HAMMERSPACE

Deploying Hammerspace in Azure Marketplace

Revision 2

Hammerspace Version 5.2

Hammerspace, Inc.

Corporate Office:
305 Main Street
Redwood City, CA 94063

Mailing Address:
1900 S. Norfolk Ste. 350
San Mateo, CA 94403

Table of Contents

Hammerspace 5.2

This document covers how to deploy Hammerspace in Microsoft Azure Marketplace. Hammerspace software is available in two consumption models, namely Pay-As-You-Go (PAYGO) and Bring Your Own License (BYOL).

Hammerspace BYOL (Bring Your Own License)

BYOL licensing is a software subscription model that is activated by contacting Hammerspace. This is often a suitable choice for customers who have a mix of cloud and on-premises deployments and a desire to consolidate licensing.

Hammerspace PAYGO (Pay-As-You-Go)

PAYGO licensing is a standard cloud consumption model in which usage is metered and billed to the cloud provider on an hourly, monthly, or yearly basis.

Solution Overview

Hammerspace Data Platform consists of two main software components, a metadata node (Anvil) and a data services node (DSX).

Anvil

The following services are provided by the Anvil instance(s):

- Management GUI & CLI
- Metadata management.
- Mount point for Parallel NFS (NFSv4.2).

DSX

The Data Services instance(s) provide the following services:

- Global namespace.
- Global file system.
- Mount point for NFSv3, SMBv3, and S3
- Data mobility
- Storage and volume management

Hammerspace System Requirements

Anvil must be given sufficient resources to deliver low-latency performance for applications and end users. Anvil metadata nodes take full advantage of allocated resources. It is not unusual for Anvil to operate at 40% or higher CPU utilization even with a relatively modest metadata workload in a large file system. Metadata performance may suffer if the system becomes resource constrained. Therefore, it is crucial to ensure that Anvil metadata nodes have sufficient system resources.

Listed below are the minimum system resource recommendations for Anvil and DSX in a bare minimum deployment. Please note that production environments or environments requiring high performance need substantially more than the listed minimum recommendation.

	Anvil Metadata Node	DSX Data Node
Azure Virtual Machine	2 x Standard E4as v4	1 x Standard F2s v2
CPU Cores	16 vCPU	8 vCPU
RAM	32 GB (more recommended)	4 GB (more recommended)
Boot disk	200 GB (if memory is larger than 160 GB multiply by 1.3 for sizing).	200 GB minimum
Additional disk drives for metadata storage	2 x 400 GB (minimum) backed by SSD or NVMe	As needed for DSX data storage
Network adapter	2 x 10 Gbps Ethernet. One link is dedicated to HA services	1 x 10 Gbps Ethernet

IMPORTANT: The choices of virtual machine sizes, as well as disk types and sizes, require careful planning. A metadata disk size of 200 GB will accommodate approximately 25-50 million files. For small-to-medium environments or lab/demo scenarios, the default settings are typically adequate. For large or workload-intensive environments, please consult with Hammerspace before deployment. This is particularly important where metadata performance is critical.

IMPORTANT: For environments with more than 500 clients using the SMB protocol to access the solution, a larger-sized virtual machine type and/or additional DSX nodes are strongly recommended. Additional Data Store disks can be added non-disruptively and without downtime post-deployment.

Deployment Steps

1. Open a web browser (Chrome recommended), and point and navigate to https://portal.azure.com to log in with your Azure account.
2. Navigate to the Marketplace.
3. Search for Hammerspace.
4. Select either the BYOL or PAYGO product listing.

