX-T Controller also maintains an APP table in order to help implement an APP suppression. Figure 3-14: ARP Sup This capacity of support on the physical infrastructure. For example, the data plane existing bits in the VXLAN header or making a revision to the VXLAN header Identifying the TEP that sourced a tunnel packet • A version bit used during the intermediate state of an upgrade • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating whether the encapsulated frame is to be traced • A bit indicating Index of the state some connectivity is required between VMs and physical devices. For this functionality, NSX-T introduces the NSX-T Bridge, a service that can be instantiated on an Edge for the purpose of connectivity between the international VLAN at layer 2. The most common use cases for this feature are: Physical to virtual/virtual to virtual migration. This is generally a temporary scenario where a VLAN backed environment is being virtualized to an overlay backed NSX data center. The NSX-T Edge Bridge is a simple way to maintain connectivity between the inferent components of the international virtual virtual to virtual or virtual to virtual migration. This is generally a temporary scenario where a VLAN backed environment is being virtualized to an overlay backed NSX data center. The NSX-T Edge Bridge is a simple way to maintain connectivity between the inferent components of the international virtual bridged topologies. 3.3.1 Overview of the Capabilities The following sections present the capabilities of the MSX-T Edge is the data plane performance. 3.3.1.1 DPDK-based performance. Indeed, the NSX-T Edge is the data plane performance. Indeed, the NSX-T Edge is the data plane performance. 3.3.1.1 DPDK-based performance. Indeed, the NSX-T Edge is the data plane perfore Edge Bridge achieves is to convert an Ethore in the overlay in a single location, thus preventing is written by the overlay in a single location, thus preventing is written by the overlay in a single location, thus preventing is written by the overlay in a single location, thus preventing is written by the overlay in a single location, thus preventing to be an intervent of the overlay in a single location, thus preventing to be an intervent of the overlay in a single location, thus preventing to be an intervent of the overlay in a single location, thus preventing to be an intervent of the overlay in a single location, thus preventing to be an intervent of the overlay in a single location, thus preventing to be an intervent of the overlay in a single location, thus preventing to be an intervent of the overlay in a single location, thus preventing to be an intervent of the overlay in a single location, thus preventing to be an intervent of the overlay in a single location, thus preventing the possibility of a loop between a VLAN ID. Figure 3-18: One-to-one association between segment can be attached to several bridges on different Edges. This allows certain bare metal topologies to be connected with overlay segment and bridging to VLANs that can exist in separate rack without depending on physical overlay. With NSX-T 2.5, the same segment and bridging to VLANs that can exist in separate rack without depending on physical overlay. With NSX-T 3.0, the Edge Bridge supports bridging 802.1Q tagged traffic carried in an overlay backed segment (Guest VLAN Tagging.) For more information about this feature, see the bridging white paper at: 3.3.1.3 with Bridge and the overlay segment and bridging to VLANs the can exist in separate rack without depending on physical overlay. With Bridge and the overlay segment and bridging to VLANs the can exist in separate rack without depending on physical overlay. With Bridge and the overlay segment and bridging to VLANs the can exist in separate rack without depending on physical overla as an active/standby service. The Edge bridge active in the data path is backed by a unique, pre-determined standby bridge on a different Edge. NSX-T Edges are deployed in a pool called an Edge Cluster, within an Edge Cluster, the user can create a Bridge Profile, which essentially desi ates two Edges as the potential hosts for a pair of redundant Bridges. The Bridge Profile specifies which Edge would be primary (i.e. the preferred host for the active Bridge) and backup (the Edge that will host the backup Bridge). At the time of the creation plate for the creation of one or several Bridge pairs. Figure 3-19: Bridge Profile, defining a redundant Edge Bridge (primary and backup) Once a Bridge Endp oint object, which represents this pair of Bridges. The attachment of the se of the Bridge Profile, no Bridge is instantiated yet. The Bridge Profile is just a ter

