1. Use Cases and Scenarios

This service is designed to support a wide range of enterprise scenarios where seamless Layer 2 connectivity is required between non-VMware environments and Azure VMware Solution (AVS). Key use cases include:

- **Workload Migration**
  Extend L2 networks to AVS to simplify VM migration without re-IP, ensuring application continuity across platforms.
- **Hybrid Application Deployment**
  Maintain consistent network policies and security controls across on-premises and cloud workloads, enabling true hybrid operations.
- **Disaster Recovery and Business Continuity**
  Use AVS as a secondary site for workloads running in non-VMware environments, replicating traffic over the extended L2 network.
- **Cloud Bursting for Legacy Platforms**
  Extend compute capacity into AVS when local environments (e.g., Hyper-V, bare metal) reach limitations, without requiring major refactoring.
- **Testing and Dev Environments**
  Mirror existing VLANs in AVS for dev/test environments that need to simulate production connectivity.
- **Multi-tenant Network Isolation**
  Assign each user or tenant a dedicated VLAN, leveraging the one-user-per-network model to ensure strict network segmentation.

2. Architecture Overview

The architecture for this service includes the following logical components:

- **Source Environment**
  Non-VMware infrastructure such as physical servers, Hyper-V, KVM, or legacy virtualization platforms.
- **L2 Extension Gateway**
  A physical or virtual appliance placed at the edge of the source environment to encapsulate Layer 2 traffic using technologies like VXLAN, L2TPv3, or SD-WAN tunnels.
- **Secure Tunnel (L2 over L3)**
  The Layer 2 traffic is tunneled securely over Layer 3 (IP-based) transport to Azure, leveraging encrypted VPN tunnels or private ExpressRoute connectivity.
- **AVS Private Cloud**
  The Azure VMware Solution environment receives and bridges the extended VLANs through a designated NSX-T segment that matches the incoming encapsulated traffic.
- **Network Segmentation Control**
  Each VLAN is isolated, adhering to the “one user = one network” policy, allowing scalable multi-user support.

3. Supported Environments

This service is compatible with a wide variety of infrastructure types. Supported source environments include:

- **Microsoft Hyper-V**
  On-premises Hyper-V clusters or standalone hosts.
- **KVM-based Platforms**
  Including Proxmox VE, OpenStack KVM, Red Hat Virtualization (RHV), and similar.
- **Physical Servers / Bare Metal**
  Any x86 or ARM-based hardware with bridged network access.
- **Mainstream Operating Systems**
  Linux distributions (RHEL, Ubuntu, CentOS, SUSE), Windows Server (2012+), and BSD variants.
- **Legacy Systems**
  Older, non-virtualized platforms can be supported via custom L2 encapsulation appliances.
- **Edge Devices and Firewalls**
  Compatibility with SD-WAN appliances, Layer 2 VPN devices, or specialized L2 gateways.

The only requirement is IP connectivity between the source environment and Azure, either through VPN or ExpressRoute. NSX-T support in AVS is used to terminate and manage the extended VLANs on the cloud side.