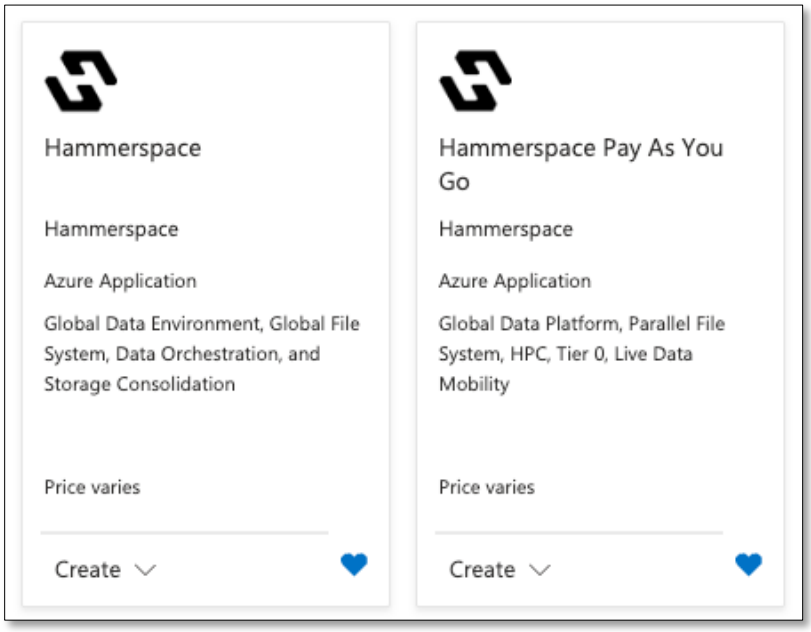

Figure 1

5. Select the subscription to use for the deployment.
6. Select **Hammerspace 5.2**

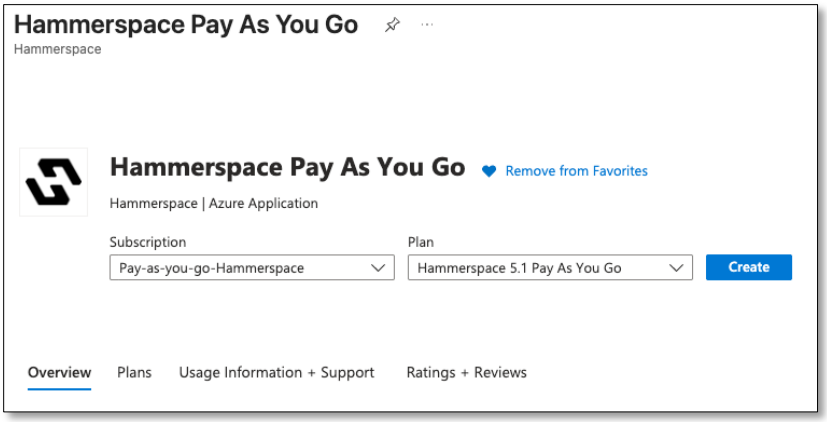

Figure 2

7. Click **Create** to begin the five-step deployment.

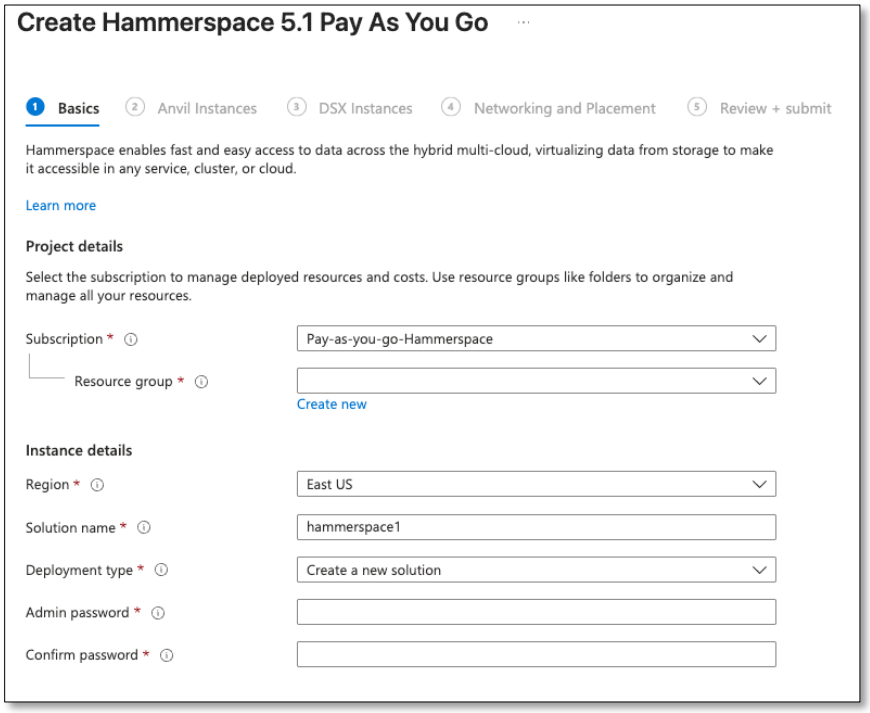

Figure 3

Setting	Value
Project details	
Subscription	Select desired subscription.
Resource group	Click Create new and provide a name in the pop-up menu.
Instance details	
Region	Select a region from the dropdown menu.
Solution name	Give the deployment a name.
Deployment type	Select Create a new solution (unless you are adding DSX nodes).
Admin password	Create a password.
Confirm password	Confirm the password.

8. Click **Next** at the bottom of the page.

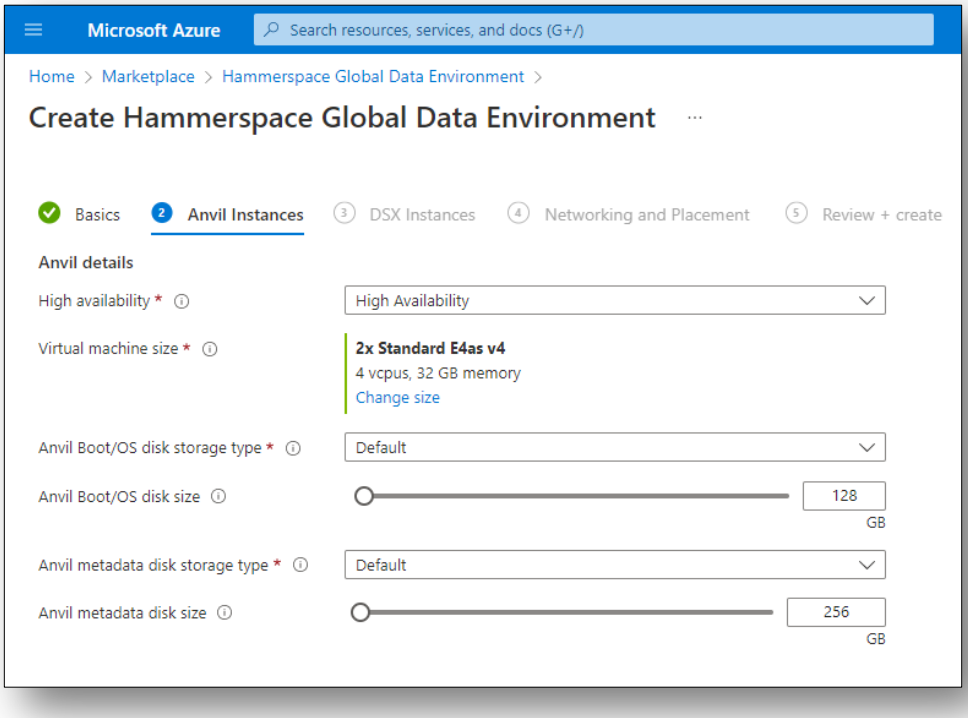

Figure 4

Settings for Anvil Instances tab

Setting	Value
High availability	Select High Availability or Standalone from the dropdown menu.
Virtual machines	Accept the default selection or click **Change size**.
Boot/OS disk type	Select disk type for the system binaries and libraries.
Boot/OS disk size	200 GB recommended minimum.
Metadata disk storage type	Select disk type to suit performance and cost requirements.
Metadata disk size	200 GB recommended minimum.