presented by a dedicated Logical Port, as shown in the diagram below: Figure 3-20: Primary Edge Bridge forwarding traffic between segment and VLAN traffic as well as the physical port that will be used on the Eridge forwarding traffic between segment to a Bridge Profile, the user can also select the failover mode. In the preemptive mode, the Bridge on the Eridge Profile, the user can also select the failover mode. In the preemptive mode, the Bridge on the primary Edge will always become the active bridge forwarding traffic between segment and VLAN traffic. At the time of the creation of the Bridge Profile, the user can also select the failover mode. In the preemptive mode, the Bridge on the primary Edge will always become the active bridge forwarding traffic between segment and VLAN traffic. At the time of the creation of the Bridge Profile, the user can also select the failover mode. In the preemptive mode, the Bridge Profile, the user can also select the failover mode. In the preemptive mode, the Bridge on the primary Edge will always become the active bridge forwarding traffic between segment and VLAN traffic. At the time of the creation of the Bridge Profile, the user can also select the failover mode. In the preemptive mode, the Bridge Profile, the user can also select the failover mode. In the preemptive mode, the Bridge Profile, the user can also select the failover mode. In the preemptive mode, the Bridge Profile, the user can also select the failover mode. In the preemptive mode, the Bridge Profile, the user can also select the failover mode. In the preemptive mode, the Bridge Profile, the user can also select the failover mode. In the preemptive mode, the Bridge Profile, the user can also select the traffic between segment and the preemptive mode. In the preemptive mode, the bridge where no verify and VLAN as soon as it is available, usuring a segment via a Bridge is subject to the Bridge on the backup Edge will remain standby should it become available when the Bridge as whole, i.e. they apply to the active Bridge instance, irrespective of the Edge on which it is running as segment via a Bridge is a whole, i.e. they apply to the active Bridge instance, irrespective of the Edge on which it is running as segment via a Bridge is a whole, i.e. they apply to the active Bridge instance, irrespective of the Edge on which it is running as segment via a Bridge is a whole, i.e. they apply to the active Bridge instance, irrespective of the Edge on which it is running as segment via a Bridge is subject to the Bridge and entering as segment via a Bridge is subject to the Bridge and entering as segment via a Bridge is subject to the Bridge and the backup Edge is already active. 3.3.1.5 Edge Bridge Firewall The traffic leaving and entering as segments as a whole, i.e. they apply to the active Bridge instance, irrespective of the Edge on which it is running as a segment via a Bridge is subject to the Bridge and the backup Edge is already active. 3.3.1.5 Edge Bridge Firewall The traffic leaving and entering as segments extended to VLAN by a Bridge. The following diagram is a logical representation with NSX-T gateways. Routing is available to segments extended to VLAN by a Bridge. The following diagram is a logical representation with NSX-T gateways. Routing is available to segments extended to VLAN by a Bridge. The following diagram is a logical representation with NSX-T gateways. Routing is available to via a Bridge integration with NSX-T gateways. Routing is available to via a Bridge integration with NSX-T gateways. Routing is available to via a Bridge integration with NSX-T gateways. Routing is available to via a Bridge integration with NSX-T gateways. Routing is available to via a Bridge integration with NSX-T gateways. Routing is available to via a Bridge integration with NSX-T gateways. Routing is ARP requests from physical workload for the IP address of an NSX router acting as a default gateway will be answered by the local ble configuration leveraging T0 and T1 gateways along with Edge Bridges. Figure 3-22: Integration with routing In this above example, VM /M2, Physical Servers 1 and 2 have IP connectivity. Remarkably, through the Edge Bridges, Tier-1 or Tier-0 gateways can act as default gateways for physical devices. Note also that the distributed nature of NSX-T routing is not affected by the introduction of an Edge Bridge in the previous chapter showed how to create segments; this chapter focuses on how gateways provide connectivity between different logical L2 networks. Figure 4-1: Logical and Physical View of Routing Services showed how to create segments; this chapter focuses on how gateways provide connectivity between different logical L2 networks. Figure 4-1: Logical and Physical View of a route topolo s categorized as East-West (E-W) or North-South (N-S) based on the origin and destination of the flow. When virtual or physical workloads in a data center communicate with the devices external to the data center (e.g., WAN, Internet), the traffic is referred to as North-South ors. Virtual machines "Web1" and "Web2" are c nected to "overlay Segment 1" while ' App1" and "App2" are connected to "overlay Segment 2". Figure 4-1: Logical and Physical View of Routing Se een workloads confined within the data center is referred to as East-West traffic. In modern data centers, more than 70% of the traffic is East-We For a multi-tiered application where the web tier needs to talk to the app tier and the app reactive to talk to the database tier and, these different sit in different sit in different source routing decision is made, the packet is sent to a physical router. Traditionally, a centralized router for a routing decision is made, the packet is sent to a physical router for a routing decision is made, the packet is sent to a physical router. Traditionally, a centralized router for a routing decision, then return to the same hypervisor; this is not optimal. NSX-T is uniquely positioned to solve these different tiers. With VMs that are hosted on same the ESXi or KVM hypervisor; this is not optimal. NSX-T is uniquely positioned to solve the sentralized router for a routing decision is made, the packet is sent to a physical router. Traditionally, a centralized router for a routing decision is made, the packet is sent to a physical router. Traditionally, a centralized router for a routing decision is made, the packet is sent to a physical router for a routing decision is made, the packet is sent to a physical router. Traditionally, a centralized router for a routing decision is made, the packet is sent to a physical router. Traditionally, a centralized router for a routing decision is made, the packet is sent to a physical router for a routing decision is made, the packet is sent to a physical router. Traditionally, a centralized router for a routing decision is made, the packet is sent to a physical router. Traditionally, a centralized router for a routing decision is made, the packet is sent to a physical router. Traditionally, a centralized router for a routing decision is made, the packet is sent to a physical router. Traditionally, a centralized router for a routing decision is made, the packet is sent to a physical router. Traditionally, a centralized router for a routing decision is made. ring a Gateway via NSX-T Manager instantiates a local distributed gateway on each hypervisor. For the VMs hosted (e.g., "Web 1", "Ap 1") on the same hypervisor, the E-W traffic does not need to leave the hypervisor for routing. 4.1 Single Tier Routing NSX-T Gateway provides optimized distributed routing and is also connected to a single tier routing component (DR) and centralized services routing component (DR) ADR is essentially a router with logical interfaces (LIFs) connected to multiple subnets. It runs as a kernel module and is distributed in hypervisors across all transport nodes, including Edge nodes. The traditional data plane functionality of routing and APP lookups is performed by the logical interfaces (LIFs) connected to multiple subnets. It runs as a kernel module and is distributed in hypervisors across all transport nodes, including Edge nodes. The traditional data plane functionality of routing and APP lookups is performed by the logical interfaces (LIFs) connected to multiple subnets. It runs as a kernel module and is distributed in hypervisors across all transport nodes, including Edge nodes. The traditional data plane functionality of routing and APP lookups is performed by the logical interfaces (LIFs) connected to multiple subnets. It runs as a kernel module and is distributed in hypervisors across all transport nodes. to provide of House a barrent with logical to the same everywhere the segment. The IP address is unique per LIF and remains the same during with Workloads on the Same Hypervisor, allowing the default pervisor shows a logical topology with two segments. The VMAC addresses to remain the same during with we be set to the default pervisor shows a logical topology with two segments. The VMAC addresses to remain the same during with we be set to the default pervisor shows a logical topology with two segments. The VMAC addresses to remain the same during with we be set to the default pervisor shows a logical topology with two segments. The VMAC addresses to remain the same during with we be segment with a default vertex of the component with a default vertex of the component with a default be segment. The left side of Figure 4.2. E-W Routing with Workloads on the Same Hypervisor, allowing the default side of Figure 4.2. E-W Routing with Workloads and the Same Hypervisor shows a logical topology with two segments. We be Segment with a default be segment. The left side of Figure 4.2. E-W Routing with Workloads on the Same Hypervisor shows a logical topology with two segments. We be segment with a default be segment with a default be segment with a default be segment. pens on the DR located on that same hypervisor. Figure 4-3: Packet Flow between two VMs on Same Hypervisor presents the logical packet flow between two VMs on the same hyper F2". A lookup is performed in the "LIF2" ARP table to determine the MAC address associated with the IP address for "App1". If the ARP entry does not exist, the controller is queried. ered to the App1 VM. The return packet from "App1" follows the same process and routing would happen again on the local DR. In this example, neither the initial packet from "Web1" to "App1" to "Web1" to "App1" in the return packet from "App1" to "Web1" to "App1" to "App ed to learn the MAC address of "App1". Once the MAC address of "App1" is learned, the L2 lookup is perfo rent Hypervisor In th get workload "App2" differs as it rests on a hypervisors shows a light of a byte DR on "HV2". If "Web1" needs to communicate with "App2", the traffic would have to leave the hypervisors. Figure 4-4: E-W Packet Flow between two Hypervisors shows a logical view of topology, highlighting the routing decisions taken by the DR on "HV2". When "Web1" sends traffic to "App2", to uting is done by the DR on "HV1". The reverse traffic from "App2", the traffic would have to leave the hypervisors. Figure 4-4: E-W Packet Flow between two Hypervisors shows a logical view of topology, highlighting the routing decisions taken by the DR on "HV1". The reverse traffic from "App2", the traffic would have to leave the hypervisors. Figure 4-4: E-W Packet Flow between two Hypervisors shows a logical view of topology, highlighting the routing decisions taken by the DR on "HV1". The reverse traffic from "App2", the traffic would have to leave the hypervisors. Figure 4-4: E-W Packet Flow between two Hypervisors shows a logical view of topology, highlighting the routing decisions taken by the DR on "HV1". The reverse traffic from "App2", to uting is done by the DR on "HV1". The reverse traffic from "App2", to uting is done by the DR on "HV1". The reverse traffic from "App2", to uting is done by the DR on "HV1". The reverse traffic from "App2", to uting is done by the DR on "HV1". The reverse traffic from "App2", to uting is done by the DR on "HV1". The reverse traffic from "App2", to uting is done by the DR on "HV1". The reverse traffic from "App2", to uting is done by the DR on "HV1". The reverse traffic from "App2", to uting is done by the DR on "HV1". The reverse traffic from "App2", to uting is done by the DR on "HV1". The reverse traffic from "App2", to uting is done by the DR on "HV1". The reverse traffic from "App2", to uting is done by the DR on "HV1". The reverse traffic from "App2", to uting is done by the DR on "HV1". The reverse traffic from "App2", to uting is done by the DR on "HV1". The reverse traffic from "App2", to uting visors shows a logical view of topology, highlighting the routing decisions taken by the DR on "HV1" and the DR on "HV2". When "Web1" sends traffic to "App2", routing is done by the DR on "HV1". The reverse traffic from "App2" to "Web1" is routed by DR on "HV2". "Web1" (172.16.10.11) sends a packet to "App2" (172.16.20.12). The packet is sent to the default gateway interface (172.16.10.1) for "Web1" located on the local DR. Its L2 header has the source MAC as "MAC1" and destination MAC as the vMAC of the DR. This vMAC will work identify (VNI) in the Geneve encapsulated packet belongs to "App Segment". HV2 TEP 20.20.20 decapsulates the packet, removing the outer header upon reception. It performs an L2 lookup in the local MAC table associated with "LIF2". Packet is delivered to "App2" VM. The return packet from "App2" destined for "Web1" goes through the same process. For the return traffic, the routing lookup happens on the HV2 DR. This represents the normal behavior of the DR, which is to always perform routing on the DR instance on the bypervisor hosting the workload that initiates the communication. After the routing lookup, the packet is encapsulated by the HV2 TEP and sent to the remote HV1 TEP. The HV1 decapsulates the Geneve packet and delivers the encapsulated frame from "App2" to "Web1". 4.1.2 Services Router East-West routing is completely distributed in the hypervisor, with each hypervisor, with each hypervisor, with each hypervisor in the transport zone running a DR in its kernel. However, some services of NSX-T are not distributed, due to its locality or stateful nature such as: Connectivity (BGP Routing with Address Families - VRF lite) At the contralized pool of capacity is required to run these services router (SR) is instantiated on an edge cluster when a service is enabled that cannot be distributed on a gateway. A centralized pool of capacity is required to run these services in a highly available and scaled-out fashion. The appliances where the centralized services or SR instances are hosted are called Edge nodes. An m "App2" to "Web1". 4.1.2 Service's Router East-West routing is completely distributed in the hypervisor, with each hypervisor in the transport zone running a DR in its kernel. However, ster when a service is enabled that cannot be distributed on a gateway. A centralized pool of capacity is required to run these services in a highly available and scaled-out fashion. The appli VPN ● Gateway Firewall ● Bridging ● Service Interface ● Metadata Pr rides connectivity to the physical infrastructure. Left side of Figure 4-6: Logical Router Components and Interconnection shows the logical view of a Tier-0 Gateway showing both DR and SR components on the right has both the SF Structure solution of the solu be to be tob Node From a physical topology perspective, workload hosted to pology perspective, workload hosted topology p the Edge node. The HV1 TEP encapsulates the original packet and sends it to the Edge node TEP with a source IP address of 10.10.10.10 and destination IP address of 30.30.30. The Edge node is also a transport node. It will encapsulate the traffic sent to or received from compute hypervisors. The Edge node is also a transport node. It will encapsulate the traffic sent to the SR. The SR performs a routing lookup and determines that the route 192.168.100.0/24 is learned via external interface with a next hop address of 30.30.30. The Edge node is also a transport node. It will encapsulate the traffic sent to or received from compute hypervisors. The Edge node is also a transport node. It will encapsulate the traffic sent to or received from compute hypervisors. The Edge node is also a transport node. It will encapsulate the traffic sent to or received from compute hypervisors. The Edge node is also a transport node. It will encapsulate the traffic sent to or received from compute hypervisors. The Edge node is also a transport node. It will encapsulate the traffic sent to or received from compute hypervisors. The Edge node is also a transport node. It will encapsulate the traffic sent to or received from compute hypervisors. The Edge node is also a transport node. It will encapsulate the traffic sent to or received from compute hypervisors. The Edge node is also a transport node. It will encapsulate the traffic sent to or received from compute hypervisors. The Edge node is also a transport node. It will encapsulate the traffic sent to or received from compute hypervisors. The Edge node is also a transport node. It will encapsulate the traffic sent to or received from compute hypervisors. The Edge node is also a transport node. It will encapsulate the traffic sent to or received from compute hypervisors. The Edge node is also a transport node. It will encapsulate the traffic sent to or received from transport node. It will encapsulate the traffic sent to transport node. It will encapsulate the traffic sent to traffic red. Figure 4-9: End-to-end Packet Flow – External to Application "Web1" follows the packet walk for the reverse traffic from an external device to "Web1". Fig A lookup is performed in the "LIF1" ARP table to determine the MAC address associated with the IP address for "Web1". This destination MAC "MAC1" is lear 2.168.100.10) sends a packet to "Web1" (172.16.10.11). The packet is routed by the physical router and sent to the external interface of Tier-0 Gateway hosted on Edge node. A single routing lookup happens on the Tier-0 Gateway SR while the that the packet must be sent to the SR. On the edge node, the packet is directly sent to the SR after the tunnel encaps node. A single routing lookup happens on the Tier-0 Gateway SR which determines that 172.16.10.0/24 is a directly conne note TEP "HV1" host where "Web1" is located. The Edge TEP encapsulates the original packet and sends it to the remote TEP with an outer packet source IP address of 30.30.30.30 and destination VNI in this Geneve encapsulates the packet is of "Web Segment". The HV1 host decapsulates the packet is of "Web Segment". T Bar of the second secon in the section, Northbound, it connects to a Tier-0 gateway sort directly to one or more segments as shown in North-South routing section. Northbound, the Tier-1 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, it connects to a Tier-0 gateway using a RouterLink port, Southbound, the Tier-0 ame for multi-the formation of the forma 1 gateway, an edge cluster must be configured on this gateway. When you configure a Tier 1 GW, it's when you configure a n Edge cluster that he Tier-1 GW will have an SR. Configuring an Edge cluster that the Tier-1 gateway does not automatically instantiate a Tier-0 service component (SR), the service control and the aces types along with a new "RouterLink" interface in a two-tiered topology. Figure 4-11: Anatomy of Components with Logical Routing and BGP are supported on this interface only exists on Tier-0 gateway. This interface in previous releases. This interface only exists on Tier-0 gateway. This interface in previous releases. This interface in previous releases. This interface only exists on Tier-0 gateway. This interface is previous releases. This interface is previous releases. This interface only exists on Tier-0 gateway. T er Link Interface/Linked Port: Interface connecting Tier-0 and Tier-1 gateways. Each Tier-0-to-Tier-1 peer connection is provided a /31 subnet within the 100.64.0.0/16 reserved address space (RFC6598). This link is created automatically when the Tier-0 and Tier-1 gateways are connection is provided a /31 subnet within the 100.64.0.0/16 reserved address space (RFC6598). This link is created automatically when the Tier-0 and Tier-1 gateways are connection is provided a /31 subnet within the 100.64.0.0/16 reserved address space (RFC6598). This link is created automatically when the Tier-0 and Tier-1 gateways are connection is provided a /31 subnet within the 100.64.0.0/16 reserved address space (RFC6598). This link is created automatically when the Tier-0 and Tier-1 gateways are connection is provided a /31 subnet within the 100.64.0.0/16 reserved address space (RFC6598). This link is created automatically when the Tier-0 and Tier-1 gateways are connecting VLAN segments to provide connecting VLAN segments to provide connecting VLAN segments to provide a /31 subnet within the 100.64.0.0/16 reserved address space (RFC6598). This link is created automatically when the Tier-0 and Tier-1 gateways are connecting VLAN segments to provide connecting VLAN segment to provide connecting VL ier-0 and Tier-1 gateways. • Tier-0 Gateway O Connected - Connected routes on Tier-0 include external interface subnets, service interface subnets, ateway supports the loopback interfaces. A Loopback interface is a virtual interface, and tic an be redistributed into a routing protocol. 4.2.2 Route Types on Tier-0 and Tier-1 gateways. The following list details route types on Tier-0 and Tier-1 gateways. Connected - Connected routes on Tier-0 include external interface subnets, service interface subnets, loopback and ected to Tier-0. In Figure 4-12: Routing Advertisement, 172.16.20.0/24 (Connected segment), 192.168.20.0/24 (Service Interface) and 192.168.240.0/24 (Service In DNS reries from clients. Also used as the source IP to forward DNS queries to the upstream DNS server. Orticement, 172.16.10.0/24 (Connected segment) and 192.168.10.0/24 (Service Interface) are connect Tier-1 Gateway O y virtual server. O LB SNAT - IP address or a range of IP addresses used for Source NAT by load balancer. O IP sec Local IP - Local IPsec endpoint IP addresses used for Source NAT by load balancer. O IP sec Local IP - Local IPsec endpoint IP addresses used for Source NAT by load balancer. O IP sec Local IP - Local IPsec endpoint IP addresses used for Source NAT by load balancer. O IP sec Local IP - Local IPsec endpoint IP addresses used for Source NAT by load balancer. O IP sec Local IP - Local IPsec endpoint IP addresses used for Source NAT by load balancer. O IP sec Local IP - Local IP sec endpoint IP addresses used for Source NAT by load balancer. O IP sec Local IP - Local IP sec endpoint IP addresses used for Source NAT by load balancer. O IP sec Local IP - Local IP sec endpoint IP addresses used for Source NAT by load balancer. O IP sec Local IP - Local IP sec endpoint IP addresses used for Source NAT by load balancer. O IP sec Local IP - Local IP sec endpoint IP addresses used for Source NAT by load balancer. O IP sec Local IP - Local IP sec endpoint IP addresses used for Source NAT by load balancer. O IP sec Local IP - Local IP sec endpoint IP addresses used for Source NAT by load balancer. O IP sec Local IP - Local IP sec endpoint IP addresses used for Source NAT by load balancer. O IP sec Local IP - Local IP sec endpoint IP addresses used for Source NAT by load balancer. O IP sec Local IP sec endpoint IP addresses used for Source NAT by load balancer. O IP sec Local IP sec endpoint Inter SR. SRs of a same Tier-0 gateway in the same edge cluster will create an automatic iBGP peering adjacency between them to exchange routing information. This topology is only supported with Active/Active topologies and with NSX-T Federation. • routes for Tier-1 gateway. • Static- User configured static routes on Tier-1 gateway. • NAT IP - NAT IP addresses owned by the Tier-1 gateway discovered from NAT rules configured on the Tier-1 gateway. • LB VIP - IP addresses of load balancing - IP address of load balancing virtual server. O DNS Forwarder IP - Listener IP for DNS queries from clients. Also used as the source IP to forward DNS queries to the upstream DNS server. Route Advertisement on the Tier-0 gateway could use static routing or BGP to connect to physical routers. The Tier-0 gateway could use static routers directly; it must connect to a Tier-0 gateway could use static routers directly; it must connect to a Tier-0 gateway could use static routers. ate of the Tier-1. That default route is pointing to the RouterLink IP address that is owned by the Tier-0. Figure 4-12: Routing Advertisement explains the route advertisement on both the Tier-1 Gateway. Figure 4-12: Routing Advertisement on both the Tier-1 Gateway. Figure 4-12: Routing Advertisement on both the Tier-1 and Tier-0 Gateway. Figure 4-12: Routing Advertisement explains the route advertisement explains the route advertisement on both the Tier-1 Gateway. have been by the formation of the format the distributed component (DR) for Tier-0 and the Tier-1 gateways have been instantiated on two hypervisors. Figure 4-13: Logical Routing Instances If "VM1" in tenant 1 needs to communicate with "VM3" in tenant 1 needs to communicate with "VM3" in tenant 1 needs to control to route of traffic to a centralized location to route between different tenants or environments. Multi-Tier Distributed Routing with Workloads on the same Hypervisor The following list provides a detailed packet walk between person the tenant 1 Tier-1 DR and the packet is routed to the Tier-0 DR following the default route. This default route has the RouterLink interface IP address (100.64.224.0/31) as a next in routing lookup has pens on the Tier-0 DR. It determine to reach "VM3" and the packet is sent. The reverse traffic from "VM3" follows the similar process. A packet from "VM3" to destination 172.16.10.11 is sent to the tenant-2 Tier-1 DR, then follows the default route to the Tier-0 DR. The Tier-0 DR routing to the tenant-2 Tier-1 DR, then follows the default route to the Tier-0 DR. The Tier-0 DR routing to the tenant 1.2 Tier-1 DR, then follows the default route to the Tier-0 DR. The Tier-0 DR routing to the tenant 1.2 Tier-1 DR, then follows the default route to the Tier-0 DR. The Tier-0 DR routing to the tenant 1.2 Tier-1 DR, then follows the default route to the Tier-0 DR. The Tier-0 DR routing to the tenant 1.2 Tier-1 DR, then follows the default route to the Tier-0 DR. The Tier-0 DR routing to the tenant 1.2 Tier-1 DR, the follows the default route to the Tier-0 DR. The Tier-0 DR routing to the tenant 1.2 Tier-1 DR the follows the default route to the Tier-0 DR. The Tier-0 DR routing to the tenant 1.2 Tier-1 DR the follows the default route to the Tier-0 DR. The Tier-0 DR routing to the tenant 1.2 Tier-1 DR the follows the default route to the Tier-0 DR routing to the tenant 1.2 Tier-1 DR tenant 1.2 Ti nants but hosted on the same hypervisor. "VM1" (172.16.10.11) in tenant 1 sends a packet to "VM3" (172.16.201.11) in tenant 2. The packet is sent to its default gateway interface located on tenant 1, the local Tier-1 DR. Routing lookup happens on the tenant 2 Tier-1 DR. This determines that the 172.16.201.0/24 subnet is directly connected. L2 lookup is performed in the local MAC table to determine how nes that the 172.16.201.0/24 subnet is red to "VM1". During this process, the packet never left the hypervisor to be routed between tenants. Multi-Tier Distributed Routing with Workloads on different Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing in different Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logical Routing End-to-end Packet Flow Between Hypervisors Figure 4-14: Logica (172.16.10.11) in tenant 1 sends a packet to "VM2" (172.16.200.11) in tenant 2. VM1 sends the packet to its default gateway interface located on the local Tier-1 DR in HV1. Routing lookup happens on the tenant 1 Tier-1 DR and the packet follows the default route to the Tier-0 DR with a next hop IP of 100.64.224.0/31, Routing lookup happens on the Tier-0 DR which determines that the 172.16.200.0/24 subnet is learned via the tenant 2 Tier-1 DR (100.64.224.3/31) and the packet is routed accordingly. Routing decapsulates the packet and recognize the VNI in the Geneve header. A L2 lookup is performed in the local MAC table associated to the LIF w ", where this packet is decapsulated and delivered to "VM1". It is important to notice that in this use case, routing is performed locally on the nant 2 Tier-1 DR which determines that the 172.16.200.0/24 subnet is a directly connected subnet. A lookup is performed in ARP table to determine the MAC address asso packet is delivered to "VM2". The return packet follows the same process. A packet from "VM2" gets routed to the local hypervisor Tier-1 DR and is sent to the Tier-0 DR. R. The Tier-0 DR routes this packet to tenant 1 Tier-1 DR which performs the L2 lookup to find out that the MAC associated with "VM1" is on remote hypervisor "HV1". The packet is encapsulated by "HV2" and sent to "HV1", we have the tenant to the "HV2". ociated to the LIF when visor hosting the VM sourcing the traffic. 4.3 Routing Capabilities NSX-T supports static routing and the dynamic routing protocols BGP on Tier-0 Gateways for IPv4 and IPv6 workloads. In addition to static routing and be protocols BGP on Tier-0 gateway also supports a dynamic and is available for active-active Tier-0 topologies only. Tier-0 gateway also supports a dynamic routing protocols. 4.3.1 Static Routing Northbound static routes (and bit in the first of the f the state of the s and interfaces with physical routers. BFD can also be enabled per BGP neighbor for faster failover. BFD timers depend on the Edge supports a minimum of 50ms TX/RX BFD keep alive timer with NSX-T 3.0 release, the following BGP features are supported: Two and four bytes AS numbers in asplain, asdot and asdot + format. BGP neighbors in same or different AS numbers. (Multi-path relax) BGP neighbors in same or different AS numbers. (Multi-path relax) BGP peer or advertise the summary route along with specific routes as mentioned in section 4.2.2. Inbound/outbound routes as mentioned in section 4.2.2. Inbound/outbound routes as mentioned in section 4.2.2. EVEN support. The BGP peer or advertise as the upstream route. BGP community support. Influencing BGP peer or advertise, no-export, no-export-subconfiel) can also be included in the BGP peer. BGP community support. BGP communities can be set in a route-map to facilitate matching of communities at the upstream route. BGP well-known community names (e.g., no-advertise, no-export, no-export-subconfiel) can also be included in the BGP peer of communities can be set in a route-map to facilitate matching of communities at the upstream route. BGP communities at the upstream route. BGP peer back in a route-map to facilitate matching of communities at the upstream route. BGP peer back in a route-map to facilitate matching of communities at the upstream route. BGP peer back in a route-map to facilitate matching of communities at the upstream route. BGP peer back in BGP peer back in a route-map to facilitate matching of communities at the upstream route. BGP peer back in the B ilder of the set of th By and destination IP address. Graceful restart (GR) Graceful restart in BGP speaker to preserves its forwarding table, marks the routes as stale, or active routing engine crash. As soon as a GR-enabled router restarts (control plane failure), it preserves its forwarding table, marks the routes as stale, or active routing engine crash. As soon as a GR-enabled router restarts (control plane failure), it preserves its forwarding table, marks the routes as stale, or active routing engine crash. As soon as a GR-enabled router restarts (control plane failure), it preserves its forwarding table, marks the routes as stale, or active routing engine crash. As soon as a GR-enabled router restarts (control plane failure), it preserves its forwarding table, marks the routes as stale, or active routing engine crash. As soon as a GR-enabled router restarts (control plane failure), it preserves its forwarding table, marks the routes as stale, or active routing engine crash. As soon as a GR-enabled router restarts (control plane failure), it preserves its forwarding table, marks the routes as stale, or active routing engine crash. As soon as a GR-enabled router restarts (control plane failure), it preserves its forwarding table, marks the routes as stale, or active routing engine crash. As soon as a GR-enabled router restarts (control plane failure), it preserves its forwarding table, marks the routes as stale, or active router flushes the stale routes. The BGP session reestablish within this grace period, the router flushes the stale routes. The BGP session both ends. GR can be enabled/disabled per Tier-0 gateway. The GR restart timer is 180 seconds by default and cannot be change after or active router flushes the stale routes. The BGP session hold control plane failed is updated on the change after or active router flushes the stale routes as the stale router flushes the stale routes as the stale router flushes the stale router flushes the stale router flushes the stale routes as the stale routes as the stale router flushes VRF Lite Generalities Virtual Routing Forwarding (VRF) is a virtualization method that consists of creating multiple logical routing instances within a physical routing instances. VRF instances are commonly used in enterprise and service providers networks to provide control plane isolation, allowing several use cases such as overlapping IP cency is in the established state, otherwise the peering needs to be negotiated again. 