9. Click **Next** at the bottom of the page to proceed to the DSX Instances tab.

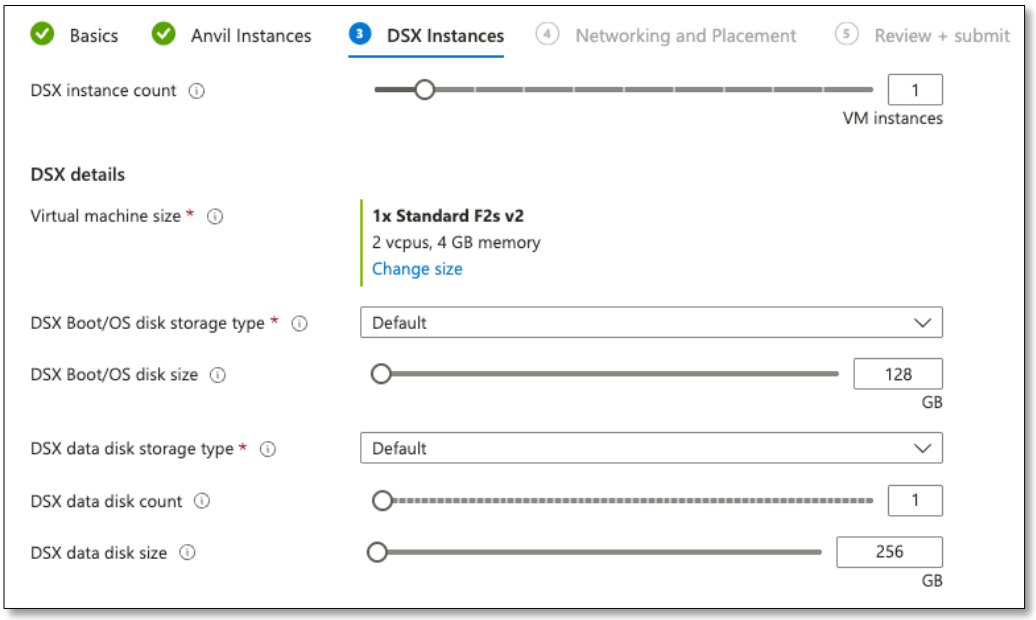

Figure 5

Settings for DSX Instances tab

Setting	Value
DSX instance count	Select the number of DSX VM instances to deploy.
DSX details	
Virtual machine size	Accept the default selection of click **Change size**.
Boot/OS disk type	Select disk type for the system binaries and libraries.
Boot/OS disk size	100 GB recommended minimum.
Data disk storage type	Select disk type to suit performance and cost requirements.
DSX disk size	500 GB recommended minimum.

10. Click **Next** to proceed to the Networking and Placement tab.

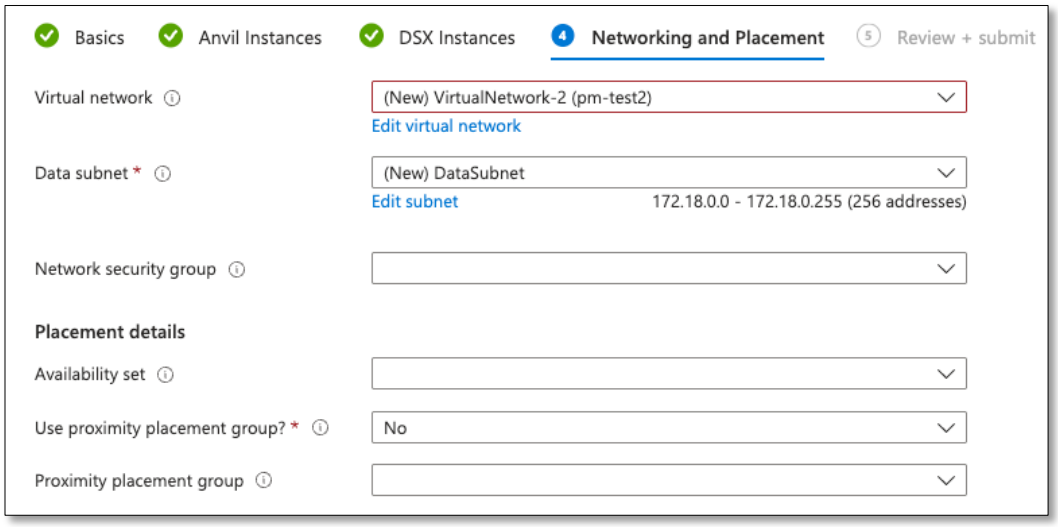

Figure 6

Setting for Networking and Placement tab

Setting	Value
Virtual network	Select from the dropdown menu.
Data subnet	Select from the dropdown menu.
Network security group	Select from the dropdown menu or leave blank
Placement details (these are optional)	
Availability set	Select an existing AS or leave blank to create a new AS.
Use proximity placement group	Optional
Proximity placement group	Optional

11. Click **Next** to review the configuration.
12. Click **Create** (or use the Previous button to make edits).

Post-Deployment Tasks

Once the deployment completes, you should see the following screen:

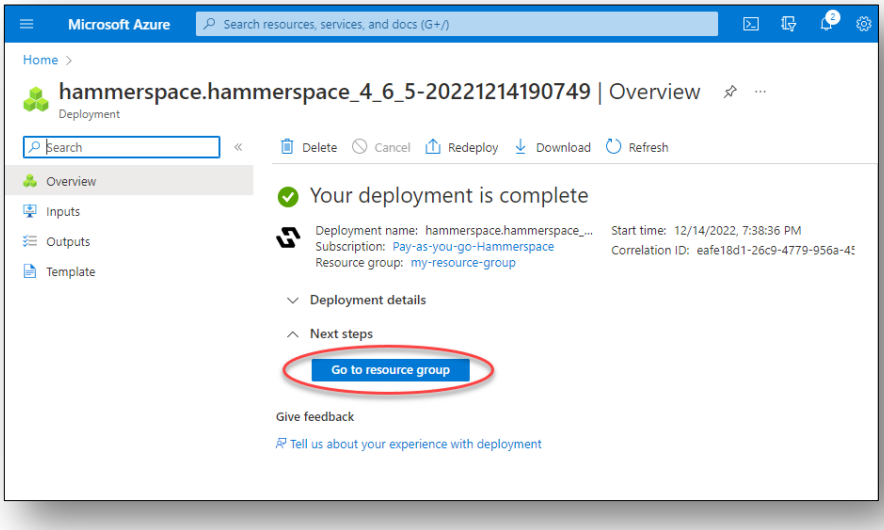

Figure 7

1. Press **Go to resource group** to proceed.

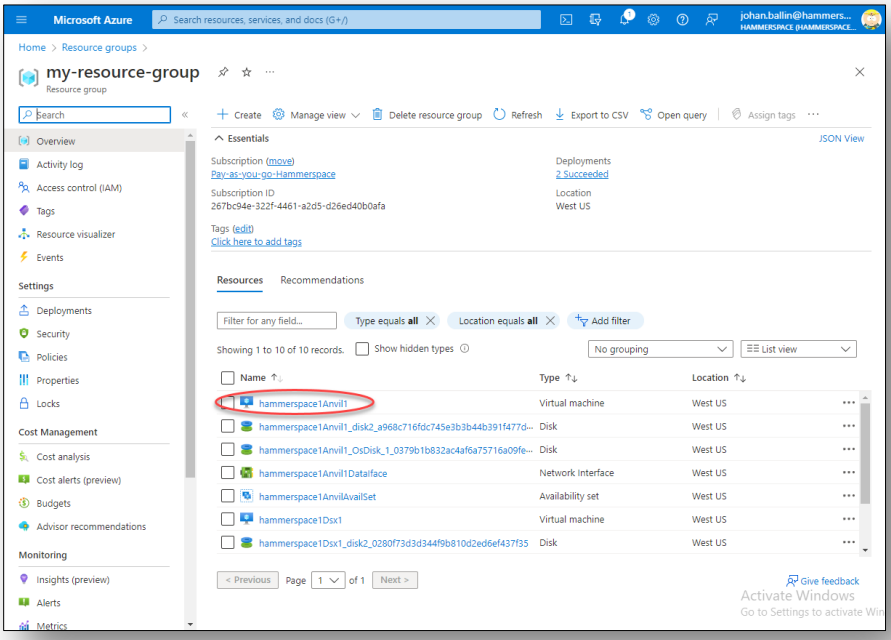

Figure 8

2. Click the Anvil hyperlink in your resource group to obtain the IP address of the Management GUI and CLI.

Hammerspace Management GUI

Point your web browser (Chrome browser recommended) to the IP address obtained from the Anvil virtual machine in your resource group. The IP address alone is usually sufficient, as Hammerspace will redirect to HTTPS and TCP port 8443, for example, https://10.41.1.6:8443.

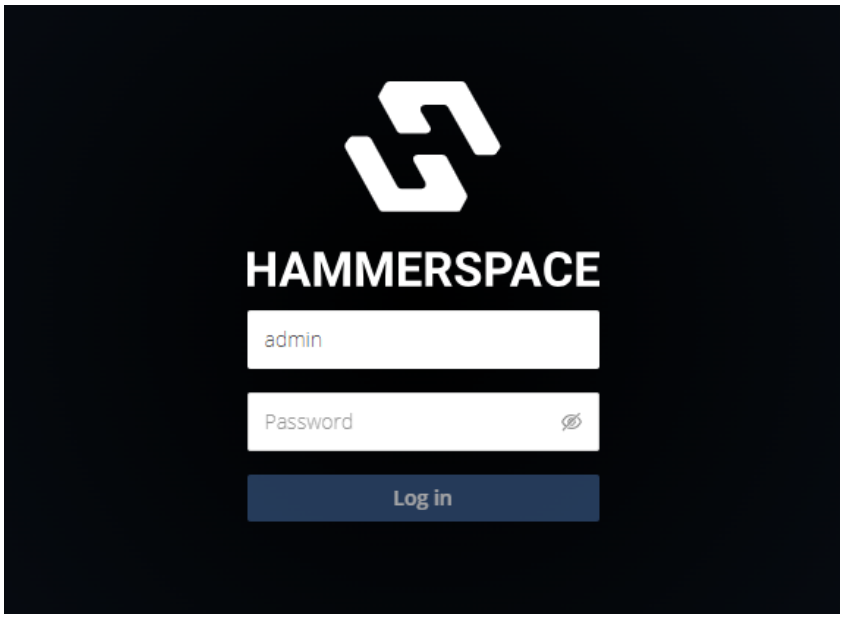

Figure 9

- Enter username and password in the form fields:

  Username: admin

  Password: *The password you created in "Step 1 – Basics"*

When you initially log in, a pop-up window will prompt you to accept the Hammerspace EULA (End User License Agreement). This only occurs once.

Validating the Deployment with the Management GUI

From the gear icon in the left navigation pane, select the **Network** tab. All Anvil and DSX nodes provisioned through the deployment template should be visible here.

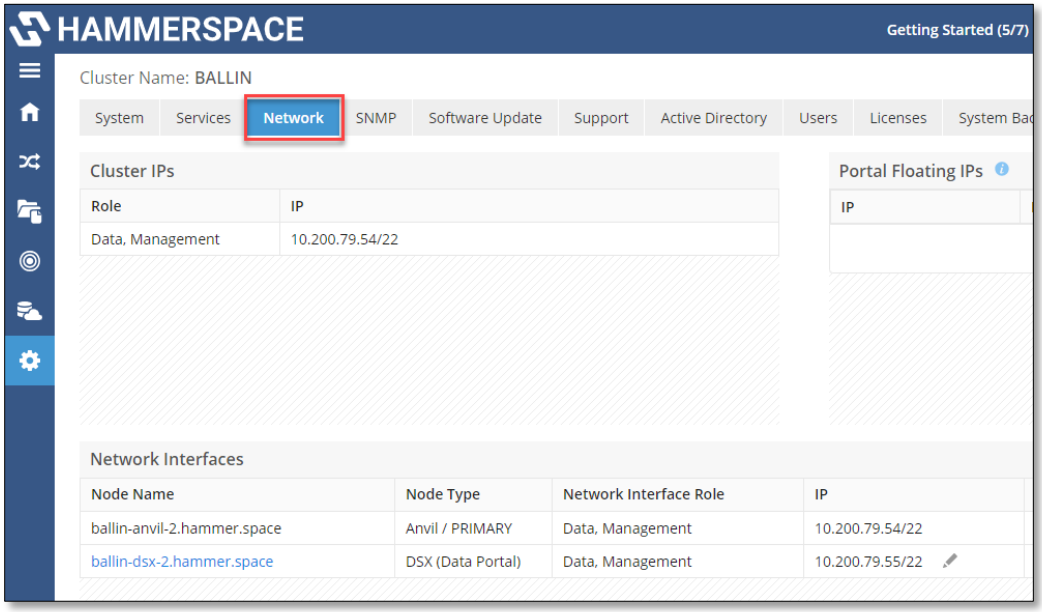

Figure 10

IMPORTANT: Please take note of the DSX IP address(es) and or hostname(s). The DSX node(s) should contain the key term “Data Portal”. This is the mount point for all front-end protocols, such as SMB (v1, 2, and 3), NFS (v3.0 and 4.2), and the Kubernetes Container Storage Interface (CSI driver).