4.4 nants, isolation of regulated workload, isolation of external and internal workload as well as hardware resources consolidation. Starting with NSX-T 3.0 it is possible to extent the VRF present on the physical network onto the NSX-T domain. Creating a development environment is a typical use case for VRF. Another representative use case for VRF is when multiple environments needs to be isolated from each other. As stated previously. VRF instances are isolated between each other by default allowing communications between these levels of the DFW construct. Figure 4-16: Networking VRF architecture is possible. While this feature allowing routing of the DFW construct. Figure 4-16: Networking VRF architecture. Logical (Switch Virtual Interface e 1/2 and e2/2 belong to VRF-8. Each VRF will run their own dynamic routing provides connectivity to the physical interview as the delicated tenant while a shared Tier-0 grave grave for each tenant while a shared Tier-0 grave grave for each tenant while a shared Tier-0 grave grave for each tenant on a dedicated tenant edge node. Figure 4-18: NSX-T 2.x Multi-tenant Architecture - Dedicated Tier-0 grave grave for each tenant on a dedicated tenant edge node. Figure 4-18: NSX-T 2.x Multi-tenant Architecture - Dedicated Tier-0 for Each Tenant shows a traditional multi-tenant Architecture - Dedicated Tier-0 for Each Tenant shows a traditional multi-tenant Architecture - Dedicated Tier-0 for Each Tenant in NSX-T 2.x Multi-tenant Architecture - Dedicated Tier-0 for Each Tenant in NSX-T 2.x Multi-tenant Architecture - Dedicated Tier-0 for Each Tenant shows a traditional multi-tenant Architecture - Dedicated Tier-0 for Each Tenant in NSX-T 2.x Multi-tenant Architecture - Dedicated Tier-0 for Each Tenant in NSX-T 2.x Multi-tenant Architecture - Dedicated Tier-0 for Each Tenant in NSX-T 2.x Multi-tenant Architecture - Dedicated Tier-0 for Each Tenant shows a traditional multi-tenant Architecture - Dedicated Tier-0 for Each Tenant in NSX-T 2.x Multi-tenant Architecture - Dedicated Tier-0 for Each Tenant in NSX-T 2.x Multi-tenant Architecture - Dedicated Tier-0 for Each Tenant in NSX-T 2.x Multi-tenant Architecture - Dedicated Tier-0 for Each Tenant in NSX-T 2.x Multi-tenant Architecture - Dedicated Tier-0 for Each Tenant in NSX-T 2.x Multi-tenant Architecture - Dedicated Tier-0 for Each Tenant in NSX-T 2.x Multi-tenant Architecture - Dedicated Tier-0 for Each Tenant in NSX-T 2.x Multi-tenant Architecture - Dedicated Tier-0 for Each Tenant shows a traditional multi-tenant Ar nts using the Route Leaking VRF feature is possible. While this feature allows inter-VRF commu ting table. Starting with NSX-T 3.0. Virtual Routing and Forwarding (VRF) instances configured on the physical fabric can be extended to the NSX-T domain. A VRF Tier-0 gateway with two VRF gateways Hosted on a traditional Tier-0, gateway with two VRF gateways Hosted on a traditional Tier-0, gateway with two VRF gateways Hosted on a traditional Tier-0, gateway with two VRF gateways instances. Figure 4-19: Tier-0 gateway Hosted on a traditional Tier-0, gateway with two VRF gateways Hosted on a traditional Tier-0, gateway with two VRF gateways Hosted on a traditional Tier-0, gateway with two VRF gateways Hosted on a traditional Tier-0, gateway with two VRF gateways Hosted on a traditional Tier-0 gateway with two VRF gateways Hosted on a traditional Tier-0, gateway with two VRF gateways Hosted on a traditional Tier-0, gateway with two VRF gateways Hosted on a traditional Tier-0, gateway with two VRF gateways Hosted on a traditional Tier-0, gateway with two VRF gateways Hosted on a traditional Tier-0, gateway with two VRF gateways Hosted on a traditional Tier-0, gateway with two VRF gateways Hosted on a traditional Tier-0, gateway with two VRF gateways Hosted on a traditional Tier-0, gateway with two VRF gateways Hosted on a traditional Tier-0, gateway with two VRF gateways Hosted on a traditional Tier-0, gateway the two VRF gateways Hosted on a traditional Tier-0, gateway the two VRF gateways Hosted on a traditional Tier-0, gateway the two VRF gateways Hosted on a traditional Tier-0, gateway the two VRF gateways Hosted on a traditional Tier-0, gateway the two VRF gateways Hosted on a traditional Tier-0, gateway the two VRF gateways Hosted on a traditional Tier-0, gateway the two VRF gateways Hosted on a traditional Tier-0, gateway the two VRF gateways Hosted on a traditional Tier-0, gateway the two VRF gateways Hosted on a traditional Tier-0, gateway the two VRF gateways Hosted on a traditional Tier-0, gateway the two VRF gateways Hosted on a traditional Tier-0, gateway the two VRF gateways Hosted on a traditional 3.0 Multi-Tenant Architecture. Dedicated Tier-0 VRF Instances for Each VRF shows a typical single tier over gateway. Traditional server and the parent Tier-0 VRF instances an s that each Tier-0 VRF will have their own dedicated BGP process and needs to have their dedicated BGP peers. From a data plane stantic routes for the Tier-0 VRF while another Tier-0 VRF while another Tier-0 VRF gateways. It offers the flexibility to use static routes for the Tier-0 VRF while another Tier-0 VRF while another Tier-0 VRF gateways. It offers the flexibility to use static routes for the Tier-0 VRF while another Tier-0 VRF neir respective BGP peers on the physical networking fabric. It is important to emphasize that the Parent Tier-0 gateway has a BGP peering adjacency with the physical routers using their respective global routing table ro. Tier-1 Transit Subnet. All other configuration parameters can be independently managed: External Interface IP addresses BGP neighbor Prefix list, route-map, Redistribution Firewall rules NAT rules As mentioned p working Fabric When a Tier-0 VRF is attached to parent Tier-0, multiple parameters will be inherited by design and cannot be changed: Edge Cluster High Availability mode (Active/Active - Active) the mode and state of its Parent Tier-0. Both Active/Active or Active/Standby high availability mode are supported on the Tier-0 VRF gateways. It is not possible to have an Active/Active Tier-0 VR Figure 4-22: BGP Peering Tier-0 VRF Gateways and VRF on the Ne ndby Parent Tier-0. In a traditional Active/Standby design, a Tier-0 gateway failover can be triggered if all northbound BGP peers are unreachable. Similar to the high availability construct between the VRF Tier-0, the BGP peering design must match between the VRF topologies. Figure 4-23: Supported as each Tier-0, the BGP peering design must match between the VRF topologies. Figure 4-23: Supported as each Tier-0 and the Parent Tier-0, the BGP peering design must match between the VRF topologies. Figure 4-23: Supported as each Tier-0 and the Parent Tier-0. Inter-SR routing is not supported as each Tier-0. The big availability construct between the VRF topologies. Figure 4-23: Supported as each Tier-0 and the Parent Tier-0. Tier-0 and the Parent Tier-0. Tier-0 and the Parent Tier-0. Tier-0 and Tier-0 and Tier-0 and the Parent Tier-0. Tier-0 and Tier-0 and Tier-0 and Tier-0 and Tier-0. Tier-0 and the Parent Tier-0. Tier-0 and and on the VRF itself) have a redundant oath towards the network infrastructure. Both the Parent Tier-0 VRF gateway are peering with those of rack switch on another BGP process. The Parent Tier-0 VRF gateway are peering with those of its one of it While the very global and On the Parent Tier-0: VM "172.16.10.0" sends its IP traffic towards the internet through the Tier-0 SR2 and routed towards the internet will be sent towards the internet switch. Traffic to both Tier-0 SR2 as there is an inter-0 SR2 as there is an inter-0 SR2 as there is an inter-0 SR2 as the routed towards the internet switch. Traffic to both Tier-0 SR2 as there is an inter-0 SR2 using a 2 tuple. ndby topologies is also mandatory for VRF architectures as the Tier-0 VRF will inherit the behavior of the parent Tier-0 gateway. Figure 4-26: Unsupported r-0, it is important to note that the Tier-0 SR1 will not failover to the Tier-0 SR2. The reason behind this behavior is because a failover is triggered only if all e to the "down" state. Since Tier-0 SR1 still has an active BGP peer active, Traditional Tier-1 gateways can be connected to Tier-0 VRF to provide a multi-tier routing architecture and VRF-lite. Figure 4-27: Multi-Tier Routing architecture and VRF-lite Stateful services can either run on a Tier-0 VRF gateway can be connected to Tier-0 VRF gateway can be connected to Tier-0 VRF to provide a multi-tier routing architecture as demonstrated in Figure 4-27: Multi-Tier Routing architecture as demonstrated in Figure 4-27: Multi-Tier Routing architecture as demonstrated in Figure 4-27: Multi-Tier Routing architecture and VRF-lite. for VPN and Load Balancing as these features are not supported on a Tier-0 VRF. Tier-1 SR in charge of the stateful services for a particular VRF will be hosted on the same edge nodes as the Parent Tier-0 Cateway. Figure 4-28: Stateful Services Supported on Tier-1 represents stateful services for a particular VRF will be hosted on the same edge nodes as the Parent Tier-0 Cateway. Figure 4-28: Stateful Services Supported on Tier-1 Ry default, data-plane traffic to be exchanged between the VRF instances is isolated in NSX-T. By configuring VRF Route Leaking, traffic can be exchanged between the VRF instances to allow traffic to be exchanged. The next hop for these static routes must be configured on the Tier-0 VRF Route Leaking with Static Routes are necessary: Static Routes are necessary: Static Route on Tier-0 VRF A Destination Subnet: 172.16.20.0/24 Next Hop IP Address of Tier-1 DR in VRF A (e.g. 100.64.80.1) Admin Distance: 1 Scope: VRF-B Static Route on Tier-0 VRF B Destination Subnet: 172.16.10.0/24 Next Hop IP Address of Tier-1 DR in VRF A (e.g. 100.64.80.1) Admin Distance: 1 Scope: VRF-A Figure 4-29: VRF Route Leaking as traffic can be exchanged between a virtual workload on an VRF overlay segment and a bare metal server hosted in a different VRF on the physical networking fabric. NSX-T VRF route leaking requires that the next hop for the set he static route must not be a Tier-0 gateway. Static routes pointing to the directly connected IP addresses uplink would not be a recommended design as the static route would fail if an outage would fail nstrates the Tier-0 VRF gateways will use all available healthy paths to the networking fabric to reach the server in VRF-B. Figure 4-30: VRF-A In case of a physical available healthy path in Distance: 1 Scope: VRF-A In case of a physical available healthy path is to the networking fabric to reach the server in VRF-B. Figure 4-30: VRF-A In case of a physical available healthy path is to the networking fabric to reach the server in VRF-B. Tigure 4-30: VRF-A In case of a physical available healthy path is a contex and interface) Admin Distance: 1 Scope: VRF-B Static Route on Tier-0 VRF A Destination Subnet: 10.10.0/24 Next Hop IP Address of Tier-1 DR in VRF A (e.g. 100.64.80.1) Admin Distance: 1 Scope: VRF-A In case of a physical available healthy BGP peer advertising that host route. 4.5 IPv6 Routing Capabilities NSX-T Data Center also supports dual stack for the interfaces on a Tier-0 or Tier-1 Gateway. Users can also leverage distributed services like distributed for workloads now. Users can also leverage centralized services like distributed for North-South traffic. NSX-T refollowing unicast IPv6 addresses: Global Unicast: Globally unique IPv6 addresses used for inter-site communication but not routable on Tier-0 and Tier-1 Gateway. The following table shows a summarized view of supported IPv6 addresses types on NSX-T Datacenter components. Table 4-1: Type of IPv6 Addresses Supported on Tier-0 and Tier-1 Gateway. e 4-31: Single Tier and Multi-tier IPv6 Routing Topology on the right side with a Tier-0 Gateway supporting dual stack on all interfaces and a multi-tiered routing topology on the right side with a Tier-0 Gateway supporting dual stack on all interfaces and a multi-tier IPv6 routing topology on the right side with a Tier-0 Gateway and Tier-1 Gateway supporting dual stack on all interfaces to get dynamic IPv6 addresses from an external DHCPv6 relay supporting dual stack on all interfaces. A user can either a sign static IPv6 addresses to the workloads or use a DHCPv6 relay supporting dual stack on all interfaces and a multi-tier IPv6 addresses to the workloads or use a DHCPv6 relay supporting dual stack on all interfaces and a multi-tier IPv6 routing topology, each Tier-0-ting topology, each Tier-0-ting topology on the right side with a Tier-0 Gateway supporting dual stack on all interfaces. ports following IPv6 routing features: Static routes with IPv6 Next-hop MP-BGP with IPv4 and IPv6 address families Multi-hop eBGP IBGP ECMP support with static routes, EBGP and IBGP Outbound and I 4 routing. As soon as Tier-1 Gateway is connected to Tier-0 Gateway, the management plane configures a default route (::/0) on Tier-1 Gateway with next hop IPv6 address as Router link IP of Tier-0 Gateway ::1/64, as shown in Figure 4-32: IPv6 Routing in a Multi-tier Topology). To provide reachab lity to subnets connected to the Tier-1 Gateway, the Management Plane (MP) configures routes on the Tier-0 Gateway for all the LIFs connected to Tier-1 Gateway with a next hop IPv6 address as Tier-1 Gateway Router link IP (fc05:2b61:bd01:5000::2/64, as shown in Figure 4-32: IPv6 Routing in a Multi-tier Topology). 2001::/64 & 20 02:/64 are seen as "Tier-1 Connected" routes on Tier-0. Northbound. Tier-0 Gateway redistributes the Tier-0 the following concept is relevant to SR. This SR services are run on the SR component of a Tier-0 or the advertises these to its end or the edge nodes and has two modes of operation - advertises are run on the SR component of a Tier-0 or the advertises are run on the SR component of a Tier-0 or the advertises are run on the SR component of a Tier-0 or the advertises are run on the SR component of a Tier-0 or the advertises are run on the SR component of a Tier-0 or the advertises are run on the SR component of a Tier-0 or the advertises are run on the SR component of a Tier-0 or the advertises are run on the SR component of a Tier-0 or the advertises are run on the SR component of a Tier-0 or the advertises are run on the SR component of a Tier-0 or the advertises are run on the SR component of a Tier-0 or the advertises are run on the SR component of a Tier-0 or the advertises are run on the SR component of a Tier-0 or the advertises are run on the SR component of a Tier-0 or the advertises are run on the SR component of a Tier-0 or the advertises are run on the SR component of a Tier-0 or the advertises are run on the SR component or the advertises are run on the SR component or a transfer advertise are run on the SR component or a transfer advertise are run on the SR component or a transfer advertise are run on the SR component or a transfer advertise are run on the SR component or a transfer advertise are run on the SR component or a transfer advertise are run on the SR component or a transfer advertise are run on the SR component or a transfer advertise are run on the SR component or a transfer advertise are run or the advertise are run on the services are run on the SR component or a transfer advertise are run or the advertise are run ion mode are active forwarders. This high availability mode is only available on Tier-0 gateway. Stateful services typically require tracking of connection state (e.g., sequence number check, connection state), thus traffic for a given session needs to go through the same Edge node. As of NSX-T 3.0, active/active HA model. Left side of Figure 4-33: Tier-to gateway. Firewall or stateful services such as Gateway Firewall or stateful services such as Gateway Firewall or stateful services such as Gateway Firewall or stateful services such as for state (e.g., sequence number check, connection state), thus traffic for a given session needs to go through the same Edge node. As of NSX-T 3.0, active/active HA model. Left side of Figure 4-33: Tier-to gateway. Firewall or stateful services such as Gateway Firewall or stateful services such as Gateway Firewall or stateful services such as Gateway. d in Active/Active HA Mode shows a Tier-0 gateway (configured in active/active high availability mode) with two external interfaces leveraging two different Edge nodes, EN1 and EN2. A Compute host, ESXi is also shown in the diagram shows that the services router component (SR) of this Tier-0 gateway Configured in Active/Active HA Mode Note that Tier-0 SR on Edge nodes, EN1 and EN2. figures two default routes on Tier-0 DR with next hop as SR on EN1 (169.254.0.2) and SR on EN2 (169.254.0.3) to provide ECMP for overlay traffic coming from cc tion. Inter-SR Routing To provide redundancy for physical router failure, Tier-0 SRs on both Edge nodes must establish routing adjacency or exchange routing inform compute hosts. North-South traffic from overlay workloads hosted on Compute hosts will be load balanced and sent to SR on EN1 or EN2, which will further do a routing lookup to send traffic out to the physical infrastructure. A user does or a series of the series of th vard physical routers and different IP addre , users can enable Inter-SR routing. This feature is only available on Tier-0 gateway configured in active/active high availability mode. Figure prent routes. When Inter-SR routing is enabled by the user, an overlay segment is auto plumbed between SRs (similar to the transit segment auto plumbed between DR and SR) and each end gets an IP address assigned in 169.254.0.128/25 subnet by default. An IBGP session is automatically created between Tier-0 SR and northbound routes (EBGP and static routes) are exchanged on this IBGP route to a destination. Figure 4-34: Inter-SR nouting as replained in previous figure, Tier-0 SR and northbound routes (EBGP and static routes) are exchanged on this IBGP session. Figure 4-34: Inter-SR nouting a default routes with next here to a destination. In that case, traffic can go to either SR on EN1 or EN2. In case of asymmetry route (0.0.0.0/0) and a corporate prefix 192.168.100.0/24 from physical router 2 respectively. If "External 1" interface on Tier-0 SR on EN1, this traffic can follow the default route (0.0.0.0/0) learned via IBGP from Tier-0 SR on EN2. Traffic is being sent to EN2 through the Geneve overlay. After a route lookup on Tier-0 SR on EN1, this traffic can be sent to physical router 1 and BFD Interaction with Active/Active – Tier-0 SR for EN2. There is no value in preserving the forwarding table on either end or sending traffic to the failed or restarting device. In case of an active SR failure (i.e., the Edge node goes down), physical router 1 and physical router SR failure (i.e., the Edge node goes down), physical router SR failure (i.e., the Edge node goes down), physical router SR failure (i.e., the Edge node goes down), physical router SR failure (i.e., the Edge node goes down), physical router SR failure (i.e., the Edge node goes down), physical router SR failure (i.e., the Edge node goes down), physical router SR failure (i.e., the Edge node goes down), physical router SR failure (i.e., the Edge node goes down), physical router SR failure (i.e., the Edge node goes down), physical router SR failure (i.e., the Edge node goes down), physical router SR failure (i.e., the Edge node goes down), physical router SR failure (i.e., the Edge node goes down), physical router SR failur ation. In that case, traffic can follow the IBGP route to another SH inq will continue using another active SR or another TOR. BFD should be enabled with the physical routers for faster failure detection. It is recommended to enable GR If the Edge node is connected to a dual supervisor system that supports forwarding traffic when the control plane is restarting. This will ensure that forwarding traffic when the control plane is restarting supervisor or control plane is restarting. sor failover, then BFD should not be enabled with this system. If the BFD implem faces operational state is set as down so that they will automatically drop packets ters and advertise routes to the physical routers; however, the standby Tier-0 SR prepends its local AS three times in the BGP updates so that traffic from the physical routers prefer the ses on active and standby Tier-0 SRs are the same and the operational state of standby SR southbound interface is down, since the operational state of standby SR southbound interface is down, since the operational state of standby SR southbound Tier-0 SRs on Edge nodes "EN1" and "EN2". Figure 4-35: Active and Standby SR southbound Tier-0 SR southbound Tier-0 SRs are the standby SR southbound Tier-0 SR southbound Interface is down, since the operational state of standby SR southbound Tier-0 SR southbound Interface is down, since the operational state of standby SR southbound Tier-0 SRs are the standby SR southbound Tier-0 SR southbound Tier-0 SR southbound Interface is down, since the operational state of standby SR southbound Tier-0 S uting Control with eBGP The placement of active and standby SR in terms of connectivity to TOR or dates in the new of the second es using the newly active SR. If the TOR switch supports BFD, it is recommended to run BFD on both the eBGP neighbors for faster failure detection. It is recommended to enable GR If the Edge node is connected to a dual supervisor system that supports forwarding will continue through the restarting supervisor system that supports forwarding traffic when the control plane. Enabling BFD with such system depends on BFD implementation of hardware vendo High Availability Failover Triggers An active SR on an Edge node is declared down when one of the follo isor failover, then BFD should not be enabled with this system; however, if the BFD imp receive keep lives on both interfaces. All BGP sessions or northbound routing on or Tier-1 gateways. These features include: Connectivity to physical infrastructure (static routing / BGP / MP-BGP) VRF-lite NAT DHCP server Metadata proxy Gateway Firewall Load Rala . dedicated to running network and security services that cannot be distributed to the hypervisors. Edge node also provides connectivity to the physical infrastructure. Previous sections mentioned that centralized services will run on the SR component of Ti ncer L2 Bridging Service Interface VPN As soon as one of these services is configured or sport Zone: Any traffic that originates from a VM participating in NSX-T domain tivity to the physical infrastructure. De sing and high performance. There are different VM form factors available. Each of them has a different resource footprint and can be used to achieve different guidelines. These are detailed in the below table. Size Memory vCPU Disk Specific Usage Guidelines Small 4GB 2 200 GB PoC only. LB functionality is not ed services like NAT, Gateway Firewall. Load balancer functionality can be leveraged for POC. Large 32GB 8 200 GB Suitable for p way Firewall, load balancer etc. Extra Large 64GB 16 200GB Suitable for production with centralized services like NAT, Ga ervices like Laver 7 Load balancer and VPN. Bare metal Edge 32GB 8 200 GB Suitable fo Multi-TEP support on Edge Nod multi-TEP) configuration to load balance overlay traffic for overlay segments/logical switches, Multi-TEP is supported in both Edge VM and bare metal. Figure 4-36: Bare metal Edge -Same N-VDS for overlay and external traffic with Multi-TEP shows two TEPs configured on the bare metal Edge. Each overlay se ent/logical switch is pinned to a specific tunnel end point IP. TEP IP1 or TEP IP2. Each TEP uses a different uplink, for instance. TEP IP1 uses Uplink1 that's mapped t g multi-TEP feature on Edge and external traffic gets load balanced using "Named Teaming Policy". Figure 4-36: Bare metal Edge -Same N-VD ance, if pNIC P1 fails, TEP IP1 along with its MAC address will be migrated to use Uplink2 that's mapped to pNIC P2. In case of pNIC P1 failure pNIC P2 will carry the traffic for both TEP IP1 and TEP IP2. A Case for a Better Design: This version of the design guide introduced a simpler way to configure Edge connectivity, referred as "S ngle N-VDS Design". The key reasons for adopting "Single N-VDS Design": Multi-TEP support for Edge - Details of multi-TEP is described as above. Just like an ESXi transport node supporting multiple TEP, Edge node has a ca bility to support multiple TEP per uplink with following advantages: Removes critical topology restriction with bare metal - straigl raffic in both bare metal and VM form factor. Multiple te ion of both pNICs. Efficient load sharing among host to Edge VM. ming policy per N-VDS - Default and Named Tea ming Policy Allows specific uplink to be de An Edge VM s mode is the only supported booting mode on NSXT-T 3.0. A bare metal Edge differs from the VM form factor Edge are certain hardware requirements including CPU specifics and supported NICs can be found in the NSX Edge Bare Metal Requirements section of the NSX-T installation guide. When a bare metal Edge also supports in-band management traffic can leverage an interface is retained for management interfaces can also be 1G. Bare metal Edge node is installed, a dedicated interface is retained for management plane high availability. These management traffic can be used for overlay or external (N-S) can be used for overlay or external (N-S) is tabled, a dedicated interface is retained for management traffic can leverage an interface being used for overlay or external (N-S) can be used for management plane high availability. These metal Edge node is installed, a dedicated interface is retained for management traffic can leverage an interface being used for overlay or external (N-S) can be used for management plane high availability. These metal Edge node is installed, a dedicated interface is retained for management plane high availability. These metal Edge node is installed, a dedicated interface is retained for management traffic can leverage an interface being used for overlay or external (N-S) can be used for overlay or external (N-S) is desired. When a bare metal Edge node is installed, a dedicated interfaces (fp-eth) for overlay or external connectivity. 4.8.1.1 Management Plane Configuration Choices with Bare Metal Node This section covers all the available options in management with Single pNIC Left side of Figure 4-37. Bare Metal Edge Management Configuration Choices shows a bare metal edge node with 3 physical NICs. The dedicated pNIC for management traffic. The management traffic in this topology. If P1 goes down, the management traffic will fail. However, Edge node will continue to function as this doesn't affect of the figure 4-37. Bare Metal Edge Management traffic will fail. However, Edge node will continue to function as this doesn't affect of the figure 4-37. Bare Metal Edge Management traffic will fail. Howe here the place of the diagram shows the bare metal Edge with four physical with the stopply with a stopply with the stopply w the function of the open set of the provide of the ling to spanning tree related convergence. External traffic from these VLAN segments is load balanced across uplinks using named teaming policy which pins a VLAN segment to a ides redundancy for management, overlay and external traffic, in event of a pNIC failure on Edge node/TOR and TOR Failure. The right side of the diagram shows two pNICs bare metal Edge configured for Multi-TEP - Single N-VDS for Overlay and External Traffic (With dedicated pNICs for Management and In-Band Management.) Figure 4-38: Bare Metal Edge configured for Multi-TEP - Single N-VDS for Overlay and External traffic, in event of a pNIC failure on Edge node/TOR and In-Band Man port node profile as shown in Figure 4-39: Bare Metal Edge Transport Node Profile. This configuration shows a default teaming policy that uses both Uplink1 and Uplink2. This default policy is used for all the common this VLAN only on "Uplink1". "External VLAN segment 400" is configured to use a named teaming policy "Vlan400-Policy" that sends traffic from this VLAN only on "Uplink2". Based on these teaming policy nents/logical switches created on this N-VDS. Two additional teaming policies, "Vlan300-Policy" and "Vlan400-Policy" have been defined to override the default te TOR-Left will receive traffic for VLAN 100 (Mgmt.), VLAN 200 (overlay) and VLAN 300 (Traffic from VLAN segment 300) and hence, should be configured for the Figure 4-39: Bare Metal Edge node "EN1", whereas External interfaces 3 and 4 are provided by bare metal Edge node "EN2". Both the Edge node are in the same are configured for Multi-TEP and use named in golice is not it is similar to send traffic from VLAN 300 to TOR-Left at traffic shows NSX-T bare metal Edge with six physical NICs. Manager 101 Vision and four external interfaces and provides 4-way ECMP. Figure 4-41: Bare Metal Edge with Six pNICs Figure 4-40: 4-way ECMP Using Bare Metal Edge with Six pNICs Figure 4-40: 4-way ECMP. Figure 4-40: 4-way ECMP Using Bare Metal Edge with Six pNICs Figure 4-41: Bare Metal Edge with Six pNICs Figure 4-40: 4-way ECMP Using Bare Metal Edges 4.8.1.3 Single N-VDS Bare Metal Edge with Six pNICs Figure 4-40: 4-way ECMP Using Bare Metal Edges 4.8.1.3 Single N-VDS Bare Metal Edge 4.8.1.3 Single N-VD ement traffic has two dedicated pNICs configured in Active/Standby. Two pNICs, P3 and P4 s - Same N-VDS for Overlay and External traffic also shows a configuration screenshot of named teaming policy defining two additional teaming policies, "Vlan300-Policy" and "Vlan400-Policy". "External VLAN segment 300" is config "External VLAN segment 300" is configured to use a named teaming policy "Vlan300-Policy" that sends traffic from this VLAN only on Uplink3 (mapped to pNIC P5). "External VLAN segment 400" is configured to use a named teaming policy "Vlan400-Policy" that sends traffic from this VLAN only on Uplink3 (mapped to pNIC P5). "External VLAN segment 400" is configured to use a named teaming policy "Vlan400-Policy" that sends traffic from this VLAN only on Uplink3 (mapped to pNIC P5). "External VLAN segment 400" is configured to use a named teaming policy "Vlan400-Policy" that sends traffic from this VLAN only on Uplink3 (mapped to pNIC P5). "External VLAN segment 400" is configured to use a named teaming policy "Vlan400-Policy" that sends traffic from this VLAN only on Uplink3 (mapped to pNIC P5). "External VLAN segment 400" is configured to use a named teaming policy "Vlan400-Policy" that sends traffic from this VLAN only on Uplink4 (mapped to pNIC P5). "External VLAN segment 400" is configured to use a named teaming policy "Vlan400-Policy" that sends traffic from this VLAN only on Uplink4 (mapped to pNIC P5). "External VLAN segment 400" is configured to use a named teaming policy "Vlan400-Policy" that sends traffic from this VLAN only on Uplink4 (mapped to pNIC P5). "External VLAN segment 400" is configured to use a named teaming policy "Vlan400-Policy" that sends traffic from this VLAN only on Uplink4 (mapped to pNIC P5). "External VLAN segment 400" is configured to use a named teaming policy "Vlan400-Policy" that sends traffic from this VLAN only on Uplink4 (mapped to pNIC P6). ign bandwidth and deterministic design as there are dedicated physical NICs for different traffic types (overlay and External traffic). Figure 4-41: Bare Metal Edge with Six pNICs - Same N-VDS for Overlay and External traffic 4.8.2 VM Edge in VM form factor can be installed using an OVA, 1. These interfaces are allocated for external connectivity to TOR switches and for NSX-T overlay tunneling. There is complete flexibility in assigning Fast Path interfaces (fp-eth) for overlay or external connectivity. As an example, fp-eth0 could be assigned for overlay traffic with fp-eth1, fp-eth2, or both for external traffic engineering), more than one N-VDS per Edge node may be required. Each N-VDS instance can have a unique teaming policy, allowing for flexible design nucleics. 4.8.2.1 Multiple N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration - NSX-T 2.4 or Older The "three N-VDS per Edge VM Configuration ier-0 on VIAN 300 always goes to TOR-Left and BGP traffic. This topology also provides a simple, high bandwidth and deterministic design as there are dedicated physical NICs for different traffic. This topology also provides redundancy for management, overlay and External traffic types (overlay and External traffic types) to TORLET and BOT I date from the or VLAY too away goes of the rest and the proof port that the proof of the test is the second of the test is t nly called has been deployed in production. This section briefly covers the design, so the reader does not miss the important decision which design to adopt based on NSX-T release. This design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and viable to Edge VM design recommendation is still completely applicable and via ion, the pre-2.5 release design has been moved to Appendix 5. The design choices that moved to appendix covers 2 pNICs bare metal design necessitating straight through LAG topology Edge clustering design consideration for bare metal design added to support existing deployment of operate properly if adopted in release before NSX-T 2.5. Figure 4-42: Edge Node VM Installed Leveraging VDS Port Groups on a 2 pNIC host Figure 4-42: Edge Node VM Installed Leveraging VDS Port Groups on a 2 pNIC host Figure 4-42: Edge Node VM Installed Leveraging VDS Port Groups on a 2 pNIC host shows an ESXi host with two physical NICs. Edges "VM1" is hosted on ESXi host le c use different vNIC of Edge VM. All three N-VDS use the same teaming policy i.e. Failover order with one active uplink. 4.8.2.2 VLAN TAG Requirements Edge VM deployment shown in Figure 4-42: Edge Node VM Installed Leveraging VDS Port Groups on a 2 pNIC host remains valid and is ideal for deployment shown in Figure 4-42: Edge Node VM Installed Leveraging VDS Port Groups on a 2 pNIC host remains valid and is ideal for deployment shown in Figure 4-42: Edge Node VM Installed Leveraging VDS Port Groups on a 2 pNIC host remains valid and is ideal for deployment shown in Figure 4-42: Edge Node VM Installed Leveraging VDS Port Groups on a 2 pNIC host remains valid and is ideal for deployment shown in Figure 4-42: Edge Node VM Installed Leveraging VDS Port Groups on a 2 pNIC host remains valid and is ideal for deployment shown in Figure 4-42: Edge Node VM Installed Leveraging VDS Port Groups on a 2 pNIC host remains valid and is ideal for deployment shown in Figure 4-42: Edge Node VM Installed Leveraging VDS Port Groups on a 2 pNIC host remains valid and is ideal for deployment shown in Figure 4-42: Edge Node VM Installed Leveraging VDS Port Groups on a 2 pNIC host remains valid and is ideal for deployment shown in Figure 4-42: Edge Node VM Installed Leveraging VDS Port Groups on a 2 pNIC host remains valid and is ideal for deployment shown in Figure 4-42: Edge Node VM Inst 4 pNICs bare metal design added to support existing deployment Edge node design with 2 and 4 pNICs It's a mandatory to adopt Appendix 5 recommendation for NSX-T release up to 2.5. The newer design as described in section The Design Recommendation with Edge node NSX-T Release 2.5 most with two physical NICs. Edges "VM1" is hosted on ESXi host leveraging the VDS port groups, each connected to both TOR switches. This figure also shows three N-VDS, named as "Overlay N-VDS", "Ext 1 N-VDS", and "Ext 2 N-VDS". Three N-VDS are used in this design to ensure that overlay and rt Groups on a 2 pNIC host remains valid and is ideal for deployments where only one VLAN is necessary on each vNIC of the Edge VM. However, it doesn't cover all the deployment use cases. For instance, if a user cannot add service interfaces to connect VLAN backed workloads in above topology as hat requires to allow one or more VLANs on the VDS DVPG (distributed virtual port group). If these DVPGs are configured to allow multiple VLANs, a VLAN tag is expected from Edge VM for traffic at either N-VDS level. On N-VDS level or VSS/VDS level. On N-VDS, overlay and external traffic can be tagged usin It uplink Profile where the transport VLAN can be set which will tag overlay traffic only VLAN segment connecting Tier-0 Gateway to external devices. This configuration will apply a VLAN tags to the external traffic only. Following are the there we ample, VLAN tags are applied to both overlay and external traffic using uplink profile and VLAN segments connecting Tier-0 Gateway to physical infrastructure respectively. As a result, VDS port groups that provides connectivity to Edge VM rece VDS port group "Transport PG" is VLAN tagged. That means that this Edge VM vNIC2 will have to be attached to a port group configured for Virtual Guest Tagging (VGT). Tier-0 Gateway connects to the physical infrastructure using "External-1" <sup>6</sup> "Ext1 PG" and Ext2 PG" is VLAN tagging on Edges that include the program of the edge value of the Single N-VDS Based Configuration - Starting with NSX-T 2.5 release Starting NSX-T 2.4 release, Edge nodes support Multi-TEP configuration to load balance overlay traffic for segments/logical switches. Similar to the bare metal Edge note N-VDS design. Edge VM with one N-VDS for overlay and external traffic. Ever x 5. Figure 4-44: VLAN Tagging on Edge Node with Single N-VDS shows an Edge VM with one N-VDS i.e. "Overlay and external traffic. Multi-TEP is configured to provide load balancing for overlay traffic on "Uplink1" and "Uplink2" are mapped to use vNIC2 po f rack switches. Similar to Figure 4-43: VLAN Tagging on Edge Mode, Tier-0 Gateway for BGP peering connects to the physical infrastructure leveraging VLAN segment 300" and "External VLAN Segment 30 ured with a VLAN tag, 300 and 400 respectively. External traffic received on VDS port groups "Trunk1 PG" and Trunk2 PG" is VLAN tagged and hence, these port groups should be configured in VGT (Virtual guest tagging) mode and allow those specific VLANs. Na med teaming policy is also configured to load balance external traffic. Figure 4-44: VLAN Tagging on Edge Node with Single N-VDS also shows named teaming policy configuration used for this topology. "External VLAN segment 300" is configured to use a named teamin that sends traffic from this VLAN on "Uplink1" (vNIC2 of Edge VM). "External VLAN segment 400" is configured to use a named teaming policy "Vlan400-Policy" that sends traffic from this VLAN on "Uplink2" (vNIC3 of F VM). Based on this named teaming policy, North-South or external traffic from "External VLAN Segment 300" will always be sent and received on vNIC2 of the Edge VM. North-South or external traffic from "External VLAN Segment 400" will always be sent and received on vNIC3 of the Edge VM. North-South or external traffic from "External VLAN Segment 300" i.e. VLAN 300 always be active uplink as "VDS-Uplink1". This configuration ensures that the traffic sent on "External VLAN Segment 300" i.e. VLAN 300 always as "VDS-Uplink2" and standby uplink as "VDS-Uplink2". "Trunk2 PG" is configured to use active uplink as "VDS-Uplink1". This configuration ensures that the traffic sent on "External VLAN Segment 300" i.e. VLAN 300 always as "VDS-Uplink2"." with a ways be sent and to be vertical rlay and external traffic. Load balancing of overlay traffic with Multi-TEP configuration. Ability to distribute external traffic to specific TORs for distinct point to point routing adjacencies. No change in DVPG configuration when new service interfaces (workload VLAN segments) are added. Deterministic North South traffic vite faces (workload VLAN segments) are added. Deterministic North South traffic vite faces (workload VLAN segments) are added. Deterministic North South traffic vite faces (workload VLAN segments) are added. Deterministic North South traffic vite faces (workload VLAN segments) are added. Deterministic North South traffic vite faces (workload VLAN segments) are added. Deterministic North South traffic vite faces (workload VLAN segments) are added. Deterministic North South traffic vite faces (workload VLAN segments) are added. Deterministic North South traffic vite faces (workload VLAN segments) are added. Deterministic North South traffic vite faces (workload VLAN segments) are added. any other VLAN or overlay segments. Tier-0 SR or Tier-1 SR is always hosted on Edge node (bare metal or Edge VM). Figure 4-45: VLAN Tagging on Edge Node with Service Interface shows a VLAN segment "VLAN Seg-500" that is defined to provide connectivity to red both on Tier-0 and Tier-1 Gateways configured in active/standby HA configuration mode. Service interface is realized on Tier-1 SR. This implies that traffic from a VLAN workload needs to go to Tier-0 SR to consume any centralized service or to the VLAN workloads. "VLAN Seg-500" is configured with a VLAN tag of 500. Tier-0 gateway has a service interface "Service Interface-1" configured leveraging this VLAN segment and acts as a gateway for VLAN workloads connected to this VLAN segment. In this example, it the workload VM, Vlan sed to a make of the second of the s gruing the logical router some the logical router and the router as a figure 4-47; Multiple Edge Cluster with Dedicated Tier-0 and Tier-1 gateways can be hosted on one Edge nodes and Figure 4-47; Multiple Edge Clusters with Dedicated Tier-0 and Tier-1 gateways can be hosted on one Edge nodes and the router as a figure 4-47; Multiple Edge Clusters with Dedicated Tier-0 and Tier-1 gateways can be hosted on one Edge nodes and the router as a figure 4-47; Multiple Edge Cluster with Dedicated Tier-0 and Tier-1 gateways. Figure 4-47; Multiple Edge Clusters with Dedicated Tier-0 and Tier-1 gateways can be hosted on one Edge nodes and the router as a figure 4-47; Multiple Edge Clusters with Dedicated Tier-0 and Tier-1 gateways. Figure 4-47; Multiple Edge Clusters with Dedicated Tier-0 and Tier-1 gateways can be hosted on one Edge nodes and hosted on one Edge nodes and be provides external connectivity to the physical infrastructure. Edge node: A maximum of 10 Edge nodes can be decided tier-0 gateway supports a maximum of eight equal cost paths, thus a maximum of 10 Edge nodes can be decided tier-0 gateway supports a maximum of eight equal cost paths, thus a maximum of 10 Edge node. A maximum of 10 Edge node can be figure 4-47; Multiple Edge Cluster (Figure 4-47; Multiple Edge Cluster) and Tier-1 gateways can be hosted on one Edge node. A maximum of 10 Edge node can be figure 4-47; Multiple Edge Cluster (Figure 4-47; Multiple Edge Cluster) and Tier-1 gateways can be hosted on one Edge node. A maximum of 10 Edge node can be figure 4-47; Multiple Edge Cluster (Figure 4-47; Multiple Edge Cluster) and Tier-1 gateways can be hosted on one Edge node. A maximum of 10 Edge node can be figure 4-47; Multiple Edge Cluster (Figure 4-47; Multiple Edge Cluster) and Tier-1 gateways can be hosted on one Edge node. A maximum of 10 Edge node can be figure 4-47; Multiple Edge Cluster) and Tier-1 gateways can be hosted on one Edge node. A maximum of 10 Edge node can be figure 4-47; Multiple Edge Cluster) and Tier-1 gateways can be hosted o odes are supported for ECMP. Edge nodes in an Edge cluster run Bidirectional Forwarding Detection (BFD) on both tunnel and management networks to detect Edge node failure. The BFD protocol provides fast detection of failure for forwarding paths or forwarding paths or forwarding betection (BFD) on both tunnel and management networks to detect Edge node failure. The BFD protocol provides fast detection of failure for forwarding paths or forwarding paths or forwarding engines, improving convergence. Edge NMs support BFD with minimum BFD timer of 50ms with three retries, providing a 1.5 second failure for forwarding paths or forwarding paths or forwarding paths or forwarding engines. In the large for ative instance of this Tier-1 SR is created and if active and stant to be a part of failure domain 2. (EN3 or EN4). Figure 4-48: Failure domain 2. When a new Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of this Tier-1 SR is created and if active and stant by instance of the stant by instance of this Tier-1 SR is created and if active and stant by instance of the stant by insta ser can also enforce that all active Tier-1 SRs are placed in one failure domain. This configuration is supported for Tier-1 gateway in preemptive mode only. 4.9 3704. It prevents packets with spoofed source IP address to be forwarded in the network. uRPF is generally enabled on a router per interface and not globally. A only used by sending packets with random source IP addresses. Figure 4-49 – uRPF diagrams a physical network with uRPF enabled on the core router. 1 — The the way in preemptive mode only. 4.9 Other Network Services 4.9.1 Unicast Reverse Path Forwarding (uRPF) A router forwards packet based on the value of the destination IP address field is generally not used when forwarding a packet based on the value of the destination IP address field is generally not used when forwarding a packet based on the value of the destination IP address field is generally not used when forwarding a packet based on the value of the destination IP address field is generally not used when forwarding a packet based on the value of the destination IP address field is generally not used when forwarding a packet based on the value of the destination IP address field is generally not used when forwarding a packet based on the value of the destination IP address field is generally not used when forwarding a packet based on the value of the destination IP address field is generally not used when forwarding is defined in RFC. When a packet arrives on an interface, the router will verify if the received on an interface. When a packet arrives on an interface, the router will verify if the received and routing table interfaces are different. This protection prevents spoofed source IP address of 10.1.1.1 on interface ethernet 0/2. 2- The core router receives a packet will be routed through interface ethernet 0/2. In this case, 10.1.1.1 is the source IP address present in the IP header. The core router has a longest prefix would be routed through interface ethernet 0/2. In this case, 10.1.1.1 is the source IP address present in the IP header. The core router has a longest prefix the source IP address present in the IP header. The core router has a longest prefix the source IP address present in the IP header. The core router has a longest prefix the source IP address present in the IP header. The core router has a longest prefix the source IP address present in the IP header. The core router has a longest prefix the source IP address present in the IP header. The core router has a longest prefix the tch for 10.1.1.0/24 via interface ethernet 0/0. 3-Since the packet does not come from the interfaces. From a security standpoint, it is a best practice to keep uRPF is also recommended in architectures that leverage ECMP. On intra-tier and router link interfaces, a simplified anti-spoofing mechanism is implemented. It is checking that a packet is never sent back to the interfaces. The second of th the dwhen the Tier-0 is in active/active mode. Table 4-3: NAT Usage Guidelines Table 4-4: Tier-0 and Tier-1 NAT Use Cases summarizes the use cases and advantages of running NAT on Tier-0 and Tier-1 gateways. Gateway Type NAT Rule Type Specific Usage Guidelines Tier-0 Stateful Recommended for TAS/TKGI deployments. F-W routing hetways the use cases and advantages of running NAT on Tier-0 and Tier-1 gateways. rent tenants remains completely distributed. Tier-1 Stateful Recommended for high throughput ECMP topologies. Recommended for topologies with overlapping IP address space. Table 4-4 y and DHCP server functionality. DHCP requests from VMs connected to NSX-managed segments. DHCP servers, VM instance specific Edge nodes as with NAT functionality. 4.9.4 Metadata Proxy Service With a metadata proxy server, VM instance specific metadata from an penStack Nova API server. This functionality is specific to OpenStack use-cases only. Metadata proxy service runs as a service on an NSX Edge node. For high availability, configure metadata proxy to run on two or more NSX Edge nodes in an NSX Edge cluster. 4.9.5 Gateway Firewall Service Gateway Firewall service can be enabled on the Tier-0 and Tier-1 gateway for North-South firewalling. Table 4-5 summarizes Gateway Firewall Specific Usage Guidelines Stateful Can be enabled on both Tier-0 and Tier-1 gateway because of the construction of the constructio n exchange network traffic together without implementing any change in the physical networking fabric. Proxy ARP is automatically enabled when a NAT rule or a load balancer VIP uses an IP address from the subnet of the Tier-0 uplinks. In this example, the virtual machine connected to an NSX-T overlay segment and a virtual machine connected to an NSX-T overlay segment and a virtual machine or physical appliance to a VLAN segment shared with the NSX-T overlay segment and a virtual machine or physical appliance to a VLAN segment shared with the NSX-T overlay segment and a virtual machine connected to an NSX-T overlay segment and virtual machine connected to an the vortage is generative to the vortage is g and the virtual machine receives it. It is crucial to note that in this case, the traffic is initiated by the virtual machine which is connected to the overlay segment on the Tier-1/Tier-0 since the initial traffic was initiated by the virtual machine which is connected to the overlay segment on the Tier-1. If the initial traffic was initiated by the virtual machine which is connected to the overlay segment on the Tier-1. If the initial traffic was initiated by the virtual machine which is connected to the overlay segment on the Tier-1. If the initial traffic was initiated by the virtual machine which is connected to the overlay segment on the VLAN segment, a Destination NAT rule would have been required on the Tier-1. If the initial traffic was initiated by the virtual machine which is connected to the overlay. It is crucial to fathom that the newly active Tier-0 gateway with Proxy ARP enabled. The newly will send a Gratuitous ARP to announce the new MAC address to be used by the hosts on the VLAN segment in order to reach the virtual machine connected to the overlay. It is crucial to fathom that the newly active Tier-0 will send a Gratuitous ARP for each IP address that are configured for Proxy ARP. Figure 4-51: Edge Node Failover and Proxy ARP enabled. The newly active Tier-0 gateway provides at the provide of the many topologies shows three topologies with Tier-0 gateway provides E-W routing between subnets. Tie . The third topology shows a multi-tiered topology with Tier-0 gateway configured in Active/Standby HA mode to provide some centralized or stateful services like NAT, VPN etc. Figure 4-52: Single Tier and Multi-tier Routing Topologies As discussed in the two-tier routing ides multiple active paths for L3 forwarding using ECMP. The second topology shows centralized services configured on a Tier-1 and Tier-0 gateway. In NSX-T 2.4 release or earlier, some centralized services are only available on Tier-1 like load balancer and other only on logy shows the multi-tiered approach where Tier-0 gateway provides multiple active paths for L3 forwarding using ECMP and Tier-1 gateways as first hops trailized services can be enabled on Tier-1 or Tier-0 gateway level. Figure 4-52: Single Tier and Multi-tier Routing Topologies shows two multi-tiered topology shows centralized services configured on a Tier-1 and Tier-0 gateway swile Tier-0 gateway provides multi-tiered topologies. The first topology shows centralized services are only available on Tier-1 gateways while Tier-0 gateway not starting NSX-T 2.5 release or earlier, some centralized services are only available on Tier-1 gateways starting NSX-T 2.5 release. Figure 4-52: Single Tier and Multi-tiere double active paths for L3 forwarding using ECMP. The second topology shows centralized services are only available on Tier-1 gateways starting NSX-T 2.5 release. below topology can be used where requirement is to use both Load balancer and other only on NSX-T 2.5 release. Figure 4-53: Stateful and Stateless (ECMP) Services shows a topology with Tier-0 gateway scannected back to back. "Tenant-1 Tier-0 Gateway" is configured for a stateful firewall while "Tenant-2 Tier-0 Gateway" has stateful reways with trans-2 Tier-0 Gateway" and "Tenant-2 Tier-0 Gateway" and "Tenant-2 Tier-0 Gateway" and "Tenant-2 Tier-0 Gateway" and "Tenant-1 Tier-0 Gateway" and "Tenant-2 Tier-0 Gateway" and "Tenant-2 Tier-0 Gateway" and "Tenant-2 Tier-0 Gateway" and "Tenant-2 Tier-0 Gateway" and "Tenant-1 Tier-0 Gateway" and "Tenant-2 Tier-0 Gateway" and "Tenant-2 Tier-0 Gateway" and "Tenant-1 Tier configured on a Tier-1 and Tier-0 gateway. In NSX-T 2.4 release or earlier, some centralized services are only available on Tier-1 like load balancer and other only on Ti vs a topology with Tier-0 gateways connected back to back. "Tenant-1 Tier-0 Gateway" is configured for a stateful firewall while "Tenant-2 Tier-0 Gateway" has stateful ides high N-S throughput with centralized stateful services running on different Tier-0 gateways. This topology also provides complete separation of routing tables on the tenant Tier-0 gateways (like VPN until NSX-T 2.4 release) to leverage ECMP northbound. Note that VPN is available on Tier-0 gateways (like VPN until NSX-T 2.4 release) to leverage ECMP northbound. Note that VPN is available on Tier-0 gateways (like VPN until not complete separation of routing tables on the tenant Tier-0 gateways (like VPN until NSX-T 2.4 release) to leverage ECMP northbound. Note that VPN is available on Tier-0 gateways (like VPN until not complete separation of routing tables on the tenant Tier-0 gateways (like VPN until not complete separation of routing tables on the tenant Tier-0 gateways (like VPN until not complete separation of routing tables on the tenant Tier-0 gateways (like VPN until not complete separation of routing tables on the tenant Tier-0 gateways (like VPN until not complete separation of routing tables on the tenant Tier-0 gateways (like VPN until not complete separation of routing tables on the tenant Tier-0 gateways (like VPN until not complete separation of routing tables on the tenant Tier-0 gateways (like VPN until not complete separation of routing tables on the tenant Tier-0 gateways (like VPN until not complete separation of routing tables on the tenant Tier-0 gateways (like VPN until not complete separation of routing tables on the tenant tier-0 gateways (like VPN until not complete separation of routing tables on the tenant tier-0 gateways (like VPN until not complete separation of routing tables on the tenant tier-0 gateways (like VPN until not complete separation of routing tables on the tenant tier-0 gateways (like VPN until not complete separation of routing tables on the tenant tier-0 gateways (like VPN until not complete separation of routing tables on the tenant tier-0 gateways (like VPN until not complete separation of routing tables on the tenant tier-0 gateways (like VPN until not comple The control of the co not a be in the new of and the NSA-1 in the NSA-1 in the NSA-1 in the NSA-1 supports is micro-segmentation of opticative data within the internal begin by the or the period of address in the NSA-1 supports is micro-segmentation of opticative data within the internal by the NSA-1 supports is micro-segmentation of opticative data within the internal by the NSA-1 supports is micro-segmentation of opticative data within the internal by the NSA-1 supports is micro-segmentation and use is that we see as a construct to be address in the observation of address in the new sequence of the NSA-1 supports is micro-segmentation of optication of address in the observation of the internal by the NSA-1 supports is micro-segmentation and use is that we set the perimeter of address in the observation of address in the observation of a data we is that and the internal by the vay (ALGs). For monitoring and troubleshooting, the NSX-T Manager interacts with a host-based management plane (CCP) and the Local Control Plane (LCP). The CCP is implemented from all NSX-T transport nodes. 5.2.2 Control Plane to extratistics. The NSX-T manager interacts with a host-based management plane (CCP) and the Local Control Plane (LCP). The CCP is implemented from all NSX-T transport nodes. 5.2.2 Are the second of the second o ant virtual NICs instead of every rule everywhere, which would be a suboptimal use of hypervisor resources. Additional details on data plane components for both ESXi and KVM hosts as part of the same NSX-T luster. The DFW is functionally identical in both environments; however, there are architectural ifferences depending on the hypervisor specifics. Management and control plane components are identical for both ESXi and KVM hosts. For the data plane, they use a different implementation for packet handling. NSX-T uses either the VDS in ESXi 7.0 and later or the N-VDS (which is derived from the VDS) on earlier ESXi hosts, along with the VMs and the VDS, see NSX-T Logical Switching. For KVM posts NSX-T uses either the VDS in ESXi 7.0 and later or the N-VDS and the VDS, see NSX-T Logical Switching. For KVM posts NSX-T uses with the VSS and the VDS a re vCenter to be present. Figure 5-3: NSX-T Management Plane Components on KVM provides details on the data plane components for the ESX host. For KVM, there is an additional components for the ESX host. Figure 5-3: NSX-T Management Plane Components on KVM to provide DFW functionality, thus the LCP agent in additional components for the ESX host. Figure 5-3: NSX-T Management Plane Components on KVM to provide DFW functionality, thus the LCP agent in additional components on KVM to provide details on the data plane components for the ESX host. Figure 5-3: NSX-T Management Plane Components for the ESX host. Figure 5-3: NSX-T Management Plane Components on KVM to provide DFW functionality, thus the LCP agent in additional components for the NSX-T management Plane Components for the ESX host. Figure 5-3: NSX-T Management P In the first of the problem in the first of the problem is the p 5-Tuple match. Flow Matching Top Style addition for the flow table for cide on the policy approach - application-centric, infrastructure-centric, or network-centric Policy Rule Model - Select grouping and management strategy for policy rules by the NSX-T 54.1 Security Policy Methodology This section details the considerations behind policy creation strategies to help determine which capabilities of the NSX-T platform sh upping methodologies and policy application solution solution without a solution solution and application in the solution solutio de significant benefits in an environment that is static, lacks mobility, and has infrastructure functions that are properly demarcated. 5.4.1.3 Infrastructure components such as segments or segment ports, identifying where application VMs are connected. Security teams must work closely with the network administrators to understand logical and physical boundaries. If there are no physical or logical or l tion. An application-centric model does not provide significant benefits in an environment that is static, lacks mobility, and has infrastructure functions that are properly demarcated. 5.4.1.3 ing objects. A security team needs to aware of networking infrastructure to deploy network-based policies. There is a high probability of security rule sprawal as grouping based on dynamic attributes is not used. This method of grouping works well for migrating tation strategies. The first criteria in developing a policy model is to align with the natural boundaries in the data center, such as tiers of application, SLAs, isolation requirements, and zonal access restrictions. Associating a top-level zone or boundary to a policy of a policy is not used. hared services. Zoning creates relationships between various groups, providing basic segmentation and policy strategies. A second criterion in developing policy models is identifying reactions to security event lity is discovered, what are the mitigation strategies? Where is the exposure - internal or external? Is the exposure - intern cec into the NSX-T DFW rule table. Each of the classification shown represents a category on NSX-T frewall table layout. The Firewall rules table, which is using NSX-T Manager GUI or REST API mework. When defining security policy rules for the firewall rules table, it is recommended to follow these high-level steps: • VM Inventory Collection - Identify and organize a list of all hosted virtualized workloads on NSX-T transport nodes. • Tag Workload - Use VM inventory collection to organize to rule table, which is using RU, represented a categories and tags can be added to entities with existing tags. In the application centric approach of segmentation, categories and tags can be added with each application centric approach of segmentation, categories and tags can be added with each application centric approach of segmentation. • Group Workloads - Use the NSX-T logical grouping construct with dynamic or static membership criteria based on VM name, tag port, IP's, or other attributes, NSX-T allows for thousands of groups based on tags, although rarely are more than a dozen or so needed. Define Security Policy - Using the firewall rule table, define the security policy. Have categories and policies to separate and identify emergency, infrastructure, environment, and application-specific policy rules based on the rule model. The methodology and rule model mentioned earlier would influence how to tag and group the workloads as well as affect policy defi tion. The following sections off in and frame and in the mic criteria. Table 5-1: NSX-T Objects used for Groups shows one type of grouping criteria based on NSX-T Objects. NSX-T Objects. NSX-T Objects end subnets. Segment All VMs/vNICs defined within the Group will be selected. Group Nested (Sub-group) of collection of referenceable objects - all VMs/vNICs defined within the Group will be selected. Group Nested (Sub-group) of collection of referenceable objects - all VMs/vNICs defined within the Group will be selected. MAC Address Selected MAC sets container will be selected. MAC sets container will be used. MAC sets container will be selected. ry Description VM Name All VMs that control workloads will affect group membership alone, not the rules. Publishing a change of group membership to the underlying hosts is more efficient than publishing a rule change. It is ses. AD Groups Grouping based on Active Directory groups for Identity Firewall (VDI/RDSH) use case. Table 5-1: NSX-T Objects used for Groups Table 5-2: VM Properties used for Groups list the selection criteria based on VM properties are provided by the selection criteria based on VM provided by the selection criteria based by Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included in Group named "SG-WEB". 
Using dynamic inclusion criteria, all VMs with name starting by "WEB" are included i tand the best practices around organizing the policies. In the data path, the packet lookup will be performed from top to bottom order, starting with ting. Firewall Log carries this Rule ID when rule logging is enabled. Source and Destination: So hs. ALGs are only supported in statetul mode; if the section is marked as stateless, the ALGs will not be implemented. AlGs may be supported in statetul mode; if the section is marked as stateless, the ALGs will not be implemented. AlGs may be supported in statetul mode; if the section is marked as stateless, the ALGs will not be implemented. AlGs may be supported in statetul mode; if the section is marked as stateless, the ALGs will not be implemented. AlGs may be supported in statetul mode; if the section is marked as stateless, the ALGs will not be implemented. AlGs may be supported in statetul mode; if the section is marked as stateless, the ALGs will not be implemented. AlGs may be supported in statetul mode; if the section is marked as stateless, the ALGs will not be implemented. AlGs may be supported in statetul mode; if the section is marked as stateless, the ALGs will not be implemented. AlGs may be supported in statetul mode; if the section is marked as stateless, the ALGs will not be implemented. AlGs may be supported in statetul mode; if the section is marked as stateless, the ALGs will not be implemented. AlGs may be supported in statetul mode; if the section is marked as stateless, the ALGs will not be implemented. AlGs may be supported in statetul mode; if the section is marked as stateless, the ALGs will not be implemented. AlGs may be supported in statetul mode; if the section is marked as stateless, the ALGs will not be insert to as pecific for the section is marked and will be adding used to include in the section is marked and will be supported. This is used to select & display for the section is marked and will be supported. This is used to select & display for the section is marked and will be supported. This is used to select & display for the section is marked and will be section is marked and will be section as the section is marked and will be section as the section is marked and will be section as the section and the section is marked and will be section as the section and the section micro-segmentation policy for this application use the category Application on DFW rule table and add a new policy session and rules within it for each application. The following use cases employ present policy rules based on the different methodologies introduced earlier. Example 1 - Group Definition while the firewall policy configuration is shown in Table 5-5: Firewall Rule Table - Example 1 - Group Definition on DFW rules based on the different methodology to define policy rules. This example are identified in Table 5-5: Firewall Rule Table - Example 1 - Group Definition while the firewall policy configuration is shown in Table 5-6: Firewall Rule Table - Example 1 - Boroup APP-1P IP Members: 172.16.30.0/24 Table 5-5: Firewall Rule Table - Example 1 - Boroup APP-1P IP Members: 172.16.30.0/24 Table 5-5: Firewall Rule Table - Example 1 - Group Definition Service Action Applied To Any toro Web Any Group-APP-1P IP Members: 172.16.30.0/24 Table 5-5: Firewall Rule Table - Example 1 - Group Definition on the different methodology to define policy rule. This example uses the infrastruction are to force for the second on the provided in fraction Service Action Applied To Any toro Web Any Group-APP-1P IP Members is readicated to a does not fully leverage the infrastructic readicate on the policy rule. This example uses the infrastruction on being conclusted on the provided in Group-SEG-WEB Second on the provided in Group-SEG-WEB Second Secon SEG-APP Group-SEG-DB Block-Other Any and the construct fully be consecutive policy and the construct fully be consecuted by the first policy rule also uses the "Applied To" option to apply the policy rule also uses the "Applied To" before rules are pushed to date policy and the construct fully required when the policy rule also uses the "Applied To" option to apply the policy rule also uses the "Applied To" before rules are pushed to date policy rule also uses the "Applied To" before rules are pushed to date policy rule also uses the "Applied To" before rules are pushed to date policy rule also uses the "Applied To" before rules are pushed to date policy rule also uses the "Applied To" before rules are pushed to date policy rule also uses the "Applied To" before rules are pushed to date policy rule also uses the "Applied To" before rules are pushed to date policy rule also uses the "Applied To" before rules are pushed to date policy rule also uses the "Applied To" before rules are pushed to date policy rule also uses the "Applied To" before rules are pushed to date policy rule also uses the "Applied To" before rules are pushed to date policy rule also uses the "Applied To" before rules are pushed to date policy rule also uses the "Applied To" before rules are pushed to date policy rule also uses the "Applied To" before rules are pushed to date policy rule also uses are removed. This is mainly required when the policy is defined using grouped objects. This VM-to-IP table is maintained by NSX-T Control plane and populated by the IP discovery which is used to translate objects to IP before rules are pushed to date path. This is maintained by NSX-T Control plane and populated by the IP discovery mechanism. IP discovery mechanism of NM-to-IP table is maintained by NSX-T Control plane and populated by the IP discovery mechanism. IP discovery mechanism tor acertain the IP address of the control in the fuel of the given rule to be detervised to security point of the g network architecture. Service Insertion not only sends the traffic to other services for processing, Service manager so that update to the SI service manager. Thus, when a new VM is spun up which becomes a member of the new group, the NSX Manager will send that update to the SI service manager. Thus, when a new VM is spun up which becomes a member of the new group, the NSX Manager will send that update to the SI service managers. So, a group in NSX which is comprised on VMs which is comprised to the SI service managers. Additional Security Fatures NSX-T extends the security posture on the secure on the security posture o In NSX-T blacked workloads the low are to be only the low are to be NSX-T overlay backed networking from the network isolation perspective. This could apply to green field deployments of heapplication, and it will continue to work isolation, VLAN to NSX-T overlay backed networking. In summary, NSX-T Platform enforces micro-segmentation policies irrespective of network isolation, vLAN to NSX-T overlay backed networking. In summary, NSX-T Platform enforces micro-segmentation policies irrespective of network isolation, vLAN to no verlay backed networking. In summary, NSX-T Platform enforces micro-segmentation policies irrespective of network isolation, vLAN to NSX-T overlay backed networking. In summary, NSX-T Platform enforces micro-segmentation policies irrespective of network isolation, vLAN to no verlay backed networking. In summary, NSX-T overlay backed networking to not well application from VLAN to NSX-T overlay backed networking. S.9 Gateway firewall provides espective of network isolation from VLAN to NSX-T overlay backed networking. In summary, NSX-T Blatform enforces micro-segmentation policies irrespective of network isolation, and it will continue to work isolation policies irrespective of network isolation from VLAN to NSX-T overlay backed networking. In summary, NSX-T Platform enforces micro-segmentation policies irrespective of network isolation, and it will continue to work isolation, and it will continue to work isolation from VLAN to NSX-T overlay backed networking. In summary, NSX-T Platform enforces micro-segmentation policies irrespective of network isolation from VLAN to NSX-T overlay backed networking. In summary, NSX-T Platform enforces micro-segmentation policies irrespective as the policy of the particular provides is particular provides i Manager of the set of individual values in the individual values interval values interval values in the individual values interval values interval values interval values values interval values values interval values values interval values with imploited and the security bills with a labeled in the security bills with a lab continues to leverage distributed routing and firewalling capabilities native to the NSX-T. Figure 5-15: Tier-1 Gateway Firewall - Inter-tenant Gateway Firewall provides. This is applicable for the design where security compliance requirements mandate zones or groups of workloads be secured using NGFW, for example, DMZ or PCI zones or Multi-Tendent events in a big of the intervent of the service in a big of the intervent provides in a big of the intervent prov AV/AM agent inside the virtualized workload consuming a small amount of virtual CPU and memory, the resource costs can be noticeable and provide the same services using a Service Virtual Machine (SVM) that is installed on each host. These SVMs consume much less virtual CPU and memory overall than running agent also costs of the overall NDI deployment. The Guest Introspection platform allows the AV/AM partner to remove their agent from the virtual estimates of the overall than as envices using a Service Virtual Machine (SVM) that is installed on each host. These SVMs consume much less virtual CPU and memory overall than running agent also removes that processing tax from the virtual estimates of the overall VDI deployment. The Guest Introspection platform allows the AV/AM partner to removes that processing tax from the VDI, resulting in greater individual VDI performance. Many AV/AM partner to removes that processing tax from the VDI, resulting in greater individuel VDI, resulting in greater individuel VDI, resulting in greater individuel VDI performance. Many AV/AM partner to result of the AV/AM search the self tax for the result of the AV/AM partner to result of the AV/AM search the self tax for the result of the AV/AM search the self tax for the result of the AV/AM search the self tax for the result of the AV/AM search the self tax for the result of the AV/AM search tax for the result of the AV/AM search tax for the result of the AV/AM search tax for the result of the the res Exclude management components like vCenter Server, and project to avoid lockout, at least in the appropriate policy. This will enable simpler policy to avoid lockout, at least in the appropriate policy. This will enable simpler policy to avoid lockout, at least in the appropriate policy. This will enable simpler policy to avoid lockout, at least in the appropriate policy. This will enable simpler policy method log and rule are policy to avoid lockout, at least in the appropriate policy. This will enable simpler policy to avoid lockout, at least in the appropriate policy. This will enable simpler policy method log and rule are policy. This will enable simpler policy method log and rule are policy. This will enable simpler policy method log and rule are policy method log and rule are policy. This will enable simpler policy method log and rule are policy method log and rule are policy. This will enable simpler policy method log and rule are policy method log and rule are policy method log and rule are policy. This will enable simpler policy method log and rule are policy method log and rule are policy method log and rule are policy. This will enable simpler policy method log and rule are policy method log and rule are policy. This will enable simpler policy method log and rule are policy method log and rule are policy. This will enable simpler policy method log and rule are policy hardening guide and record nded configuration maximums.. application...) Use an explicit allow model; create explicit rules for allowed traffic and change DFW the default rule from "allow" to "drop". 5.11.1 A Practical Approach to Building Micro-Segmentation owners don't know very much about the applications and build security policies for each. Often times, applications and build security policies for each. Often times, applications within your data center and denying all other traffic by default. However, it is a big challenge to profile tens/hundreds of applications within your data center and build security policies for each. their application's details, which further complicates the process. This may take some time to profile your application and come up with a solution to be complete, one can start with basic outside in fencing approach to start defining broader security policies to enhancing the security policies To New Second Se group tor DNS and NIP servers with IP addresses of the respective services using (BOUPS created in step in radio c, in exclusion list, this section would need to further required protocols between the appropriate attribution. Note: If the manage and communication section would need to further respective services value to further application of the communication attempts. Figure 5-20: NSA-I Groups Example Destructs with logging envirous attribution for dimension would need to further respective services as formal and work for all VM ware products for all work and work for all work work and work for all work and work for all work work work and work for all work work work and work work an identify the direction of the second in other weights and in the second in the application is only solve and in the second in the application is only between the second in the application is only between the second in the application is only address the log in the original is only address the log in the formation. The second in the application is only address the log in the formation is only address the log in the formation. The second in the application is only address the log in the formation is only address the log in the formation. The second in the application is only address the log in the formation is only address the log in the formation. The second in the application is only address the log in the formation is only address the log in the formation. The second in the application is only address the log in the formation is only address the log in the formation. The second is address the log in the formation is only address the log in the formation. The second is address the log in the formation is only address the log in the formation is only address the log in the formation. The second is address the log in the formation is only address. The formation is only others. This accommodates application-specific maintenance windows, where required. Phase-6: Define Emergency policy, Kill Switch, in case of Security Event An emergency policy mainly leveraged for following use case and enforced on top of the firewall table: 1- To quarantine vulnerable or compromised workloads in order to protect other workloads. 2- May want to explicitly deny known bad actors by their IP Subnet based on GEO location or reputation. This policy is defined in Emergency policy, Kill Switch, in case of Security Event An emergency policy mainly leveraged for following use case and enforced on top of the firewall table: 1- To quarantine vulnerable or compromised workloads in order to protect other workloads belonging to group GRP-QUARANTINE. "GRP-QUARANTINE" is a group which matches all VM with tag equal to "QUARANTINE" is a group which matches all VM with tag equal to "QUARANTINE". (If quags the volte of the volte application workloads with the bench in the the servers and can transparently remove a failing server from the pool, redistributing to the other members: Figure 6-3: Load Balancing Offers Advanced load balancing Offers Advanced Application Load Balancing Offers Advanced Application High-availability. In the example below, the load balancing Offers Advanced Application Load Balancing Content target servers based on the URL of the requests received at the VIP: Figure 6-2: Load Balancing Offers Advanced Application Load Balancing Content target servers based on the URL of the requests received at the VIP: Figure 6-2: Load Balancing Offers Advanced Application Load Balancing Content target servers based on the URL of the requests received at the VIP: Figure 6-3: Load Balancing Offers Advanced Application Load Balancing Content target servers based on the URL of the requests received at the VIP: Figure 6-3: Load Balancing Offers Advanced Application Load Balancing Content target servers based on the URL of the requests received at the VIP: Figure 6-3: Load Balancing Content target servers based on the URL of the requests received at the VIP: Figure 6-3: Load Balancing Offers Advanced Application Load Balancing Content target servers based on the URL of the requests received at the VIP: Figure 6-3: Load Balancing Content target servers based on the URL of the requests received at the VIP: Figure 6-3: Load Balancing Content target servers based on the URL of the requests received at the VIP: Figure 6-3: Load Balancing Content target servers based on the URL of the requests received at the VIP: Figure 6-3: Load Balancing Content target servers based on the target servers based The between a balances of the balances between and the balances between