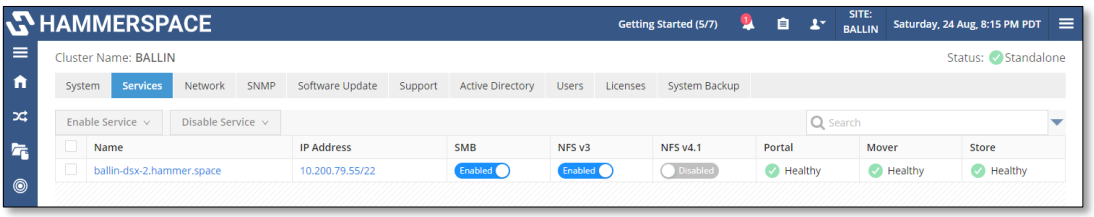

Figure 11

The **Services** tab validates that the Data Portal, Data Mover, Store, as well as SMB and NFS protocols are up and running and ready to use.

Hammerspace Admin CLI

The Admin CLI provides command-line control of system configuration and provides parity with the Management GUI. It is a restricted shell also known as a CLISH. To access the Admin CLI, open a terminal session (or use an SSH client) to connect via SSH.

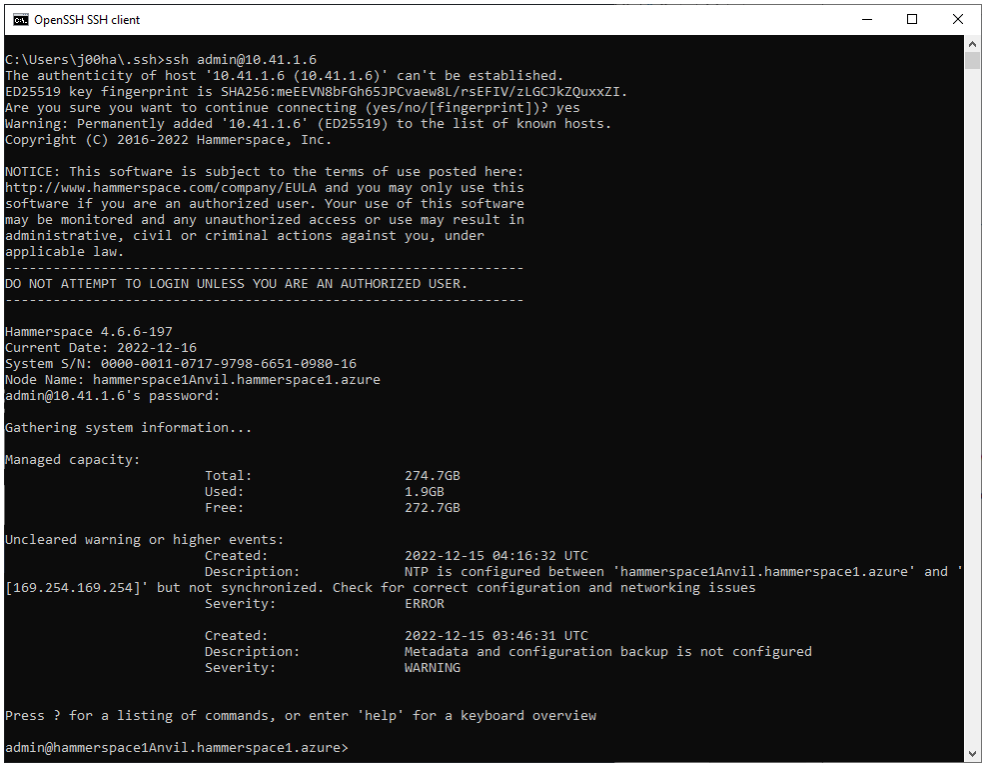

Figure 12

If using a terminal client, the command is:

```
$ ssh admin@<anvil hostname | ip address>
```

The terminal window also notifies us that the NTP configuration is erroneous or missing. Fix that by using the Hammerspace Admin CLI to enter the commands:

```
anvil> ntp-config --servers-clear
anvil> ntp-config --servers <ntp-server>
```

NOTE: You can replace the command with a NTP server or server pool of your choice. We have used an example from https://www.ntppool.org/en/. Choose the option that best suits your organization.

Appendix A: Definition of Terms

Anvil – Hammerspace metadata node. This virtual machine contains the administrative GUI and CLI as well as metadata and performs multiple critical functions in a Hammerspace deployment.

Availability Set – is a logical grouping of VMs that allows Azure to understand how your application is built to provide for redundancy and availability. Each availability set can be configured with up to three fault domains and twenty update domains. These configurations cannot be changed once the availability set has been created. Update domains indicate groups of virtual machines and underlying physical hardware that can be rebooted at the same time. Please refer to the Microsoft documentation on Availability Sets for more information.

Availability Zone – Azure availability zones are connected by a high-performance network with a round-trip latency of less than 2ms. They help your data stay synchronized and accessible when things go wrong. Each zone is composed of one or more datacenters equipped with independent power, cooling, and networking infrastructure. Availability zones are designed so that if one zone is affected, regional services, capacity, and high availability are supported by the remaining two zones.

DSX – Hammerspace data services node (Data Service eXtensions). This virtual machine provides the protocol front-end services, such as SMB, NFS, and Kubernetes CSI. It also controls backend connections and services to third-party storage volumes, data mobility services, as well as, optionally, provides directly attached storage.

Global Data Environment – provides a parallel global file system with file-granular declarative control of data. Hammerspace Objectives provides highly customizable metadata tagging and descriptors which, in turn, can be used in declarative actions that allow organizations to control business outcomes of their data. Please view the Hammerspace website for more information.

Mover – also known as the Data Mover. This provides non-disruptive and end-user transparent data mobility. Administrators of Hammerspace can move live data declaratively between backend storage systems and volumes without any disruption to productivity.

Portal – This is hosted by the DSX node and is the mount point for all front-end protocols (SMB, NFS, and the Kubernetes CSI driver) that make up the Hammerspace Global File System.

Proximity Placement Group – is a logical grouping used to make sure that Azure compute resources are physically located close to each other. Proximity placement groups are useful for workloads where low latency is a requirement. Please refer to the Microsoft documentation for additional information.

Region – Each Azure region features datacenters deployed within a latency-defined perimeter. They're connected through a dedicated regional low-latency network. This design ensures that Azure services within any region offer the best possible performance and security.

Resource Group – is a logical container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Generally, add resources that share the same lifecycle to the same resource group so you can easily deploy, update, and delete them as a group.

Store – The directly attached storage disks on DSX, such as the ones provisioned during Step 3 in the deployment process.

Appendix B: DSX High Availability Configuration

Microsoft Azure networking does not provide support for Gratuitous ARP. Therefore, it is required to configure an Azure Load Balancer to support high availability. DSX high availability in Microsoft Azure requires configuring the following items at a minimum:

- Azure Load Balancer
  - Frontend IP address
  - Backend pool
  - Health probe
  - Load balancing rule

IAM Permissions Required

To configure an Azure Load Balancer, the primary Azure Role-Based Access Control (RBAC) role required is Network Contributor. This role provides the necessary permissions to manage network resources, including creating, configuring, and managing Azure Load Balancers.

For a more granular approach, you can create a custom role with only the specific permissions needed for load balancer operations, adhering to the principle of least privilege. This can be achieved by including actions like **`Microsoft.Network/loadBalancers/*`**.

Azure Load Balancer Configuration

This section requires the following configurations:

- Frontend IP address
- Backend IP pool
- Inbound load-balancing rules

1. Log in to the Azure Portal, https://portal.azure.com.
2. Search for “load balancers” in the top center search bar, as show below:

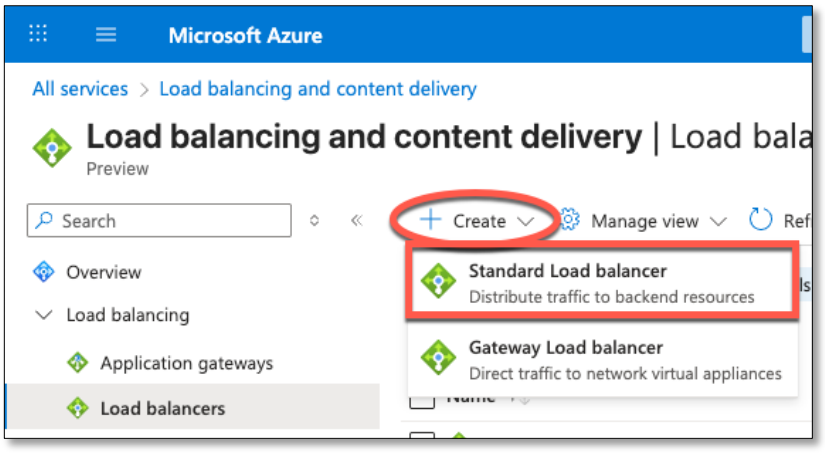

Figure 13

3. Select **Load balancers** from the dropdown search menu.
4. Select **Standard Load balancer**.

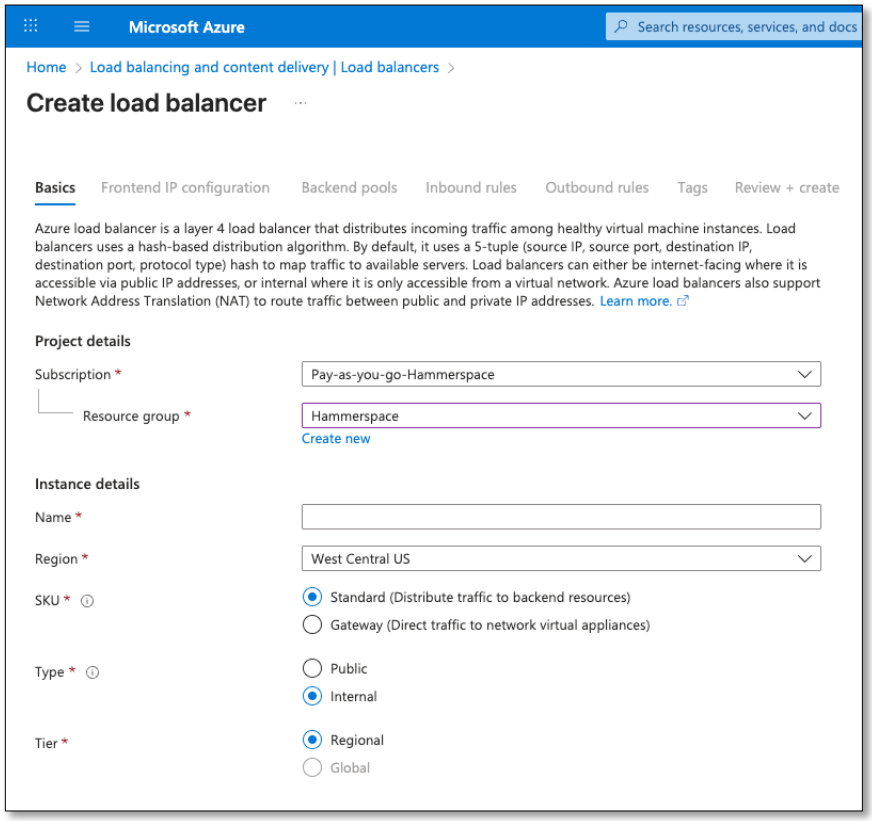

Figure 14

Load-balancer settings

Setting	Value
Project Details	
Subscription	Select your subscription.
Resource group	Select the target Resource group containing the Hammerspace nodes.
Instance Details	
Name	Give the load balancer a name.
Region	Select the Azure Region.
SKU	Standard.
Type	Internal.
Tier	Regional.

5. Select **Next: frontend IP configuration** at the bottom of the page.
6. Click +**Add a frontend IP configuration**.

Front-end configuration settings

Setting	Value
Name	Provide a name.
IP version	Select the IPv4 radio button.
Virtual network	Select the target network.
Subnet	Select the target subnet.
Assignment	Static.
IP address	Enter the frontend IP address for your load balancer.

7. Click Save at the bottom of the **Add frontend IP configuration** panel.
8. Select **Next Backend pools** at the bottom of the page.
9. Click **+ Add a backend pool**.

Back-end pool settings

Setting	Value
Name	Provide a name for the backend pool.
Backend Pool Configuration	Select the NIC radio button.

10. Click **+ Add** below the IP configurations subject heading.
11. When the side panel opens, check the DSX instances you wish to load balance.

12. Click **Add** at the bottom of the panel.
13. When the side panel closes, click **Save** at the bottom of the page.
14. Click **Next: Inbound rules**.
15. Select **+ Add a load balancing rule**.
16. Select the following when the **Add load balancing rule** panel opens.

Load-balancing rule settings

Setting	Value
Name	Provide a name for the load balancing rule.
IP version	Select the IPv4 radio button.
Frontend IP address	Select the frontend IP address you previously configured.
Backend pool	Select the backend pool you previously configured.
HA ports	Check.
Protocol	TCP
Port	Turns off when selecting High Availability Ports
Backend port	Turns off when selecting High Availability Ports
Health probe	Click to create a health probe (required).
Session persistence	Source IP
Idle timeout	30.
Enable TCP Reset	Check.
Enable Floating IP	Unchecked.