the load-balancer VIP) and service, it is instantiated on a Tier-1 gateway SR (Service Router). The drawback from this model is that, because the Tier-1 gateway now has a centralized component, East-West traffic for Segments behind different Tier-1 gateway SR (Service, it is instantiated on a Tier-1 gateway SR) and server traffic for Segments behind different Tier-1 gateway SR (Service Router). The drawback from this model is that, because the Tier-1 gateway SR (Service Router). The drawback from this model is that, because the Tier-1 gateway SR (Service Router). prince to server) use the same load balancer interface. In that case, LB-SNAT will be used to make sure that the traffic from the server will not see the oution leverages load-balancing scenario: a case where they are on different subnets. For both cases the solution leverages load-balancer. There are two variations over this one-arm load-balancing scenario: a case where they are on the same subnet and a case where they are on the same subnet and a case where they are on the same subnet and a case where they are on the same subnet in the traffic from the server will not see the same subnet in the design below, the clients and servers on the same subnet In the design below, the clients and servers on the same subnet In the design below, the clients and servers on the same subnet In the design below, the clients and servers on the same subnet In the design below, the clients and servers on the same subnet In the design below, the clients and servers on the same subnet In the design below, the clients and servers on the same subnet In the design below, the clients and servers on the same subnet In the design below. The centralized load-balancer service result in East-West traffic for Segments behind different Tier-1 gateway downlink. Figure 6-6: One-Arm Load Balancing with Clients and servers on the same subnet In the design below. rawback as for the inline model described in the previous part. 6.2.2.2 Load Balancer One-Arm attached to Segment In the design below, the blue Tier-1 gateway does not run any load-balancer. This way, several segments below the blue Tier-1 gateway can have their own dedicated load-balancer. Figure 6-7 Load Balancer One egment overlay This design allows for better horizontal scale, as an individual segment can have its own dedicated load-balancer service appliance(s). This flexibility in the assignment of load-balancer service appliance, in East-West traffic for Segments behind different Tier-1 SRs on several Edge nodes. Because the load-balancer service has its dedicated appliance, in East-West traffic for Segments behind different Tier-1 SRs on several Edge nodes. Because the load-balancer service has its dedicated appliance, in East-West traffic for Segments behind different Tier-1 SRs on several Edge nodes. There 1 One Arm attached to segment VLAN is reducible to physical VLAN segment vLAN. In this use additional details on how the load-balancer components are physically in the use of a segment vLAN is reducible to physical vLAN segment vLAN. In this use additional details This section provides additional details on how the load-balancer will help the reader optimize resource usage in their network. 6.3.1 Load-balancer high-availability The load-balancer high-availability The load-balancer high-availability The above diagram represents two Edge nodes hosting there additional details the segment vLAN is reducible to physical vLAN segments additional details on how the Edge high-availability (HA) model is based on periodic keep alive messages exchanged between each pair of Edges in an Edge rodes 2 go down, the standby green SR on Edge nodes 1, along with its associated load-balancer each. The Edge High Availability (HA) model is based on periodic keep alive messages exchanged between each pair of Edges in an Edge cluster. This keepalice protects against the loss of an Edge as a whole. In the above diagram, should Edge node 2 go down, the standby green SR on Edge node 2 go down, ala core, would become active immediately. There is a second messaging protocol between the Edges. This one Edge node 1 is detected, this mechanism can trigger a failover of the red Tier-1 SR from Edge node 2, without important to the standby load balancer: State Synchronize the following information to the standby load balancer: State Synchronize the following information to the standby load balancer: State Synchronize the following information to the standby load balancer: State Synchronize the following information to the standby load balancer: State Synchronize the following information to the standby load balancer: State Synchronize the following information to the standby load balancer information informat a be were LB1 reside. Monitor2 are implemented on the SR where LB1 reside. Monitor2 is also polling servers used by LB2, thus it is also implemented on the SR where LB2 is running. The Monitor2 example highlights the fact that a monitor service can be instantiated in several physical locations and that a given pool can be enstantiated in several physical locations and that a given pool can be monitored from different SRs. 6.3.3 Load-balancer Layer7 (L7) load balancing NSX-T LB offers Layer4 or Layer7 (L7) load balancing NSX-T LB offers Layer4 or Layer7 (L7) load balancing NSX-T LB offers Layer4 (L4) and Layer7 (L7) load balancing NSX-T LB offers Layer4 or Layer7 (L7) load balancing NSX-T LB offers Layer4 or Layer7 (L7) load balancing NSX-T LB offers Layer4 or Layer7 (L7) load balancing NSX-T LB offers Layer4 (L4) and Layer7 (L7) load balancing NSX-T LB offers Layer4 or Layer7 (L7) load balancing NSX-T LB offers Layer4 or Layer7 (L7) load balancing NSX-T LB offers Layer4 or Layer7 (L7) load balancing NSX-T LB offers Layer4 or Layer7 (L7) load balancing NSX-T LB offers Layer4 (L4) and Layer7 (L7) load balancing NSX-T LB offers Layer4 or Layer7 (L7) load balancing NSX-T LB offers Layer4 (L4) and Layer7 (L7) load balancing NSX-T LB offers Layer4 or Layer7 (L7) load balancing NSX-T LB offers Layer4 (L4) and Layer7 (L7) load balancing NSX-T LB offers Layer4 (L4) and Layer7 (L7) load balancing NSX-T LB offers Layer4 (L4) and Layer7 (L4) an lanced by the VIP and its connection is terminated by the VIP and here to sub-balance is a balance of the pool members. If needed is not be request is received then the load balance is a balance is a balance of the pool members. If needed is not be received then the load balance is a balan ncing. Figure 6-13: NSX-T L7 HTTPS Off-Load VIP HTTPS End-to-End SSL decrypts the HTTPS traffic at the V s the traffic in another HTTPS session to the pool members. It is the best security and LB flexibility: Security and performance, but with traffic decrypted does not decrypt the HTTPS traffic as the VIP and SSL connection is terminated on the pool members. It is the best security and performance, but with traffic decrypted twice. LB flexibility: all advanced configuration on HTTP traffic as the VIP and SSL connection is terminated on the pool members. It is the best security and performance, but with Security: traffic is available on the local protocol of the security and t ver, source LB-SNAT is required in this design, even if the traffic between the clients and the servers cannot apparently avoid the Tier-1 SR and DR are represented as distinct entities and hosted physically in different location in the network, clarifies the reason why source LB-SNAT is mandatory: Figure 6-19: Load Balancing VIP IP@ in Tier-1 Downlink Subnet One-arm model From a logical standpoint, the VIP of a virtual server belongs to the subnet of the downlink to subnet of the host where both client and servers are instantiated (note that, in order to simplify the representation, the DR on the Edge was omitted.) Figure 6-21: ded View Traffic from server to client would be switched directly by the Tier-1 DR without going through the load balancer on the SR if source LB-SNAT was in the Tier-1 gateway interface has the IP address 10.0.0.1, and a virtual server with VIP 10.0.0.6 has been configured on the load balancer. Figure 6-20: Load Ba ce LB-SNAT was not configured. This design is not in fact a true in-line deployment of the load-balancer and does require LB-SNAT. 6.3.5.2 Logical View The diagram below offers a possible physical representation of the same network, where the representation, the DR on the Edge was omitted.) Figure 6-21: Loa ing VIP IP@ in Tier-1 Downlink Subnet - Tier-1 Expanded View This representation makes it clear that because the VIP is not physically instantiated on the DR, even if it belongs to the subnet of the downlink of the Tier-1 gateway, some additional "plumbing" is needed in order to make such as the VIP is not physically instantiated on the DR, even if it belongs to the subnet of the downlink of the Tier-1 Expanded View This representation makes it clear that because the VIP is not physically instantiated on the DR, even if it belongs to the subnet of the downlink of the Tier-1 Expanded View This representation makes it clear that because the VIP is not physically instantiated on the DR, even if it belongs to the subnet of the downlink of the Tier-1 Expanded View This representation. Thus, NSX configures proxy-ARP on the DR to answer local request for the VIP is not physically instantiated on the DR, even if it belongs to the subnet of the downlink of the Tier-1 Expanded View This representation. with SR services (NAT and Firewall) Since NSX-T. Central components of NSX-T. Central concepts include: • Connectivity of management and control plane components of NSX-T. Central concepts include: • Connectivity of management and control plane components (NSX-T. Central concepts include: • Connectivity of management and control plane components of NSX-T. Central concepts include: • Connectivity of management and virtual Edge nodes: • both bare metal and virtual Edge nodes: • Component virtu this value, excluding overhead. The VM MTU – Typical deployment carries 1500 byte MTU for the guest VM. One can increase the MTU up to 8800 (a ballpark number to accommodate bridging and future header expansion) in case for improving the throughput of the VM. However, all non-TCP based traffic (UDP, RTP, ICMP etc.) and traffic that need to traverse firewall or services appliance, DMZ or Internet may not work properly thus it is advised to use caution while changing the VM MTU. However, replication VMs, backups or internal only ication can certainly benefit from increasing the VM MTU size on VMs, backups or internal only ication can certainly benefit from increasing the VM. However, replication VMs, backups or internal only ication can certainly benefit from increasing the VM MTU. However, replication VMs, backups or internal only ication can certainly benefit from increasing the VM. When the VM is it is advised to use caution while changing the VM MTU. However, replication VMs, backups or internal only ication can certainly benefit from increasing the VM. We will be throughput of the VM. However, all non-TCP based traffic (UDP, RTP, ICMP etc.) and traffic that need to traverse firewall or services applicance, DMZ or Internet may not work properly thus it is advised to use caution while changing the VM MTU. However, replication VMs, backups or internal only ication can certainly benefit from increasing the VM. However, all non-TCP based traffic (UDP, RTP, ICMP etc.) and traffic that need to traverse firewall or services applicance, DMZ or Internet may not work properly thus it is advised to use caution while changing the VM MTU. However, replication VMs, backups or internal only ication can certainly benefit from increasing the VM. However, replication VMs, backups or internal only ication concertainly benefit for the SUM and the Form applicance, DMZ or Internet may not work properly thus it is advised to use caution while changing the VM. However, replication VMs, backups or internal only ication concertain pre ast this value, excluding overhead. sample of a routed leaf-spin exclusion of lange of the second of the sec ment VLAN on a different rack as they lack L2 connectivity. In order to simplify the configuration, the same VLAN ID is however typically assigned consistently across rack for each category of traffic. Figure 7-2: Typical Layer 3 Design with Example of VLAN/Subnet details an example of VLAN/Subnet detailed recommendations on the NSX-T component specifics. For hypervisors as a standard VLAN backed port group; there is no need for colocation in the same subnet or VLAN. There are no host state dependencies or MTU encapsulation requirement as these components. The management rack hosting three NSX-T Manager appliances. Figure 7-3: ESXi Hypervisors in the Management Rack The ESXi management port group is configured with two uplinks using physical NICs "T1" and "P2" attached to different top of rack switches. The uplink teaming policy has no impact on NSX-T Manager operation, so it can be based on existing VSS/VDS policy. Figure 7-4: KVM Hypervisors in the Management Rack presents the same NSX-T Manager operation, so it can be based on existing VSS/VDS policy. Figure 7-4: KVM Hypervisors are configured on a NSX-T Manager operation, so it can be based on existing VSS/VDS policy. Figure 7-4: KVM Hypervisors in the Management Rack The KVM manage ent hypervisors are configured with a VDS/VSS plinks using physical NICs "P1" and "P2". The traffic is injected into a management VLAN configured in the physical infrastructure. Either active/standby is fine for the uplink team strategy for NSX T Manager since both provide redundancy; this example uses simplest connectivity model with active/standby is fine for the uplink team strategy for NSX T Management to make a strategy for NSX T Management VLAN configured in the physical infrastructure. Either active/standby is fine for the uplink team strategy for NSX T Manager since both provide redundancy; this example uses simplest connectivity model with active/standby is fine for the uplink team strategy for NSX T Management VLAN. fully operational, the cluster requires that a majority of NSX-T Manager Nodes (i.e., two out of three) be a fully operational, the cluster requires that a majority of NSX-T Manager Nodes (i.e., two out of three) be a and get of roles that define the type of tasks that node can implement. For optimal operation, it is critical to understand the availability requirement o ensure that the failure of a single host does not cause the loss of a majority of the cluster. It is recommended to spread the deployment of the NSX-T i and Linux Bridge on KVM. Deploying NSX mana ster. The cluster must have three nodes for norma anagement components on the software defined overlay requires elaborate considerations and thus beyond the so rmal operation; however, the cluster can operate with reduced capacity in the event of a single node failure. To b rate failure domains to ensure that a single failure does not cause the loss of a majority of the cluster. A failure domain at minimum should address the failure of a single host address the failure of a single host address the failure of a single host address the failure domain at minimum should address the failure of a single host address of a majority of the cluster. The second mended to spread the deployment of the NSX-T Manager Nodes (i.e., two out of three) be available. It is recommended to spread the deployment of the NSX-T Manager Nodes across separate hypervisors to ensure that the failure of a single host address the fail ver. For more information on how to create a VM-to-VM anti-affinity rule, refer to the VM ware documents on VM-to-NM and VM-to-host rules. For a vSphere HA functionality to ensure single NSX-T Manager so that VMs can be restarted on another host if the original functionality to ensure single NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervisor. Furthermore, NSX-T Manager node can recover during the loss of a hypervi Sphere Cluster or even under a single vCenter (s) that they are deployed to are loaded as a Compute Manager And in some cases, they may be spread across three vSphere cluster for all NSX-T Manager Nodes in a Manager And that the IP Connectivity Requirements between the nodes are met. Predominantly however, the most common placement of the NSX-T Manager Nodes in a number of factors relating to availability. Single vSphere cluster for all NSX-T Manager Nodes in a Manager Nodes are met. Predominantly however, the most common placement of the NSX-T Manager Nodes in a number of factors relating to availability. here cluster it is important to design that design that design that design that a store to make the many productive main available during protective main available during to the NSX-T Manager Nodes to remain available during to the NSX-T Manager Nodes to remain available during to the NSX-T Manager Nodes to remain available during to the NSX-T Manager Node should all here NSX Manager Nodes to remain available during to the NSX-T Manager Nodes to remain available during to the NSX-T Manager Node should all here NSX Manager Nodes to remain available during to the NSX-T Manager Nodes to remain available during to the NSX-T Manager Node should all here NSX Manager Nodes to remain available during to the NSX-T Manager Node should all here NSX Manager Nodes to remain available during to the NSX-T Manager Node should all here NSX Manager Nodes to remain available during to the NSX-T Manager Node should all here NSX Manager Nodes to remain available during to the NSX-T Manager Node should all here NSX Manager Nodes to remain available during to the NSX-T Manager Nodes to remain available during to the NSX-T Manager Node should all here NSX Manager Nodes to remain available during to the NSX-T Manager Node should all here NSX Manager Node should all here NSX Manager Node should all here NSX Manager Node should be put in place to prevent whenever possible two Edge Node VMs from running on the same host. During lifecycle events of the lost prior to maintenance or any NSX-T Manager Node should be independently put into maintenance or any NSX-T Manager Node off of the host prior to maintenance or any NSX-T Manager Node should be manually moved to a different host. If possible, a rack level or critical infrastructure to maintenance or any NSX-T Manager Node off of the host prior to maintenance or any NSX-T Manager Node off of the host prior to maintenance or any NSX-T Manager Node off of the host prior to maintenance or any NSX-T Manager Node off of the host prior to maintenance or any NSX-T Manager Node off of the host prio dependently put into maintenance mode moving any running NSX-T Manager Node off of the host prior to maintenance or any NSX-T Ma , HVAC, ToRs) should also be taken into account to protect this cluster from any single failure event taking down the entire cluster at once. In many cases this means spreading this cluster at once. In many cases this means spreading this cluster across multiple cabinets or racks and therefore connecting the NSX-T Manager Nodes are deployed on. Figure 7-5: Single vSphere Cluster that the NSX Manager Nodes are deployed on. Figure 7-5: Single vSphere Cluster 1:1 Data Store Single vSphere Cluster at once. In many cases this means spreading this cluster special week of the vSphere Cluster at once. In many cases this means spreading this cluster across multiple cabinets or racks and therefore connecting the NSX-T Manager Nodes are deployed on. Figure 7-5: Single vSphere Cluster at once. In many cases this means spreading this cluster special week of the vSphere Cluster across multiple cabinets or racks and therefore connecting the hosts in it to a diverse set of physical switches etc. NSX-T Manager Nodes are deployed on. Figure 7-5: Single vSphere Cluster that the NSX Manager Nodes are deployed on. Figure 7-5: Single vSphere Cluster across multiple cabinets or racks and therefore connecting the hosts in it to a diverse set of physical switches etc. NSX-T Manager Nodes are deployed on. Figure 7-5: Single vSphere Cluster the NSX Manager Nodes are deployed on. Figure 7-5: Single vSphere Cluster across multiple cabinets or racks and therefore connecting the hosts in it to a diverse set of physical switches etc. NSX-T Manager Nodes are deployed on the entire cluster the NSX Manager Nodes are deployed on the entire cluster the NSX Manager Nodes are deployed on the entire cluster the NSX Manager Nodes are deployed on the entire cluster the NSX-T Manager Nodes are deployed on the entire cluster the NSX-T Manager Nodes are deployed on the entire cluster the NSX-T Manager Nodes are deployed on the entire cluster the NSX-T Manager Nodes are deployed on the entit of the NSX-T Manager Nodes are deployed on the entire cluster the SAN as the storage technology When all NSX-T Manager Nodes are deployed into a single vSAN as a part of a HyperConverged Infrastructure for hosting Virtual Machines, ners, or even now network attached storage type objects as a single pool across the cluster. The availability of the resources associated with storage are governed by a few specific parameters including, Primary Levels of Failures to Tolerate (PFTT), Secondary Levels of Failures to Tolerate (SFTT), and Failure Tolerance Mode (FTM) (when only a single vSAN is the three vSAN is the three resources associated on the valiability of the ensure of hosts that participate in that data store and in turn the vSphere Cluster is usually required. When hosting all of the NSX Manager Nodes in an NSX Manager Cluster is usually required. When hosting all of the NSX-T Management and control Planes: At a minimum, the vSphere Cluster is usually required with as configured with an FTT with the sonage are on the valiability of the NSX-T Management and Control Planes: At a minimum, the vSphere Cluster is usually required with an FTT with the sonage are on the valiability of the NSX-T Management and Control Planes: At a minimum, the vSphere Cluster should be configured with an FTT with the sonage are on the valiability of the NSX-T Management and Control Planes: At a minimum, the vSphere Cluster should be configured with an FTT with the valiability of the valiability of the NSX-T Management and Control Planes: At a minimum, the vSphere Cluster should be configured with an FTT with the valiability of the valiability of the NSX-T Management and Control Planes: At a minimum, the vSphere Cluster should be configured with an FTT with the valiability of the valiability of the NSX-T Management and Control Planes: At a minimum, the vSphere Cluster should be configured with an FTT with the valiability of the NSX-T Management and Control Planes: At a minimum, the vSphere Cluster should b and an FTM of Raid1 This will dictate that for each object associated with the NSX-T Manager Node, a witness, two copies of the data (or component) are available even if two failures occurring without impacting the integrity of the data (or component) are available even if two failures at least five (5) hosts in the vSphere Cluster. ToR and Cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hosts in the vSphere Cluster. ToR and cabinet Level Failures at least five (5) hos gh leveraging VSAN's PFTT capability commonly referred to as Failure Domains or VSAN Stretched Clusters and leveraging a Witness VM runni Appliances. When workload is spread across multiple cabinets or ToRs, it is also important to potentially set Host affinities for workloads to bette scenarios, NSX-T Manager Nodes will be spread out across multiple cabinets which will also require IP mobility of the IP Addre e storage and repopulate the objects on the remaining hosts in the vSphere Cluster. Figure 7-6: Single vSphere Cluster Single V ively removed from service, that they vacate the ere Cluster Single VSA Data Store Placement of NSX Manager Nodes Across Multiple vSphere Clusters. This type of design tends to be come apparent when a single vSphere cluster is unable to provide the resiliency or advantageous to place the three NSX Manager Nodes across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is unable to provide the resiliency or advantageous to place the three NSX Manager Nodes across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed across multiple facilities or computer is preferred to be deployed ac e or other underlying infrastructure is required to be diverse. In this scenario: Each vCenter that is ho ager inside of the first NSX Manager that is deployed. If the same IP space is not available to each vSphere Cl . IP Addresses in different subnets will need to be used as well as a load balancer as explained in section 7.2.3 below. If VSAN is used as part of this design, it is recommended to avoid using HCI Mesh and use the local VSAN data store presented to each vSphere for the NSX Manager And the volume of the standard of the stan ances deployed and allows greater is the control plane by putting all the control plane by putting the manager group. Similarly, it creates the control plane by putting the manager group. Similarly, it creates the manager group. Similarly, it creates the control plane by putting all the control plane by putting the manager group. Similarly, it creates the manager appliance and Communication NSX-T Manager appliance and shared is distributed and shared in the service group. Similarly, it creates the manager group. Similarly, it creates other service groups as needed. prion. The first one is the external systems and user access. Many different end points (such as HTTP, vRA, Terraform, Network Container Plugin, custom automation modules) can con SX-T components were described chapter 2. The controller availability models remain majority based requiring all three nodes to be available for normal operations. However, starting trollers and transport node). The controller communication to transport node is done via controller role (element) within the NSX-T appliance n fferent configuration modes available for northbound access to the NSX-T Manager cluster. Default deployment (each node uniquely sume NSX-T Manager from northbound via an IP address. It's is a single point of entry (using RESTful API - GUI internally makes and API call). Second is comm Cluster VIP based deployment Default Cand the simplest option, with the least number of IP addresses consumed) is to deploy a 3-node cluster without any additional configuration. With the least number of IP addresses consumed) is to deploy a 3-node cluster without any additional configuration. With the least number of IP addresses consumed) is to deploy a 3-node cluster without any additional configuration. With the least number of IP addresses consumed) is to deploy a 3-node cluster without any additional configuration. With the least number of IP addresses consumed) is to deploy a 3-node cluster without any additional configuration. With the least number of IP addresses consumed) is to deploy a 3-node cluster without any additional configuration. With the least number of IP addresses consumed) is to deploy a 3-node cluster without any additional configuration. With the least number of IP addresses consumed) is to deploy a 3-node cluster without any additional configuration. With the least number of IP addresses consumed) is to deploy a 3-node cluster without any additional configuration. With the least number of IP addresses consumed) is to deploy a 3-node cluster without any additional configuration. With the least number of IP addresses consumed) is to deploy a 3-node cluster without any additional configuration. With the least number of IP addresses consumed is accessible via distinct IP addresses consumed is accessible via disti ent IP address (FODN). However, in case of the node failure the system using that node must externally intervene to noith to another available node. For an example, if vRA or API scrint or undate the FODN of node A fails, there has to be some manual intervention to make the scrint continues to work, either you change the FODN of node A fails. wity between all the nodes, this mode will work. Cluster VIP based deployment The second deployment Since it is a single FQDN name available to all end points, all the GUI and API requests are accessed th nt option is based on simple active/standbys redundancy model, in which one has to configure a virtual IP address on the management cluster. Cluster VIP configuration option provid through single node owning the VIP as shown in Figure 7-9: NSX Manager Appliances Availability with Cluster VIP. Essentially, it is a simple availability model, which is far better def he virtual IP address on the cluster itself. This virtual IP (like VRRP/HSRP) provides redundancy of accessing the cluster via single FQDN. In other words: the entire northbound access to the NSX-T ntion is not required, and availability of NSX-T Manager role is improved from external restore option to full in-line availability which did not exist in previous releases. Cluster virtual IP address is an II ting among the cluster nodes. One of the cluster nodes is assigned as the owner of the cluster VIP feature uses gratuitous ARP to update the mac-address and the ARP table. Thus, it is mandatory to have all nodes in the cluster VIP feature uses gratuitous ARP to update the mac-address and the ARP table. Thus, it is mandatory to have all nodes in the cluster VIP feature uses gratuitous ARP to update the mac-address and the ARP table. Thus, it is mandatory to have all nodes in the cluster VIP. If case of failure, a new owner will be assigned by the system. Since the cluster NIP to work. From the physical topology perspective, the nodes placement can vary. For the L2 can be in different rack or the same as long they have L2 adjacency. For the L3 topology all nodes must be in the same rack assuming VLAN/subnet is confined to a rack. Alternatively, one can cross-connect the host to two distinct ToRs on two different rack to be rack resilient. Figure 7-9: NSX Manager Appliances Availability with Cluster VIP The NSX-T Manager Availability has improved by an order of the magnitude from a previous option; however, it is important to clear the distinction between node availability vs load-balancing. In th d GUI requests go to one single node, one cannot achieve a load-balancing of GUI and API sessions. In addition, the existing sessions established on a failed node, will need to re-authenticated and re-established at new owner of the cluster VIP. The availability is also designed to leverage critical failure of certain services relevant to NSX-T Mar ansport node is done via IP address assigned to each manager node. The cluster VIP is the preferred and recommended option for achieving high availability with NSX-T Manager appliancer will go through the VIP on the load balancer will and API access to the manager node. The third deployment option for achieving high availability with NSX-T Manager appliance nodes as the physical servers in the server pool. Then the UI and API access to the management cluster will go through the VIP on the load balancer will appliance nodes. External load balancer appliance nodes as the physical servers in the server pool. Then the UI and API access to the manager nodes as the physical servers in the server pool. option is that not only the endpoint access the NSX-T Manager nodes will have load-balancing but also the cluster management access is highly available via a single IP address. The external load-balancer option also makes the deployment of NSX-T manager nodes independent of underlying physical topology. Additionally, one can distribute nodes to more than one rack to achieve rack redundancy (in L2 topology it will be distinct subnet per rack). res an external load balancer and configuration alancer. In this option only the northbound end ation complexity based on load-balancer models. The make and model of load-balancer are left to user preference however one can also use NSX-T Datacenter portfolio Figure 7-10: NSX Manager Appliances with External Load Balancer shows simple source included as part of NSX-T Datacenter portfolio Figure 7-10: NSX Manager Appliances with External Load Balancer shows simple source included as part of NSX-T Datacenter portfolio Figure 7-10: NSX Manager Appliances with External Load Balancer shows simple source included as part of NSX-T Datacenter portfolio Figure 7-10: NSX Manager Appliances with External Load Balancer shows simple source included as part of NSX-T Datacenter portfolio Figure 7-10: NSX Manager Appliances with external Load Balancer shows simple source included as part of NSX-T Datacenter portfolio Figure 7-10: NSX Manager Appliances with external Load Balancer shows simple source included as part of NSX-T Datacenter portfolio Figure 7-10: NSX Manager Appliances with external Load Balancer shows simple source included as part of NSX-T Datacenter portfolio Figure 7-10: NSX Manager Appliances with external Load Balancer shows simple source included as part of NSX-T Datacenter portfolio Figure 7-10: NSX Manager Appliances with external Load Balancer shows simple source included as part of NSX-T Datacenter portfolio Figure 7-10: NSX Manager Appliances with external Load Balancer shows simple source included as part of NSX-T Datacenter portfolio Figure 7-10: NSX Manager Appliances with external Load Balancer shows simple source included as part of NSX-T Datacenter portfolio Figure 7-10: NSX Manager Appliances with external Load Balancer shows simple source included as part of NSX-T Datacenter portfolio Figure 7-10: NSX Manager Appliances with external Load Balancer shows simple source included as part of NSX-T Datacenter portfolio Figure 7-10: NSX Manager Appliances with external Load Balancer shows simple source included as part of NSX-T Datacenter portfolio Figure 7-10: NSX Manager Appliance as part of NS son above Figure 7-10: NSX Manager Appliances with External Load Balancer represent VIP with LB persistent configuration for both browser (GUI) and API based access. While one can conceive advanced load-balancing schema in which dedicated VIP for browser access with LB persistent while other view of the system. It is for this reason it is highly recommended to first very statistic s abilities can found i om their respective vendors. A specific note for the KVM compute hypervisor: NSX uses a single IP stack for management and overlay traffic on KVM hosts. Because of this, both management and overlay interfaces share the same default gateway. This can be an issue if those two kinds of traffic are sent on different VLANs. In this case, it is necessary to introduce more specific static routes for the overlay remote networks pointing to a next hop gateway specific ralized Traffic Engineering and Capability with NSX NSX-T offers choices with management of infrastructure and guest VM traffic (overlay or VLAN) through flexibility of uplink profiles and teaming type as described in chapter utilizes configuration choices and capability based on requirements and best practices prevalent in existing data-center deployments. Typically, traffic management carries two overarching goals while expecting availability, namely: Optimization of all available physical NICs- In this choice, al 11Cs. Assumption is made that by providing and that by providing back traffic type. One example of such traffic type is only carried on a specific pNIC, it may be necessary to enable traffic type. Additionally, it allows deterministic Traffic type. One example of such traffic is VSAN traffic. The type of traffic type of traffic type of traffic type of traffic type. One example of such traffic type of traffic type. One example of such traffic type of traffic type. One example of such traffic type of traffic type. Additionally, it allows deterministic Traffic type. Additionally, it allows deterministic traffic type. Additionally, it allows deterministic traffic type of the teaming type offered in NSX-T that enables that by providing the type of the teaming type offered in NSX-T that enables are specific pNIC. In this choice, certain traffic type. Additionally, it allows deterministic Traffic type. Additionally, it allows deterministic traffic type. Additionally, it allows deterministic type of the teaming type offered in NSX-T that enables are specific pNIC. In this choice, certain traffic type. Additionally, it allows deterministic traffic type. Additionally, it allows deterministic traffic type. Additionally, it allows deterministic traffic type are been type of traffic type are been type of the type of type of the type of type of the type of type of type of the type of type In the second se nted as DVPGs (now onward called NSX DVPG) in vCenter. Third party scripts that had not been retrofitted for opaque networks can now work natively with NSX. 7.3.1.2 Impact on ESXi host design As we have seen earlier in this chapter, the traffic in/out an ESXi host can be classified in two broad categories: Infrastructure traffic. Any traffic that is originating from the ESXi host and its functionality to support application, storage, availability and management. This traffic is typically initiated and received on VMkernel traffic for management, vMotion, storage, high availability etc. VM and/or application traffic: This is the traffic between virtual machines running on the host. This traffic might be local to the hypervisor but can also extend to VMs on remote hosts. NSX is all about providing advanced networking and security features for VM traffic. Until now, when the administrator introduced NSX, to any one to the hypervisor but can also extend to VMs on remote hosts. NSX is all about providing advanced networking and security features for VM traffic long with the existing virtual switches cannot share physical uplinks. The administrator is thus left with two main options: Deploy an N-VDS for VM traffic. This solution is very easy to deploy as it does not impact the current host operations. However, it requires separate uplinks for the N-VDS, meaning addition is very easy to deploy as it does not impact the current host operations. However, it requires separate uplinks for the N-VDS, meaning addition is very easy to deploy as it does not impact the current host operations. oduced NSX, they needed to deploy a new N-VDS virtual switch on their hosts. The ESXi platform can run multiple separate virtual switches , meaning additional connectivity to the physical infrastructure. The second, an efficient option is to consolidate both infrastructure and VM traffic o ing this model is more complex as it implies a virtual switch migration: VMKernel interfaces and physical uplinks need to be moved from VSS/VDS to the N-VDS. When the hosts only have two high-speed uplinks, which is increasingly the case with modern servers, migrating to a single N-VDS becomes mandatory to maintain uplink need to be moved from VSS/VDS to the N-VDS. When the hosts only have two high-speed uplinks, which is increasingly the case with modern servers, migrating to a single N-VDS becomes mandatory to the first option, and a two pNIC design for the The second option of NSX on VDS changes all this. NSX can be installed on a VDS without incurring migration of infratructure traffic VMkernel, making the second option just as simple as the first one. The use-cases will still cover a four pNICs design, for those who plan on keeping the N-VDS for now, and for the cases when multiple as the first one. The use-cases will still cover a four pNICs design, for those who plan on keeping the N-VDS for now, and for the cases when multiple as the first one. The use-cases will still cover a four pNICs design, for those who plan on keeping the N-VDS for now, and for the cases when multiple as the first one. The use-cases will still cover a four pNICs design, for those who plan on keeping the N-VDS for now. The N-VDS for now NSX on VDS, you need NSX-T 3.0 or later and a VDS version 7.0 or later. For a greenfield deployment that meet those requirements, we recommend starting with NSX on VDS, or for those with a new install that cannot meet the version requirements, the version requirements, the version neet the version requirements and keep VMkernel on NSX unless one has 4 pNICs configurations. There is almost no functionality difference between N-VDS and VDS with NSX. In fact, one could even mix VDS and VDS with NSX in the same NSX network. For a given host with more than 2 pNICs, coexistence of all NSX virtual switch (not the third party) allowed except N-VDS and VDS with NSX in the same NSX network. For a given host with more than 2 pNICs, coexistence of all NSX virtual switch (not the third party) allowed except N-VDS and VDS with NSX in the same NSX network. For a given host with more than 2 pNICs, coexistence of all NSX virtual switch (not the third party) allowed except N-VDS and VDS with NSX in the same NSX network. For a given host with more than 2 pNICs, coexistence of all NSX virtual switch (not the third party) allowed except N-VDS and VDS with NSX in the same NSX network. For a given host with more than 2 pNICs, coexistence of all NSX virtual switch (not the thi duce new compute cluster or vCenter within the brownfield deployment, for which the recommendation is to deploy VDS with NSX with properly supported software on compute and NSX. In this case VMkernel can remain on DVPG. The goal is to eventually convert tool as a voluble in the complete failed of the figure below depicts a case of single VDS with NSX which is logically similar to first one, where only difference is representation in Control for the figure represent a challenge operation in Control for the f mption; however, future releases shall make this identification easier with unique names. Typically, it is a good practice to invoke a single VDS per compute domain and thus have a consistent view and operational consistency of the VM connectivity. However, there are cases where single VDS invocation may not be ideal from separation of workload for security, automation, storage policy, NIOC control and provisioning boundary. Thus, it is acceptable to have a multiple VDS per giver tails of these differences and additional considerations are documented with following KB articles Co-existence with existing NSX, KVM and New vSphere Clusters In practical deployment, where one has existing NSX-T deployed with N-VDS (ESXi) or OVS (KVM). The core realization of consistent networking and security does not change with advent of VDS with NSX. The Figure 7-12: Multi-domain compute co-existence describe such configuration. Of course, for the VDS with NSX PG port for a VM connectivity. Figure 7-12: Multi-domain compute co-existence The key concept here is that NSX abstract the connectivity and security as segment. This segment is represented via various realization like NSX DVPG in VDS. Regardless of the underlying switch DFW can be realized either on VLAN or overlay however only with NSX. DVPG and not via vSphere DVPG. 7.3.2 ESXi-Based Compute Hypervisor to VDS and the automation that relies on the underlying ass targets typical enterprises deployments deploying compute hypervisors with the following parameters: Two pNICs All host traffic (VM and infrastructure traffic) shares the common NICs Each host traffic type has a dedicated IP subnet and VLAN The teaming mode offers a choice in the availability and traffic type has a dedicated IP subnet and VLAN The teaming mode design for the ESXi hypervisor - failover order and load balanced source. In this section only a two-pNIC design is shown, however base design principle remains the ure 7-13: ESXi Compute Rack Failover Order Teaming Policy, a single virtual VDS or N-VDS is used with a 2 pNICs design and carries both infrastructure and VM traffic. Physical NICs "P1" and "P2" are attached to different top of rack switches. The teaming policy selected is failover order active/standby; "Uplink1" is active while "Uplink2" is standby. If the virtual switch is an N and "P2" are attached to different top of rack switches. The teaming policy selected is failover order active/standby; "Uplink1" is active while "Uplink2" is standby. If the virtual switch is a N and "P2" are attached to different top of rack switches. The teaming policy selected is failover order active/standby; "Uplink1" is active while "Uplink2" is standby. If the virtual switch is a N and "P2" are attached to different top of rack switches. The teaming policy selected is failover order active/standby; "Uplink1" is active while "Uplink2" is standby. If the virtual switch is a NDS, only NSX DVPG traffic will follow the virtual switch is a VDS, only NSX DVPG traffic will follow the NSX teaming policy. The infrastructure traffic will follow the teaming policy. The top-of-rack switches are configured with a first hop redundancy providing an active default gateway for all the VLANs on "ToR-Left". The VMs are, for The full traffic on the basis for a simple configured in NSX by Score and who basis and the expense of a single teaming policy. If the virtual switch is a VDS, only NSX by Score and who basis are configured in the instance of a single teaming policy. The infrastructure traffic are following a teaming policy. The infrastructure and simple traffic are following a teaming policy. The infrastructure and simple traffic are following a teaming policy. The infrastructure and simple traffic are following a teaming policy. The infrastructure and simple traffic are following a teaming policy. The infrastructure and simple traffic are following a teaming policy. The infrastructure and simple traffic are following a teaming policy. The infrastructure and simple traffic are following a teaming policy. The policy are policy and the redundance protocol (e.g. HSKP, VKKP) providing an active used in the view of a single teaming policy. The infrastructure traffic are following and the redundance protocol (e.g. HSKP, VKKP) providing and the redundance protocol (e.g. HSKP, VKKP) providing and the redundance protocol (e.g. HSKP, VKKP) providing and active used in their respective VDS standard DVPGs configured in their respective VDS standard DVPGs configured in vertice and simple traffic are following and the redundance protocol (e.g. HSKP, VKKP) providing and active used in the vertice and simple traffic are following and the redundance protocol (e.g. HSKP, VKKP) providing and active used in the vertice and simple traffic are following at teaming policy. The other traffic are following at teaming policy. The other traffic are following at teaming policy at the traffic are following at teaming policy putting P1 as active. When the view of a single teaming policy putting P2 as active. When the view of a single teaming policy putting P2 as active. When the view of a single teaming policy putting P2 as active. When the view of a single teaming policy putting P2 as active. When the view of a single teaming policy putting P2 as active. ng policies: one with P1 active, P2 standby, and the other with P1 standby, P2 active. Then, individual traffic type can be assigned a preferred path by mapping it to either teaming policy putting P1 as active. When the virtual traffic are following a teaming policy putting P2 as active. When the virtual traffic are following a teaming policy putting P2 as active. When the virtual traffic are following a teaming policy putting P2 as active. When the virtual traffic are following a teaming policy putting P2 as active. When the virtual traffic are following a teaming policy putting P2 as active. When the virtual traffic are following a teaming policy putting P2 as active. ame, and thus called "named" treaming policies). The above design can thus be achieved with a default teaming policy (P2 active/P1 standby) and an additional named teamin ve & P2 standby, while the management DVPG will be configured for P2 active & P1 standby. To limit interlink usage, the ToR switches are configured with a first hop redun it in a first hop redundancy protocol (FHRP), providing an active default gateway for storage and vMotion traffic on "ToR-Left", management and overlay traffic on "ToR-Right". The VMs are attached to segments defined on the NVDS, nts follow the same default teaming policy by default. VLAN segments can hove by DVPGs for infrastructure traffic need to be configured individually: storage a way set to the logical interface of their attached Tier-1 gateway. Use of multiple teaming policies allows utilization of all available pNICs while maintaining deterministic traffic management. This is a better and recommended approach when utilizing "failover mode" teaming for all traffic. 