Health-probe settings

Setting	Value
Name	Give the health probe a name.
Protocol	Select TCP.
Port	22 (suggested), but it can be any open port.
Interval	5

17. Click **Save** at the bottom of the panel.
18. Click **Next: Outbound rule**.
19. Click **Next: Tags**.
20. Optionally, create tags for the load balancer.
21. Select **Next: Review + create**.
22. After reviewing that the configuration is correct, select **Create**.

Example Topology Diagram

The following simplified diagram illustrates a client mounting the virtual IP address of the Azure Load Balancer. We have omitted the illustration of the Anvil HA configuration to simplify and highlight how DSX high availability works with Microsoft Azure.

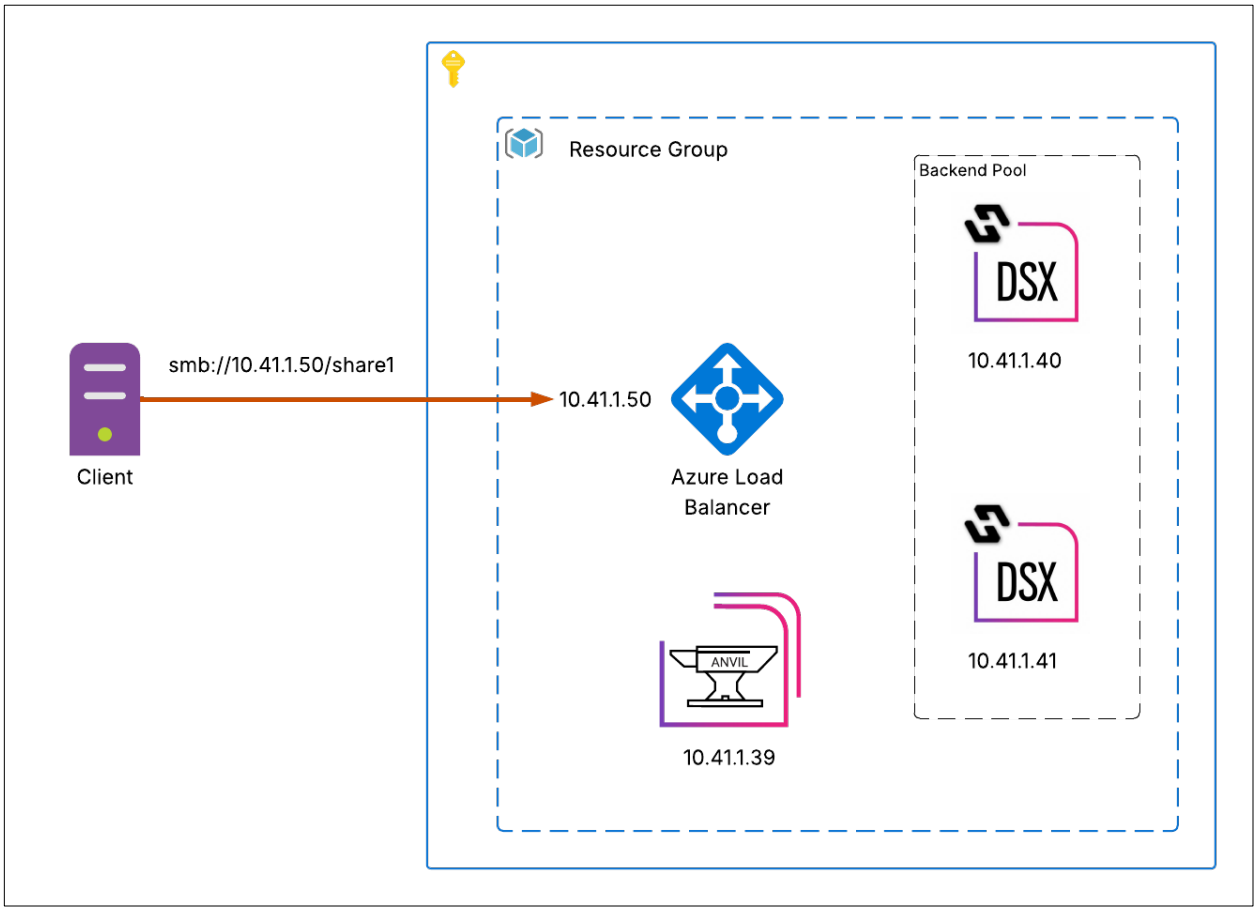

Figure 15

Appendix C: Architectural Reference Diagrams

Standalone Anvil and DSX

The minimum configuration of a Hammerspace instance consists of a single Anvil and a single DSX. Each instance requires at least two disks: one for the boot partition and the second for data or metadata.