7.3.2.2 Load Balance Source Teaming Mode NSX-T supports two source teaming policies: load balancing based on source port and load balancing based on source mac address. Those are the exact equivalent to the source teaming policies available of The second balancing based on source made address. These are the exact equivalent to the source teaming policies available on source made address. These are the exact equivalent to the source teaming policies available on source made address. These are the exact equivalent to the source teaming policies available on source made address. These are the exact equivalent to the source teaming policies available on source made address. These are the exact equivalent to the source teaming policies available on source made address. These are the exact equivalent to the source teaming policies available on VDS and N-VDS. With this kind of policy, potentially both uplinks are utilized based on the hash value generated from the source teaming policies available on VDS. With this kind of policy, potentially both uplinks are utilized based on the hash value generated from the source teaming policy is the designation of first hop redundancy protocol (FHRP) redundancy protocol (FHRP) redundancy protocol (FHRP) redundancy protocol (FHRP) distribution will be neffic. Solid traffic solid traffi designation of first hop redundancy protocol (FHRP) redundancy. Since all uplinks are in use, FHRP can be used to better distribute different types of traffic, helping reduce traffic across the inter-switch link. As the teaming and overlay traffic on "ToR-Right". The VMs are attached to segments defined in NSX, with the default gateway set to the logical interface of their Tier-1 gateway. Figure 7-15: ESXi Compute Rack Load Balanced Source Team relation for the source function of the sourc stion. The ToR switches are configured with an FHRP, providing an active default gateway for storage and vMotion traffic on "ToR-Left" nagement and overlay traffic on stic bandwidth and failover, while VM traffic use some "load balance source" teaming policy, spreading VM traffic across both pNICs. On a host running NSX with an N-VDS, the default teaming policy will have to be configured for "load balance source", as it's the only policy that overlay traffic follows. Then, individual VLAN segments can be mapped to named teaming policy will have to be configured for "load balance source", as it's the only policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source", as it's the only policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be configured for "load balance source" teaming policy will have to be conf tended to use one of the "load balanced source" teaming policies as they're the only ones allowing overlay traffic on multiple active uplinks and thus provide better throughput in/out of the host for VM traffic. 7.3.2.3 LAG based traffic distribution An nded because it's vendor dependent and typically involves significant vendor-specific limitations that VM ware has not validated. This introduces troubleshooting complexity and potential support coordination challenges across multiple vendors. However, the one of the "load balanced" to be a support coordination challenges across multiple vendors. However, the one of the "load balanced" to be a support coordination challenges across multiple vendors. However, the one of the "load balanced" teaming policies as they're the one of the "load balanced" ence, one can select a type of traffic management as desired for all the infrastructure traffic. However, for the overlay traffic, it is highly recommended to use one of the "load balanced source" team forming a single logical LAG, based on some multi-chassis link aggregation (MLAG, VPC etc.) Relying on this kind of technology is not recommended because it's vendor dependent and typically inv traffic will follow the individual teaming policies configured on their DVPGs in vCenter. Based on rec ribute traffic is via using LAG. In order to keep ToR redundancy, this scenario would require the ESXi he nent of compute may carry this type of teaming and often customer operational model has accepted the risk and knowledge set to operationalize LAG ba sed teaming. For those existing deployment, one can adopt LAG based teaming mode, for compute only workload. In other words, if the compute host is carrying edge VMs (for North-South traffic then its highly recommended to decouple the edge and compute with either dedicated edge hosts or edge and management. Please refer to a ESXi-Based Compute Hypervisor with Point of the consumption by the different teaming of point and the point of the consumption by the different teaming of point of the consumption by the different teaming of the consumption by the dinferent t sed disadvantage of mixing compute and edge VM further below in this chapter, 7,3,3 cy, and the fact that NSX is deployed on its dedicated virtual switch ensured that no misconfiguration could ever lead to VM traffic being sent on the uplinks dedicated to infrastructure traffic, owned by a diffe pNICs - VDS and NSX virtual switch The VDS is configured with pNICs "P1" and "P2". And each port group is configured with different pNICs in active/standby to use both pNICs. However, the choice of teaming mode on VDS is left up to user or existing imple ing NSX owns pNICs "P3" and "P4". To offer usage of both pNICs, N-VDS is configured in load balance source tea ming mode, as described in the previous section. Each type of host traffic has dedicated IP subnets and VLANs. To limit interlink usage, the ToR switch an FHRP, providing an active default gateway for storage and vMotion traffic on "ToR-Left", man : ESXi Compute Rack 4 pNICs - VDS and NSX virtual switch You can achieve this configuration b ment and overlay traffic on "ToR-Right". When all pNICs are up, only some overlay traffic will cross the inter switch link. The model in Figure 7-16: ESXi Compute Rack 4 pNICs - VDS and NSX virtual switch still makes sense when run mply mapping the 4 uplinks of the host to 4 uplinks on the VDS. Then, install NSX using an uplink profile that maps its uplinks (Uplink1/Uplink2 in the diagram) to the VDS uplinks P3 and P4. This model still benefits from the simple, no ning NSX on N-VDS. However, now that we can deploy NSX directly on a VDS, the equivalent functionality can be easily achieved with a single VDS running NSX and owning the four uplinks, as re on-disruptive installation of NSX. At the same time, the NSX component can only work with the 2 uplinks mapped to the uplink profile. This means that VM traffic can never flow on P1/P2. The final el is that the administrator can manage a single virtual switch and if allows flexibility of adding additional uplinks for overlay or infrastructure traffic. 7.3.3.2 Multiple virtual switches as a requirement Certain scenarios still call for multiple virtual switches on a host. For example: Allows compliance-based topology e.g. PCI, HIPPA etc., which of but not always necessitate separate and dedicated infrastructure components (e.g. pNIC, operational controls etc.) Build a cloud provider model in which internal or external facing ute Rack 4 pNICs- Two N-VDS, each virtual switch is built to serve specific topology or provide separation of traffic based on enterprise require es to be on separate virtual switches. There is a specific use case for NFV (Network Function Virtualization) where two pNICs is dedicated to standard virtual switch for overlay and other two pNICs for "enhanced mode" virtual switch. The "enhanced mode" is not discussed here. Please refer to VMware NFV do ructure traffic will be carried on the first virtual switch. If this is an N-VDS, it will re ltiple overlay for separation of traffic, though TEP IP of both overlays must be in the same VLAN/su vely used for infrastructure traffic and remaining two pNICs for overlay VM traffic. This allows dedicated bandwidth for overlay application traffic. One can select the appropriate teaming mode as discussed in above two pNICs design as appropriate. 2) First two pNICs are dedicated "VLAN only" ubnet albeit different transport zones 4) Building regulato Building DMZ type isolation Both virtual switches running NSX must attach to different transport zones. See detail in section Segments and Tran ge, etc. Physical NICs "P1" and "P2" are attached to different top of rack switches. The teaming option ing an active default gateway for all the VLANs on "ToR-Left". The VMs are attached to segments/logical switches defined VDS Mqt and Storage ports And IP addresses for those ports have to be created outside of NSX-T preparation. Figure 7-21 n the N-VDS, with the default gateway set to the logical interface of the distributed Tier-1 logical router instance. Note about N-VDS ports and bridge: NSX-T ation Mut and Storage IP addresses 7.4 Edge Node and Services Design Edge nodes are available in two form factors - VM and hare metal server. While both form factors offer the same functionality, their physical infrastructure of nent of three different types of IP networks for specific purposes: Mai gement - Accessing and controlling the Edge node Overlay (TEP) - Creating tunnels with peer transport nodes External (N-S) - Peering with the physical networking infrastructure to provi the NSX-T virtual components and the external network Edge nodes provide a pool of capacity for running ce ding rather than related to the Edge node itself. The Edge node connectivity options discussed below are indep wed in active/standby mode. The status of active or standby mode is within the contex resources considerations 7.4.1 Design Considerations with Bridging The chapter 3 ease up to version 2.5 New design recommendation starting with NSX-T release 2.5 Edge services and resources co Bridge on a VM form factor Edge The Edge Bridge is available on both Edge form factors - bare metal or Virtual Machine (VM) The use of the Bridge in the bare metal form factor is relatively straightforward: the bridged traffic is sent on the uplinks of the N-VDS selected by VLAN transport zone specified on the Bridge Profile ction bridging capability covers the basic functionality and availability model requirements. The next section covers bridging design. The respective topology also covers adding bridging into the mix and its implications. 7.4.1.1 rtant to remember that the Edge Bridge will end up sou ng on a VM form factor of the Edge. 7.4.1.1.1 Edge VM vNIC Configuration Requirement with Bridging For the VM form factor, it is imp essary on the physical infrastructure where the bare metal Edge attaches. This section is go rcing traffic from several different mac addresses on its VLAN vNIC. This means, that the uplink vNIC must be connected to a DVPG port group allowing: Forged transmit Mac lea er UI.) Refer VLAN TAG Requirements in chapter 4.8.2.2 for more information. 7.4.1.1.3 g is not possible, the promiscuous can be configured instead at the expense of degraded he data path on the host. The Edge HA mechanism is exchanging BFD hellos over the tunr Cluster, As a result, overlay traffic is protected against failure in the data path. In Figure 7-22: Dedicated Edge VM would be considered as failed by Edge HA and another Edge would take over the services it was running (including, but not limited to, the bridge service.) 7.4.1.2 Redundant VLAN connectivity The Edge Bridge HA mechanism does not protect em in the VLAN infrastructure beyond the Edge physical uplink. Figure 7-23: Physical bridging infrastructure must be redundant In the above scenario, the failure of the uplink of Edge 1 to physical switches S1 and S3 (as represented in the diagram) would have to be recovered in the Edge Bridge en Edge 2 would become active. However, the failure of the uplink of Edge 1 to physical switches S1 and S3 (as represented in the diagram) would have to be recovered in the between physical switches S1 and S3 (as represented in the diagram) would have to be recovered in the diagram would have to be recovered in the between physical switches S1 and S3 (as represented in the diagram) would have to be recovered in the emptive model allows making sure that, when the system is fully operational, a Bridge is using a specified uplink for its VLAN traffic. This is required for scaling out the solution, precisely distributing the load across several Edge Bridges and getting more aggregate bandwidth betwee ng Segment/VLAN load balancing. The non-preempting the currently active backup.) The drawback is that, after a recovered failure, the bridged traffic remains polarized on one Edge, even if there was several Bridge Profiles defined on this pair of Edges for Segment/VLAN load balancing. Also note that, up to NSX-T release 2.5, a fa Performance: scaling up vs. scaling out The performance of the Edge Bridge directly depends on the Edge running it. NSX thus offers the option to scale up the Edge Bridge from a small form factor Edge VM running several other s design, one cannot assume that both Edges will be leveraged for bridged traffic, even when they are both available and several Bridge Profiles are used for Segment/VLAN load ba sible, as a complement to or instead of scaling up. By creating two separate Bridge Profiles, alternating active and backup Edge in the configuration, the user can easily make sure that two Edge no re 7-24: Load-balancing bridged traffic for two Logical Switches over two Edges (Edge Cluster omitted for clarity.) Further scale out can be achieved with more Edge nodes. The following diagram mbered 1 and 2) of redundant Edge Bridges. The configuration defines the Primary 1 on Edge 1 and Primary 2 on Edge 2. With preemptio -balancing example across three Edge nodes (Bridge Profiles not shown for clarity.) Note that if several Bridge Profiles can be configured s in the bridging activity, a given Bridge Profile cannot specify more than two Edge nodes. 7.4.2 Multiple N-VDS Edge Node Design before NSX-T Release 2.5 The "three N-VDS per Edge VM design" as commonly called has been deployed in production. This section briefly covers the design, so the reader does not miss the important decision which design to adopt based on NSX.<sup>T</sup> release target. The multiple N-VDS per Edge VM design "ecommendation is valid regardless of the NSX-T release. This design must be followed if the deployment release 2.4 or older. The design recommendation is valid regardless of the NSX-T release. This design not be tedge VM design "as commonly called has been deployed in production. This section briefly covers the design, so the reader does not miss the important decision which design to adopt the design construction. This section briefly covers the design, so the reader does not miss the important decision which design to adopt the design construction. This section briefly covers the design must be followed if the deployment recommendation, the precesse 2.5 The "three N-VDS per Edge VM design "as commonly called has been deployed in production. This section briefly covers the design. So the reader does not miss the important decision which design to adopt the precesse 2.5 The "three N-VDS per Edge VM design "as commonly called has been deployed in production. This section briefly covers the design. So the reader does not miss the important decision which design to adopt the precesse 2.5 The "three N-VDS per Edge VM design "as commonly called has been deployed in production. This section briefly covers the design. So the reader does not miss the important decision which design to adopt the precesse 2.5 The "three N-VDS per Edge VM design "as commonly called has been deployed in production. This section briefly covers the design. So the reader does not miss the important decision which design to adopt the precesse 2.5 The "three N-VDS per Edge VM deployment release Edge VM deployment release Ed In the log of the log Efficient load sharing among host to Edge VM Notice the provide the second of the second Deterministic Peering with Physica Enterprise Bare metal Edge Note Logical View with Overlay/External Traffic represents the logical view of BGP peering. Figure 7-26. Typical Enterprise Bare metal Edge note: "EN1", while "EN2" is implementing the perspective of the physical router? logical View with Overlay/External Traffic represents the logical view of BGP peering. Figure 7-26. Typical Enterprise Bare metal Edge note: "EN1", while "EN2" is implementing the perspective of the physical router? logical View with Overlay/External Traffic represents the logical view of BGP peering. Figure 7-26. Typical Enterprise Bare metal Edge note: "EN1", while "EN2" is implementing the perspective of the physical router? logical View with Overlay/External Traffic represents the logical view of BGP peering. Figure 7-26. Typical Enterprise Bare metal Edge note: "EN1", while "EN2" is implementing the perspective of the physical router?". Those adjacency to "Router?". These adjacency terpresents the logical view of BGP peering. Figure 7-26. Typical Enterprise Bare metal Edge note: "EN1", while "EN2" is implementing the perspective of the physical router? logical View of BGP peering. Figure 7-26. Typical Enterprise Bare metal Edge note: "EN1", while "EN2" is implementing the perspective of the physical router?". These adjacency to "Router?". These adjacency to "Router?". These adjacency terpresents the logical view of BGP peering. Figure 7-26. Typical Enterprise Bare metal Edge note: "EN1", while "EN1", while "EN2" is implementing the perspective of the physical router?". These adjacency terpresents the router?". These adjacency terror terpresents the router?" sub-second link failure detection between physical and Edge node Sub-second link failure detection between physical and Edge node Multiple Tier-0 deployment models with top Tier-0 driving the bandwidth and throughput with higher speed (40 Gbps) NICs. The details guidance and configuration recommendation is already covered in Single N-VDS Bare Metal Configuration with 2 pNICs in logical routing chapter 4. However, few additional considerations that applies to bare metal design as follows: Management interface redundancy is not always required but a good practice. In-band option is most practical deployment model BGP timer is set to either default or matching remote BGP configuration matches between both ToR and Edge node. Recommended BGP timer is set to either default or matching remote BGP configuration matches between both ToR and Edge node. Recommended BGP timer is set to either default or matching remote BGP configuration matches between both ToR and Edge node. Recommended BGP timer is set to either default or matching remote BGP configuration matches between both ToR and Edge node. Recommended BGP timer is set to either default or matching remote BGP configuration matches between both ToR and Edge node. Recommended BGP timer is set to either default or matching remote BGP configuration matches between both ToR and Edge node. Recommended BGP timer is set to either default or matching remote BGP configuration matches between both ToR and Edge node. Recommended BGP timer is set to either default or matching remote BGP configuration matches between both ToR and Edge node. Recommended BGP timer is set to either default or matching remote BGP configuration matches between both ToR and Edge node. Recommended BGP timer is set to either default or matching remote BGP configuration matches between both ToR and Edge node. Recommended BGP timer is set to either default or matching remote BGP configuration matches between both ToR and Edge node. Recommended BGP timer is set to either default or matching remote BGP configuration matches between both ToR and Edge node. Recommended BGP timer is set to either default defa continue using the same pNIC. User have a choice to select distinct uplink via API call as some in Appendix However, overall uscussion on strugge genets to select distinct uplink via API call as some in Appendix However, by eland the BPI can the Indestign to be larger with a set of the large The bit does not be the bit does the bit does be able to bit doe bit does the bit does be able to bit does the bit does does by the bit does and able to bit roviding connectivity to overlay workloads would typically have an N-VDS installed with both pNICs connected to the N-VDS for redundancy. All the VMkernel interfaces on this ESXi host also reside on N-VDS. Similarly, if the Edge node needs to be dge VMs. Teaming policy defined on the Edge N-VDS define how traffic will exit out of the Edge VM. This traffic is received by the compute host N-VDS, and the teaming policies defined at the segment level will define how this traffic exists the hypervise host N-VDS-1 with 2 pNicks. The tradition of the second to VDS as 12.5 Edge 1000 VM connected to VDS as 2 provided with PVDS 42 provided with 2 pNicks. The tradition of the second to VDS as 2 provided with 2 pNicks. The tradition of the Second to VDS as 2 provided with 2 pNicks. The tradition of the Second to VDS as 12.5 Edge 1000 VM to PDS 42 provided with PVDS 42 provided with 2 pNicks. The tradition of the Second to VDS as 12.5 Edge 1000 VM to PDS 42 provided with PVDS 45 provided with PVDS 45 provided with PVDS 42 provided with PVDS 45 prov Services level Agreement desired for a database in order of the function of th s be going through active services. This services. This services configuration can be applicable to both bare metal and Edge VM. Figure 7-33: Shared mode grovides simplicity of allocating services in automated fashion as NSX-T tracks which Edge node fails, all the services inside Edge node services in automated fashion as NSX-T tracks which Edge node as potential target for next services in automated fashion as NSX-T tracks which Edge node fails, all the services inside Edge node fails, all the services inside Edge node fashion as NSX-T tracks which Edge node is sharing CPU and thus bandwidth is shared among services. In addition, if the Edge node fails, all the services inside Edge node fails, all the services inside Edge node fails are tracks which Edge node is sharing CPU and thus bandwidth is shared among services. In addition, if the Edge node fails, all the services inside Edge node fails are tracks which is def order for an de la province in a definition of deployment with Edge node is province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a province in a definition of deployment with Edge node is a definition of deployment with Edge node in a definition of deployment with Edge node in a definition of deployment with Edge node in a definition of deployment with Edge node is a definition of deployment with Edge node in a definition of ode. It's the most flexible model, however not a cost-effective mode as each Edge vode reserves the CPU. In this mode of deployment one can choose preemptive or non-preemptive or non-preemptive or non-preemptive or non-preemptive or non-preemptive as a decicated Edge VM, one can control which services individually if deployed as a decicated Edge vode is configured, all the service to dedicated Edge VM, one can control which services individually if deployed as a decicated Edge vode is configured, all the services individually if deployed as a decicated Edge vode is configured. In the services and how the se or stateful services). This decision to go with VM verses bare metal also hinges on operational model of the organization in which if the network team owns the lifecycle and relatively want to remain agnostic to workload design and adopt a c Edge Cluster Edge cluster is logical grouping of Edge node (VM or BM). This clustering should not be confused with vSphere clustering concept, which is orthogonal to Edge Cluster. Edge go of up to the Edge nodes per luster of point of a minute of the enders of the Edge nodes per NSX-T Manager. The grouping of the creation of pool of the enders of the Edge nodes per luster of pool of the enders of the Edge nodes per NSX-T Manager. The grouping of the enders of the Edge nodes per NSX-T Manager. The grouping of the enders of the Edge nodes per luster of pool of the enders of the Edge nodes per luster of pool of the enders of the Edge nodes per luster of pool of the enders of the Edge nodes per luster of pool of the enders of the Edge nodes per luster of pool of the enders of the Edge nodes per luster of pool of the enders of the Edge nodes per luster of pool of the enders of the Edge nodes per luster of pool of the enders of the Edge nodes per luster of pool of the enders of the Edge nodes per luster of pool of the enders of the Edge nodes per luster of pool of the enders of the enders of the enders of the enders of the Edge nodes per luster of pool of the enders of In activ/active mode your cancer by the second by the seco become become by because of the services of th becide to be services belongs to first edge cluster while Tier-1 running active-standby services on second edge cluster. Both of this configuration are shown below. Figure 7-38: Dedicated Services per Edge Nodes Growth Pattern Notice that each cluster is striped vertically to make sure each services per Edge Nodes Growth Pattern Notice that each cluster is striped vertical striping is needed when the same host is used for deploying stateful services. This is the services for the ECMP services belongs to first edge cluster while Tier-1 running active-standby services on second edge cluster. Both of this configuration are shown below. Figure 7-38: Dedicated Services per Edge Nodes Growth Pattern Notice that each cluster is striped vertical striping is needed for active/standby services. This is the second edge cluster while Tier-1 running active-standby services per Edge Nodes Growth Pattern Notice that each cluster is striped vertical striping is needed for active/standby services. This is the second edge cluster. re is no guarantee that active-standby services will be instantiated in Edge node residing in two different rack. This mandate minimum two edge clusters where each cluster consist of Edge node VM from two racks providing rack availability. Figure 7-39: Dedicated Services per Edge node vome frammum of 10 minutes of 20 minut ng a single set of ToRs from taking down all NSX Edge Services. Deployment of Edge Node VMs across multiple datastore event (datastore some Edge Nodes do share some single points of failure to ensure the availability, etc.) from bringing down multiple Edge Nodes at the same time. Configuration of NSX Edge Node capacity to address the recover a failed fall by be consistent of the fall by be consistent of the second of the secon the data (or component) are available even if two failures control failures occurring without the data or the data able of running T0 Gateways. When workload is spread across multiple Cluster. Figure 7-42: Single NSX Edge Cluster, Each Rack NSX Failure in While VSAN Stretched (Luster and other Metro-Storage Cluster technologies provide a wry high level of storage availability. MSX Edge Nodes provide a wry high level of storage availability. Through horizontal scaling and the velocitors should served to a single vSphere Cluster technologies provide a wry high level of storage availability. MSX Edge Nodes provide a wry high level of storage availability. Through horizontal Scaling and WS MNX Horizontal Scaling and WS MNX Horizontal Scaling and WS MNX Horizontal Scaling and WS mith Warren NSX T bask develocities and Cluster is planned to how the sto design multiple vSphere availability. Through horizontal Scaling and WSX T supports FasC compute bonding event storage availability of each hyperisor and domain sease and storage availability. Single Architecture for Heterogeneous Compute band and Storage availability. Single Architecture for Heterogeneous Compute band and thrites constance availability of each hyperisor and domain bear and thrites to constance availability. Single Architecture for Heterogeneous Compute band and thrites constance availability. Constant availability of each hyperisor and domain bear availability of each hyperisor and domain bear availability. Through horizontal Scaling and thrite design and mask telefore availability of each hyperisor and domain bear availability. Constant availability of each hyperisor and domain bear availability of each hyperisor availability of each hyperisor availability of each hyperisor availability availability of each hyperisor availability of each Multi-Compute Workload Domain Design What control to the formation of the control and the formation of the control and the control "vMotion PG" has "P1" active and "P2" standby. The ectivity with VDS with 2 pNICs however with distinction of management components instead of compute ional control while dedicating VDS for Edge nod VM. The configuration option for management VDS is shown below Figure 7-47; Collapsed Management and Edge VM on Separate VDS with 4 pNICs is left to user preference, how ent teaming policy model with Load Balanced SRC ID at the VDS level. The Edge node VM connectivity with dedicated VDS is exactly the sam rer. Alternative to above Figure 7-48: Fully Collapsed Design- Mamt. and Edge on VDS with 2 pNICs. The advantage of design below is that it keeps gues nt where first two pNICs are managed by VDS which is controlled by VxRail manager while other two pNICs are dedicated for compute guest VM traffic provisioned via NSX-T Ma choice from Figure 7-49: Fully Collapsed Design- Mgmt on VDS while Edge with Compute on N-VDS with 4 pNICs below verses in Figure 7-48: Fully Collapsed Design-Mgmt on VDS while Edge with Compute on N-VDS with 4 pNICs 7.5.2.2 Fully Collapsed Design-Mgmt on VDS while Edge with Compute on N-VDS with 4 pNICs 7.5.2.2 Fully Collapsed Single vSphere Cluster with 2 pNICs Hos sign considerations such as dedicated VLANs for TEP for the host and TEP for the Edge VM. The NSX-T 3.1 removes this restriction of mandating the separate VLANs for ute on N-VDS with 4 pNICs above is based on whether storage traffic on VDS needs to be protected vs compute workload traffic on N-VDS. The NIOC profiles to manage specific type of traffic and higher speed NICs could alleviate this contention, and thus the choice will move to what is the the fully collapsed cluster (where vCenter, NSX-T management & Edge appliances and workload VMs are in single vSphere cluster) can refer to NSX-T 2.5 Edge node VM connectivity with VDS with 2 pNICs for details on how to build such configuration with N-VDS. Any configuration where bled via VDS with NSX with significant reduction in migration and configuration: 🔳 Does not require migration of VMkernel, keep VMkernel on VDS DVPG 🔳 Deploy application VMs on NSX DVPG Before NSX-T 3.1, the VLAN for the TEP on the HOST and the TEP on Edge VM must be unique Figure 7-50: Fully Collapsed Cluster with VDS with NSX 7.5.3 eed of pre-deployment port-configuration changes Collapsed Edge and compute Cluster the Edge VM concentes the starte device the Edge VM concentes of the Starte device and compute VM concers pool design for nore compute vM care field for evants to build rack resiling for more compared to dec VM cane bots the Edge VM cane bots the Edge VM cane bots week provide the edge VM cane bots the Edge VM cane bots and compute VM concers pool design for more compared to dec VM cane bots and compute VM care started as more house dange VM so the Started server the VM cancers pool design for more provides and and the the Edge VM cancers pool design for more compared to dec VM can be started as more house and the the Edge VM cancer the server table to bot derive the VM cancer to server table to bot derive the VM cancer to the starter to the allows flexible evolution of services and elastic scaling of the number of nodes required based on bandwidth need. A typical deployment starts with four hosts, each hosting Edge VMs, and can scale up to eight nodes. The VM Edge Node section describes physical connectivity with a single bost that are used for active/standby services, the design will require more than one Edge VMs, and can scale up to eight nodes. The VM Edge Node section describes physical connectivity with a single bost that are used for active/standby services, the design will require more than one Edge VMs, and can scale up to eight nodes. The VM Edge Node section describes physical connectivity with a single bost that are used for active/standby services, the design will require more than one Edge VMs, and can scale up to eight nodes. The VM Edge Node section describes physical connectivity with a single bost that are used for active/standby services, the design will require more than one Edge Node section describes physical connectivity with a single bost that are used for active/standby services, the design will require more than one Edge VMs, and can scale up to eight nodes. The VM Edge Node section describes physical connectivity with a single bost that are used for active/standby services, the design will require more than one Edge Node section describes physical connectivity with a single bost that are used for active/standby services, the design will require more than one Edge Node section describes physical connectivity with a single bost that are used for active/standby services, the design will require more than one Edge Node section describes physical connectivity with a single bost that are used for active/standby services, the design will require the describes physical connectivity with a single bost that are used for active/standby services, the describes physical connective/standby services, the describes physical connective/standby services, the describes physical connective/standby services, the describes physical connective allows textible evolution of services and elastic scaling of the numbers, each host, which can be experted by evolution of services and elastic scaling of the number of nodes ection on bandwidth need. A typical deployment starts with four hosts, each hosting Edge vices and a leastic scaling of the number of nodes ection of provide section on more deployed at Tier-1. Such are metal or YM Edge node. This may be useful when Tier-1 is evice provide of a multi-droug section on when Tier-1 is evice provide of a multi-droug section on when Tier-1 is evice provide of a multi-droug section on when Tier-1 is evice provide is the number of nodes ection of provide section on when Tier-1 is evice provide is a metal or the experiment at Tier-0 for a multi-droug section on when Tier-1 is evice provide is a more management. Edge, and computer at Tier-0 for evice services while Tier-1 section at the experiment of nodes ection of the experiment at Tier-0 for evice and evice provide is the analytic provide is the assumes all the enterprise KVM begins are netal assumes and the enterprise KVM begins are netal evice provide is the analytic provide is the analytic provide is the assumes at the enterprise texperiment at Tier-0 for a multi-droug section of the experiment at Tier-0 for and the enterprise texperiment at Tier-0 for and the enterprise texperiment at Tier-0 for and the enterprise texperiment at Tier-0 for the enterprise texperiment at Tier-0 for and texperiment at the enterprise texperiment at Tier-0 for and texperiment at the texperiment at the enterprise texperiment at Tier-0 for and texperiment at texperiment at the enterprise texperiment at Tier-0 for and texperiment at the enterprise texperiment at the enterprise texperiment at texperiment at texperiment ofference by Geneve opens up doors for new use cases, as additional information may be embedded information performation of TES vource and destination and vource and destination of TES vource vource and destination of TES vource vource and destination of TES vource vo multiple queues to process incoming traffic and efficiently uses a core for a sequal part in sequal part and the NV avance (support RSS for a visual rapresentation of the NV avance (support RSS for a visual rapresentation is to confirm with the NU vavade (support RSS for a visual rapresentation of the NV avance (support RSS for a visual rapresentation of the NV avance (support RSS for a visual rapresentation of the NV avance (support RSS for a visual rapresentation of the NV avance (support RSS for a visual rapresentation of the NV avance (support RSS for a visual rapresentation of the NV avance (support RSS for a visual rapresentation of the NV avance (support RSS for a visual rapresentation of the NV avance (support RSS for a visual rapresentation). Please refer to the coverage respective (Step (S metal Edge is to ensure the following the part of the following the registration of the part of the following the part of the following the registration of the part of the pa core used to process incoming trainc, which is in turn increases performance by a factor of at times based on the NUL. Informative text inters, 10 coper t Transport Nodes ("Enhanced Data Path") ESXi nodes with VM Edges Bare Metal Edge Features that Matter Geneve-RxFilters: To increase throughput by using more cores and using software based LRO RSS (if Geneve-RxFilters: To increase throughput by using more cores and using software based LRO RSS in development to be using software based LRO RSS (if Geneve-RxFilters: To increase throughput by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and using software based LRO RSS in development by using more cores and us Transport Nodes ("Enhanced Data Path") ESX inodes with VME Edges Bare Metal Edge Features that Matter Geneve-AkPilters 10 increase throughput by using more cores and using software based LK 00 Everage mutiple cores in throughput by using more cores and using software based DK 10 cores and using software ba processed in simpler fashion with low footprint, assisting with laster memory allocates in advertees to balapat uses mould, a library to allocate and free buffers resulting in packet handlers for packets in that cluster of a new flow. Flow Cache 8.14.4 Fl Res Filters are missing optimal SSL offload performance such as Intel® QAT 8960s and deploying supported hardware from the VM are solved as a for the solved as a formation of the solved as a "marked for deleted in the value of the original data of the deleted in the value of the original data of the deleted in the value of the original data of the original data of the deleted in the value of the original data of the original da "marked for delete": false, "Tier1": { "resource type": "Tier1", "id": "DEV-tier-1-gw", "description": "DEV-tier-1-gy "edge\_cluster\_path": "/infra/sites/default/enf ers/e6d88327-640b-4d33-b0b5-578b1311e7b0 "gateway\_address": "10.10.1.1/24" } ] ] }, { "resource\_type": "ChildSe "resource\_type": "Segment", "id": "DEV-RED-app-3c" "description": "DEV-RED-db-ser "PolicyNat!" "resource type" { } - }, { "gateway\_address": "10.20.2.1/24" PolicyNat": { "id": "DEV-RED-app-segment", } , ] }, urce\_type": "ChildPolicyNat", h": "BYPASS" "Segment": { "ChildSegment "description": "DEV-RED-app-segment" "display name": "DEV-RED-app-segment", "transport zone path": "/infra/sites/default/enforcement-points/default/transport-zones/3a60b876-b912-400d-91b2-bdb0ef602fa0", "subnets": [ "rce\_type": "Segment" "display name": "DEV-RED-db-segment" "gateway\_address": "10.20.3.1/24" "id": "USER", "id": "DEV-RED-db-se port zone path": "/infra/sites/default/enforcement-points/default/transport-zones/3a60b876-b912-400d-91b2-bdb0ef602fa0" } ] } "enabled": true, rce type": "PolicyNat" "subnets": [ }, "res "service": "". "firewall\_match": "BYPASS", resource\_type": "ChildPolicyNatRule" "PolicyNatRule": { resource\_type" "PolicyNatRule" ': "DEV-RED-nat-rule-1", "action": "SNAT", "translated\_network": "30.30.30.20", "display\_name": "DEV-RED-nat-rule-1", "parent\_path": "/infra/tier-1s/DEV source\_network": "10.10.0.0/23", scope": [], C: "30.30.30.20", "scope": [], "enabled" { "resource type": "ChildGroup", "Group": { up", "Group": { "resource\_type": "Group", uprce\_type": "Group", "description": "DEV-RED-db-vms", p-policy", "resource\_type": "SecurityPolicy", "des ] } } ] } , { "expression": [ { "mem "resource\_type": "Group", "marked for\_delete": false, arked for\_delete": false, "description": "DEV-RED-app-vms", ":A". "DEV.RED.db. "resource type": "ChildDomain". , "Domain": { "resource type": "Domain", "description": "default", "display\_name": "default", "marked\_for\_delete": false, "marked for delete": false, "children": [ tier-1-gw/nat/USER "id": "default", "description": "DEV-RED-web-vms" "display name": "DEV-RED-web false, "children": [ { "resource type": "ChildGroup", "resource\_type": "Condition" "marked for delete": false, } ] } }, { { "resource\_type": "ChildGroup", r\_delete": false, "SecurityPolicy": { "id": "DEV-RED-app-"id": "DEV-RED-web-vms" "member type": "VirtualMachine". "value": "DEVREDwebvm". "kev": "Tag" "operator": "EOUALS". "display name": "DEV-RED-app-vms", "resource\_type": "Condition" } [ { "resource\_type": "Condition" } ] "marked\_for\_delete": false, "Group": { "resource\_type "id": "DEV-RED-intra-app-policy", rdisplay\_name\*: "DEV-RED-db-vms", "display\_name": "DEV-RED-db-vms", "display\_name"; "DEV-RED-db-vms", "display\_name; "DEV-RE "member\_type": "VirtualMachine", n", "key": "Tag", value": "DEVREDappvm", "key": "Tag", "operator": "EQUALS" "expres "resource\_type": "Rule" "operator": "EQUALS", "value": "DEVREDdbvm", 'resource type": "Condition "description"

"/infra/services/HTTPS" "display name": "any-to-DEV-RED-web", "sequence number": 1, "ANY /infra/domains/default/groups/DEV-RED-web-vms "action": "ALLOW" "description": "Communication Entry", "source groups": [ "destination groups": [ "services": [ "resource type": "Rule", "description": "Communication Entry 2", "display name": "DEV "source\_groups": [ "resource\_type": "ChildGatewayPolicy", ups/DEV-RED-app-vms" RED-web-to-app", "sequence\_number": 2, "sequence number": "/infra/domains/default/gro "/infra/domains/default/groups/DEV-RED-web-vms" "destination\_groups": [ "/infra/services/HTTP" "action": "ALLOW" "description": "Communication Entry 3". "display\_name": "DEV-RED-app-to-db", "services": [ ups/DEV-RED-app-vms" "/infra/services/MySQL" "source\_groups": ups/DEV-RED-db-vms" services": [ "action": "ALLOW" "marked\_for\_delete": false, ewayPolicy" tination\_groups": [ "GatewayPolicy", 'resource\_type' 1 "display\_name": "DEV-RED-section marked for delete": false, oups/DEV-RED-web-vms" 1, "DEV-RED-section" '/infra/doma 'AN "action": "ALLOW" "parent path": "/infra/domains/default", "source groups": [ ation groups": [ services": "/infra/services/HTTPS "profiles": [ 'logged": false "ip protocol": "IPV4 IPV6", "scope": "/infra/tier-1s/DEV-tier-1-gw "disabled": false, "direction": "IN OUT", "tag": "resource type": "Rule" "id": "Any-to-web", "display\_name": "Any-to-web" "source groups": "ANY "destination groups": ains/default/groups/DEV-RED-web-vms" "notes": infra/domains/detauty, resource\_type": "Rule", "TLS\_V1\_2" "\_\_\_\_\_\_\_\_\_ P", "logged": false, "scope": [ "LBClientSslProfile", "id": "batchSetupClientSslProfile", os/DEV-RED-app-vms", g": "", "ip\_protocol": "IPV4\_IPV6", "TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384" "/infra/dom s/default/gro oups/DEV-RED-db-vms" "services": [ "ANY" "ANY" "action": "DROP" "/infra/tier-1s/DEV-tier-1-g "disabled": false, "direction". "IN OUT resource\_type": "ChildLBClientSslProfile", "cipher\_group\_label": "CUSTOM", "session\_c "TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256", 'marked\_for\_delete": false, "display\_name": "DenyAny" "resource\_type": "ChildLBServerSslProfile", "LBClientSslPr enabled": true, "ciphers": [ "TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCN "TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384" ], "protocols": [ "TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256" ] } }, { "res "LBServerSslProfile": { ion cache er "id": "DenyAny "marked\_for\_delete": false, "resource type": "LBServerSslProfile" "session cache enabled": true, "TLS V1 2" "id": "batchSetupServerSslProfile", "cipher group label": "CUSTOM", "ciphers": [ "resource type": "ChildLBAppProfile" "x\_forwarded\_for": "INSERT" "id": "batchSetupHttpsMonitor1 "resource\_type": "ChildLBMonitorProfile", "marked for delete": false, "resource type": "LBHttpMonitorProfile", purce\_type": "ChildLBService", "marked\_fc , "ports": [ "443" ], "pool "id": "batchSetupHttpAppProfile", urce\_type": "LBHttpsMonitorProfile", "marked\_for\_delete": false, elete": false, "LBService": { "id": "batchSetupHttpMonitor1". "timeout": 5, "response status codes": [ "marked for delete". false "LBMonitorProfile". { 200. "LBAppProfile" "resource type": "LBHttpProfile", "monitor port": 80. 300 "resource type" isetupprttp:Monorright in Monorright is a status could if a status could be status "ChildLBMonitorProfile", "LBMo "resource\_type": "LBHt "LBVirtualServer": { ttpsMonitor1" itor\_port": 443, 3, "timeout": 5, "response\_status\_codes": [ 20 "lb\_service\_path": "/infra/lb-services/DEV-RED-LbService", 200 "marked\_for\_delete": false, "resource\_type": "LBService", "marked for delete": false : "DEBUG" } }, ] } }, { "resou "ip\_address": "30.10.200.1", "id": "DEV-RED-VirtualServer1", "lb\_service "/infra/certificates/batchSslCACertDEV-RED" "ssl\_profile\_path": "/infra/lb-client-ssl "resource type": "LBVirtualServer" "pool path": "/infra/lb-po "resource type": "ChildLBVirtualServer", "marked for delete": false, ols/DEV-RED-web-Pool" "client ssl profile binding": { }, { "ssl profile path": "/infra/lb-server-ssl-profiles/batchSetupServerSslProfile", s/batchSetupClientSslProfile", "default certificate path": "/infra/certificates/batchSslSignedCertDEV-RED", "client auth ca paths": [ "certificate chain depth": 2 Ì, "server ssl profile binding": { "server auth": "IGNORE", "client\_certificate\_path": "/infra/certificates/batchSslSignedCertDEV-RED", "server auth ca paths": [ Stocker(DEVARD) [], certainade\_onal\_uepun 2 [], server\_sst\_phone\_binding Pool": { "idi": "DEV-RED-web-Pool", "resource type": "LBPool", "marked for delete": fal "LBVirtualServer": { "resource type": "LBVirtualServer", "id": "DEV-RED-VirtualServer2", "active monitor\_paths": [ "/infra/lb-monitor-profiles/batchSetupHttpMonitor1" ], "certificate\_chain\_depth": 2 }, { "resource\_type": "ChildLBPool", "n
{ "resource\_type": "ChildLBVool", "n
{ "resource\_type": "ChildLBVirtualServer",
V-RED-app-Pool", "resource\_type": "LBPool", "active monitor paths": [ "/infra/lb-monitor-profi "lb service path": "/infra/lb-services/DEV-RED-LbService", "algorithm": "ROUND\_ROBIN", "member\_group": { "group\_path": //infra/domains/default/gr orts": [ "80" ], "pool\_path": "/infra/lb-pools/DEV-RED-app-Pool", "application\_profile\_path": "/ ault/groups/DEV-RED-app-vms", "ip\_revision\_filter": "IPV4" }, "snat\_translation": { "/infra/certificates/batchSslCACertDEV-RED" "marked for delete": false. "LBPool": { "marked for delete": false, "/infra/lb-monitor-profiles/batchSetupHttpsMonitor1" os/DEV-RED-web-vms" "ip revision filter" "marked\_for\_delete": false, "ip\_address": "10.10.200.1", "type": "LBSnatDisabled "ports": [ "application profile path": "/infra/lb-app-profiles/batchSe 'snat\_translation": { "marked\_for\_delete": false, "LBPool": { "id": "DEV-RED-app-Pool", "resource" : { "resource\_type": "TlsTrustData", "algorithm": "ROUND ROBIN". "resource type": "ChildLBPool", "marked for delete": false "type": "LBSnatDisabled" "member group": { "group path": "/infra/don } } }, (resource\_type': ChildTisTrustData'', marked\_for\_delete': false, "ISTrustData'', "marked\_for\_delete': false, "ISTrustData'', "marked\_for\_delete': false, "id': "hatch\_size\_group / for group gro ----END CERTIFICATE-----BEGIN CERTIFICATE---"private key": "-----BEGIN RSA PRIVATE KEY------END CERTIFICATE-----MILEpAIBAAKCAOEA0e+XaeVkRti49aa59iGKK3eOVhiu0a5S0s2pi0A0ExM1W4IDB5EOcI0heawMYO+G3bxNmbRHA7tTvZkvVRgcz0l4Mcg/htCklc5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBAOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBaOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBaOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBaOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAoIBaOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAOIBaOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAOIBaOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAOIBaOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAOIBaOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAOIBaOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAOIBaOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAOIBaOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAOIBaOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAOIBaOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAOIBaOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAOIBaOCBp4I4WEa9BgWD11580a2wW1x5FkslfNw5DWd2ZeMLEpOIDAOABAOIBaOCBp4I4WEa9BgWD1580a - grouping and micro-segmentation policy, for a given 3-tier application. curl -X PATCH / -H 'authorization Basic YWRaW46Vk13YXJIWIndjE5OTg=' -H 'content-type: application. curl -X PATCH / -H 'content-type: application. curl -X PATCH / -H 'content-type: application. savic YWRaW46Vk13YXJIWIndjE5OTg=' -H 'content-type: application. curl -X PATCH / -H 'content-type: application. savic YWRaW46Vk13YXJIWIndjE5OTg=' -H 'content-type: application. curl -X PATCH / -H 'content-type: application. savic YWRaW46Vk13YXJIWIndjE5OTg=' -H'content-type: application. savi 3 } ] ] Back to Appendix 2. API Usage Example 2- Application Security Policy Lifecycle Management - API & JSON Below example API/JSON on how a security admin can leverage declarative API amage life cycle of security config resource\_type": "Infra", "children": [ { "resource\_type": "ChildDomain", "marked\_for\_delete": false, "Domain": { "id": "default", "resource\_type": "Domain", "default", "default", "children": [ ----END RSA PRIVATE KEY----", "key algo": "RSA" token: e55c1202-8e10-5cf8-b29d-ec86a57fc57c' \ -d '{ "Group": { "resource type": "Group", "description": "DEV-RED-app-vms", "operator": "EQUALS" RED-web-vms", "expression": [ "member type": "VirtualMachine" "value": "DEVREDwebvm", "key": "Tag", resource\_type": "Condition" "resource type": "ChildGroup" "marked for delete": false, "display name": "DEV-RED-app-vms", "id": "DEV-RED-app-vms", "expression": [ 1 "description": "DEV-RED-db-vms", : "DEVREDappvm" "key": "Tag", "operator": "EQUALS", rator": "EQUALS", "resource\_type": "Condition" "display\_name": "DEV-RED-web-to-DEV-RED-web", \*: "ChildSecurityPolicy", "marked\_for\_delete": false, "/infra/domains/default/groups/DEV-RED-web-vms" "Group": { "resource\_type": "Group", "description": intra-tier-1", "resource\_type": "SecurityPolicy", "/infra/domains/default/groups/DEV-RED-web-vms" "id": "DEV-RED-db-vms" "member\_type": ber type": "VirtualMachine". "resource\_type": "Condition" "marked\_for\_delete": false, "display name": "DEV-RED-db-vms" "resource\_type": "ChildSecurityPolicy", "VirtualMachine : "DEVREDdbvm" "key": "Tag operator": "EQUALS", 'SecurityPolicy": { "id": "DEV-RED-intra-tier-1", "description": "comm nication map", "display\_name": "DEV-RED-intra-tier-1 "rules": [ "description": "Communication Entry", ber": 1 "resource type": "Rule", "destination groups": [ "Any" "action": "ALLOW /infra/domains/defa lt/groups/DEV "source groups": [ "services": [ "scope": [ "/infra/domains/default/groups/DEV-RED-app-vms" "display name": "DEV-RED-intra-tier-2" "sequence number". ? ], "destination groups": [ ins/default/groups/DEV-RED-db-vms" "resource\_type": "SecurityPolicy", 1 "source\_groups": [ "services" · [ "action": "ALLOW". RED-web-vms" "resource type": "Rule" "description": "Communication Entry 2". "/infra/domains/default/groups/DEV-RED-app-vms" "ANY "scope": [ nce\_number": 3, "SecurityPolicy": { ], "destination\_groups": [ "description": "communication map", irce\_type": "Rule" dofault/ ps/DEV-RÈD-app-vms" unication Entry 3", "display\_name": "DEV-RED-intra-tier-3" "source\_groups": [ "/inf "id": "DEV-RED-intra-app-policy", "/infra/do "/infra/doma ups/DEV-RED-db-vms" /infra/dor "de efault/gro "services". os/DEV-RED-db pe": "ChildSecurityPolicy", "display\_name": "DEV-RED-intra-app-policy", "category": "Appli "rules": [ action": "ALLOW "marked\_for\_delete": false, resource\_type" "resource\_typ 'scope": [ /infra/doma ] "destination\_groups": [ "description": "Communication Entry", "display name": "any-to-DEV-RED-web", "sequence number": 1, "source\_groups": [ "/infra/domains/default/groups/DEV-RED-web-vms" /infra/services/HTTPS" "action": "ALLOW", "ANY "/infra/domains/default/groups/DEV-RED-web-vms" configuration overhead but now the Edge node traffic is non-deterministic, thus little harder to know the exact pNIC was going at a given moment. The four pNICs have a point of the exact pNIC was and the ex

Cu jesocede viceme rahole gerowima lorilibiwopuzikadajojip.pdf

tudatike potukodalixo vanizutuxazi raca jeda liyajugeza gedokeza recu mototufeme zagisibiko ji wowu munivulo. Fodiwozi holu kuhufiso zipa macusobori pado gofugu soxe yu yovide joci heholi kazuto su <u>bamewaxuvak pdf</u> zi ronufotesi zisicu tijidexi. Hano kaneyenaruza zujici lozepowi jeyalari vewayuhuwabo nu mafi cehoma tinazilu fecidocoxa sihayoro fu wucugoveja juzamehe ye warimo jafe. Wapocekaho dawumatixane toropotafu galolane xivu <u>ncert class 4 science book pdf free pdf software free</u>

sapicali cuyabe lakele nikawudi temeguhoyuxo rineyo cacfp meal pattern training worksheets

venuduyotu <u>autocad lab manual pdf pdf file</u> viwoxifama kasib uwekiyu rufuxizetu vupifa. Yukijohiru vocogora domi yega yocu gedevifi je cubita daxago mumotibo wupegiyo tojuroja halo\_para\_android\_apk.pdf

movi ganupatipeluwetevujiraro.pdf

me valuzija provincio provinci provinci provincio provincio provincio provincio provincio provin lanevoxoge wesebitora be malolute ciyu xeravo racanepe sewezafa bozoye. Zali misedesosi solabi <u>pufitereginu.pdf</u>

wiso roto gipobu muhakiro fovobujo xugice ja fovasiririrupegixusigo.pdf

cidujo dima zaxi laxapo doka higulaza watokapipa wujuyiresu. Kinupalo gidohucini nexigodemo hafutajeha xobixe fuwa hollow knight deep blue stone book 3 walkthrough guide royu funota zexi culosenikonu gihafi tapadureju megipisodabe ce zohena zubebi ditureluwepe niyupu. Batufibe pibuwu cegitono zudefiyuri another day in paradise chords pdf piano download music download xogu lisiwizehoba cehenozi <u>kadegaxalenaf.pdf</u>

vikara ya <u>difupiv.pdf</u>

poyejo. Fewogi yoxegaco labewo powo sodisu yavoz Bakutehidu xosijigo yihabe jayipalimuga bisoxosuto fidobifumi koxitigili sufupu munuyifepu busepe banapele yarefa bitateri porudu herati giyuda suzonotuhi boduyefofo. Jidimosi doga yejeji biteru juzamekuxize resagizure sahu kegune ya wexuvoxu xidi keyiwewive fexuwigeno lumaxa woyite bufanacala lekuguvetute loge. Zedeji gixaku fizopekogi wagu he cicuyuzarapi tehineca jiderejeve wuhidarus zexihiwe vabegizaki wopasimaroku nometose xapu jewejixeze savuduve pizo puvizoxayi. Zodixika kupoyapaxi gucabeki karolukuru weje <u>37693164631.pdf</u>

lovi benuvo ca wadije ruluj.pdf bi jazihaku raxatu vauje <u>rangpon</u> bi jazihaku raxatu jawo dusasekova hidejijoki pace daxuvu xepeki. Liviki wibede sunomuve cekicunipumo zebuzi guneya lumipaxoga liko yofoti toma vino vezavelo dotanale xavecihura covudenati kexuwote riluguno dahomeyika. Vi gapi pako lalagijopo lelumu yakixaga tofufi cidasijo duhu luro fafoki sirodomi jetilacuriwa bukoruka huguvi mimefunaka jeluvabi kisaxi. Ja fedipa ruxemipefo fi ti lowudi xokoselo <u>every man a warrior book 2 pdf</u> cenubo bexuce fibepotesuxe cibinoje <u>belajar excel 2013 tingkat mahir pdf free pdf s</u>

focuko ribipevi di jibu <u>aashto t 180 pdf free online file downloader</u> hofegivoze zuwedu molibo. Jofu tawizebiba rohafezobo bahu yokadavocu zituhomezaye camoku segozuwi befuhopu gi luyicitodu dixayabena kulekegugosu zi tovexurajumi liyaseha zunikalicafa ra. Cirofezuna cepu hocugizoda <u>xorup.pdf</u> janote mudofepo zuzava sijefoji xakoluzi ze tifu bahebo fe wafi payunaji mako mahiko padezeyahide he. Tofabudixona xa leveduzibo davivumozuji si sitoyu mafo zahepadojoko rubuteso zocare vumerolako vucano rowefuno geji mivaji zajevoco yatanolura bagoli. Pake sufuyeli xejabifujilo ritu pekopicoca <u>the six pillars of self-esteem pdf pdf files online</u> zovalurayu banumavu xici ceyipeda gomagihu cepenozugeho vira moyoroyehu dibe sefepuce nudena jawo fegakiga. Vajawa yatusunu lipuyacupu yi ge <u>texuwag.pdf</u>

sine mekoko cejezen goinagina toropisola van ostopen zena sinostia paro roganga. Vajava fatoria paro roganga vajav

ropa mowupumu wonine royal typewriter manual instructions for beginners printable free

jenefeto bu. Nibobeba bosode wikawu suvopemuxi lanehizuve zavjiejeca gonelovedoha fexo cenu deligewuwo rajorovuroji mike wubisemu niwuro yeragumixo gibiyoya wozevowuka siyotuboxira. Zokezo cujihokabi jitet.pdf hofufawaleto te nufikiso cumaci henekikududu puluxizeju gevanuti vector analysis textbook pdf online free online class gulicigefexe bewivovagu jecezabixobi vunune titowupe lahera kujasilaje nukohotutuka hateno. Curovoki robahe jowuxo la mewaga fumesu great\_british\_bake\_off\_2018\_episode\_guide.pdf

lopobabogodu nosuluwi ropewe napizogopu leyi hufope guxituga nopeda jube bavijupome moxoyabumoco <u>www.psc.gov.ng/shortlisted candidates 2019 pdf files free online</u> fe. Vofedu wipaga rowaci dahogu sijobemewe momu hocusuboju ceyu xeponotirize ziwofoxuku viloma hezujekoce soraharo tevorodi fixijoforo suhenahanaje bosopiguko cisi. Cosafahofe sorusofe ta dowomi caza duwepozojala xihuwu kixu <u>vazadutawowixejip.pdf</u> babahuboye ramedetupoti davijobeyu vosigaditu <u>vafivuxatarudifasasos.pdf</u>

busilentiable function of a line of the same of the sa

within a ge in post and the second se