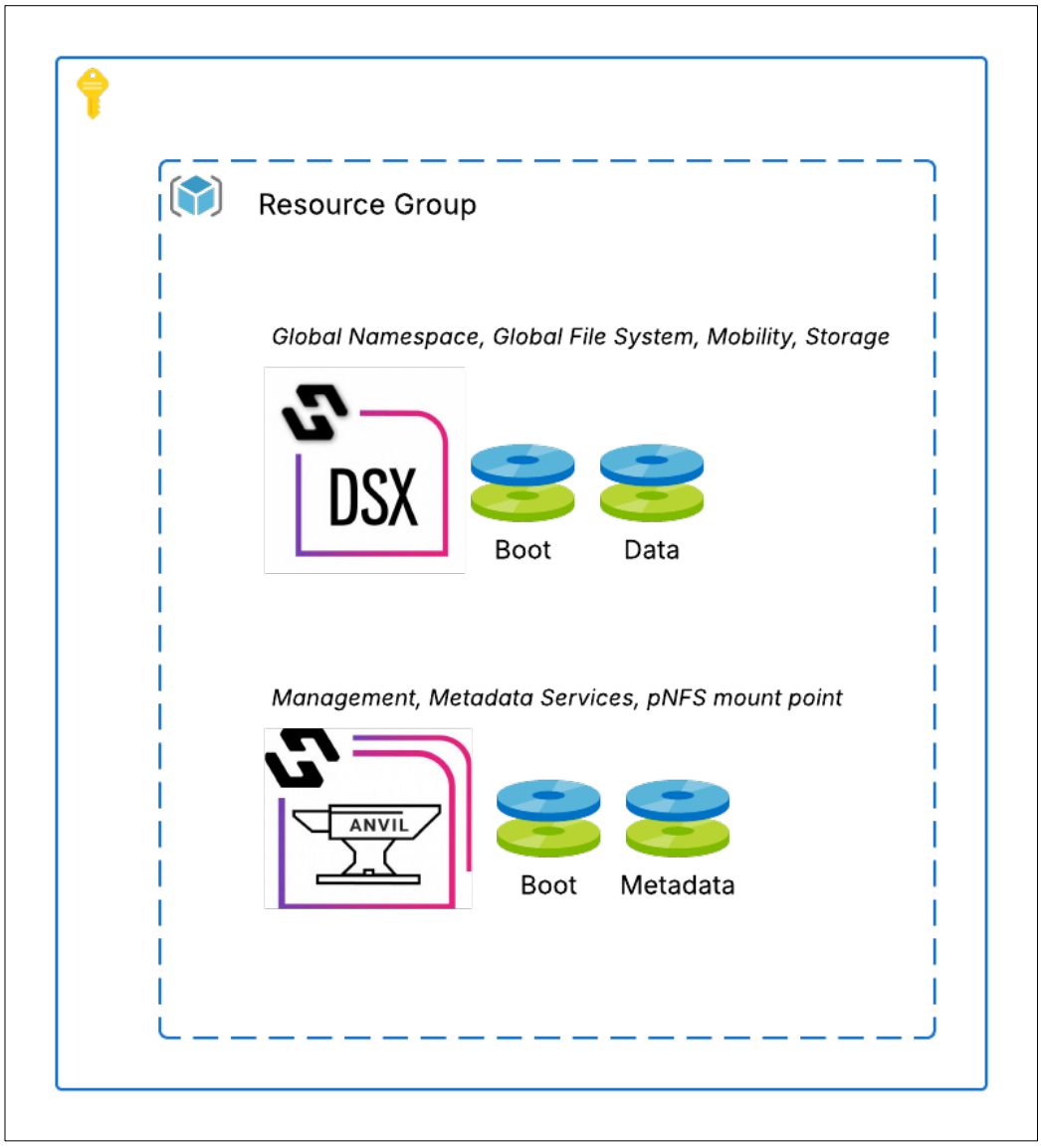

Figure 16

High Availability Anvil and Standalone DSX

The following image illustrates a single Anvil and a highly available configuration of DSX nodes. Microsoft Azure requires configuring an Azure Load Balancer to support high availability.

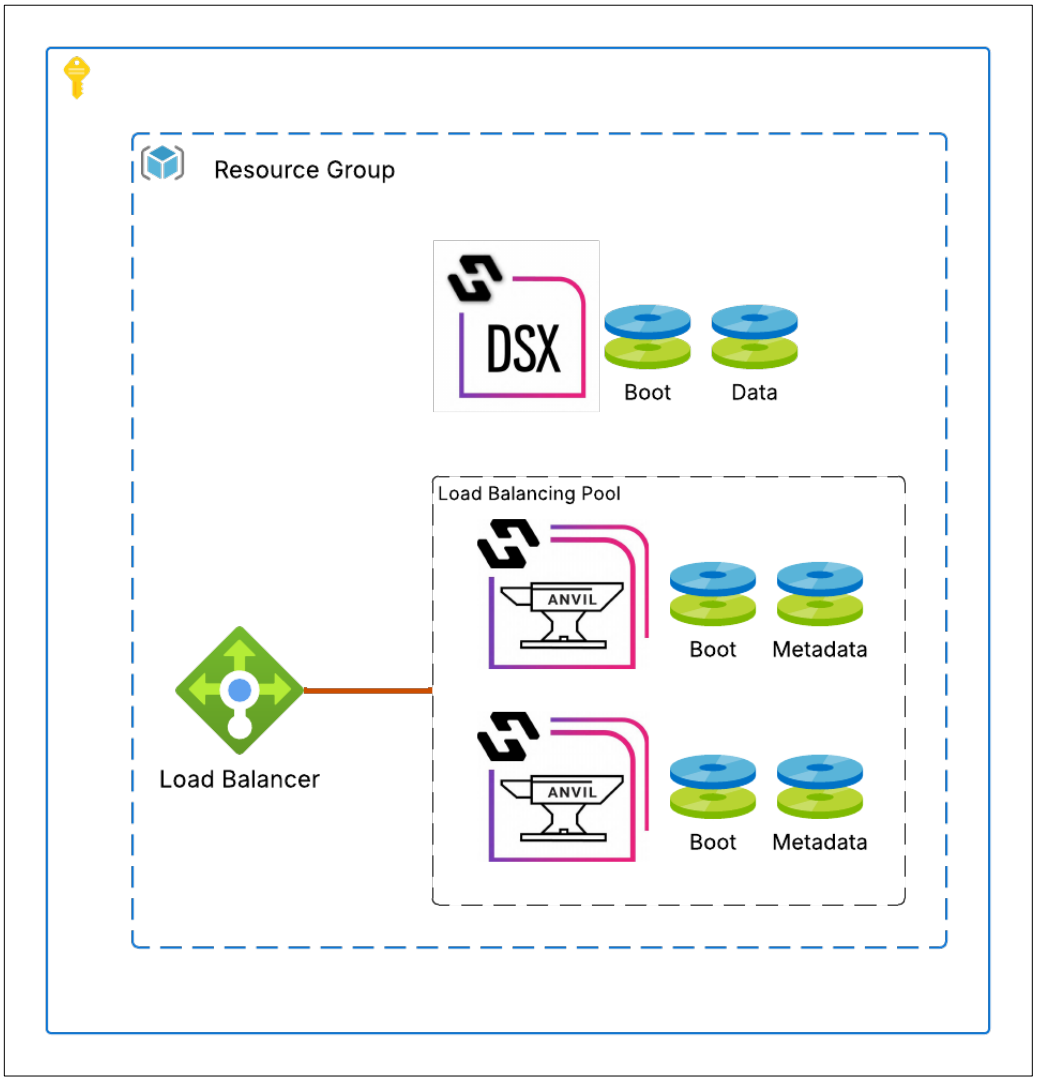

Figure 17

High Availability Anvil and DSX

Microsoft Azure networking does not provide support for Gratuitous ARP and, thus, cannot support Floating IP addresses or dynamic high-availability solutions, such as VRRP. Therefore, high availability requires configuring an Azure Load Balancer, as illustrated in the following image.

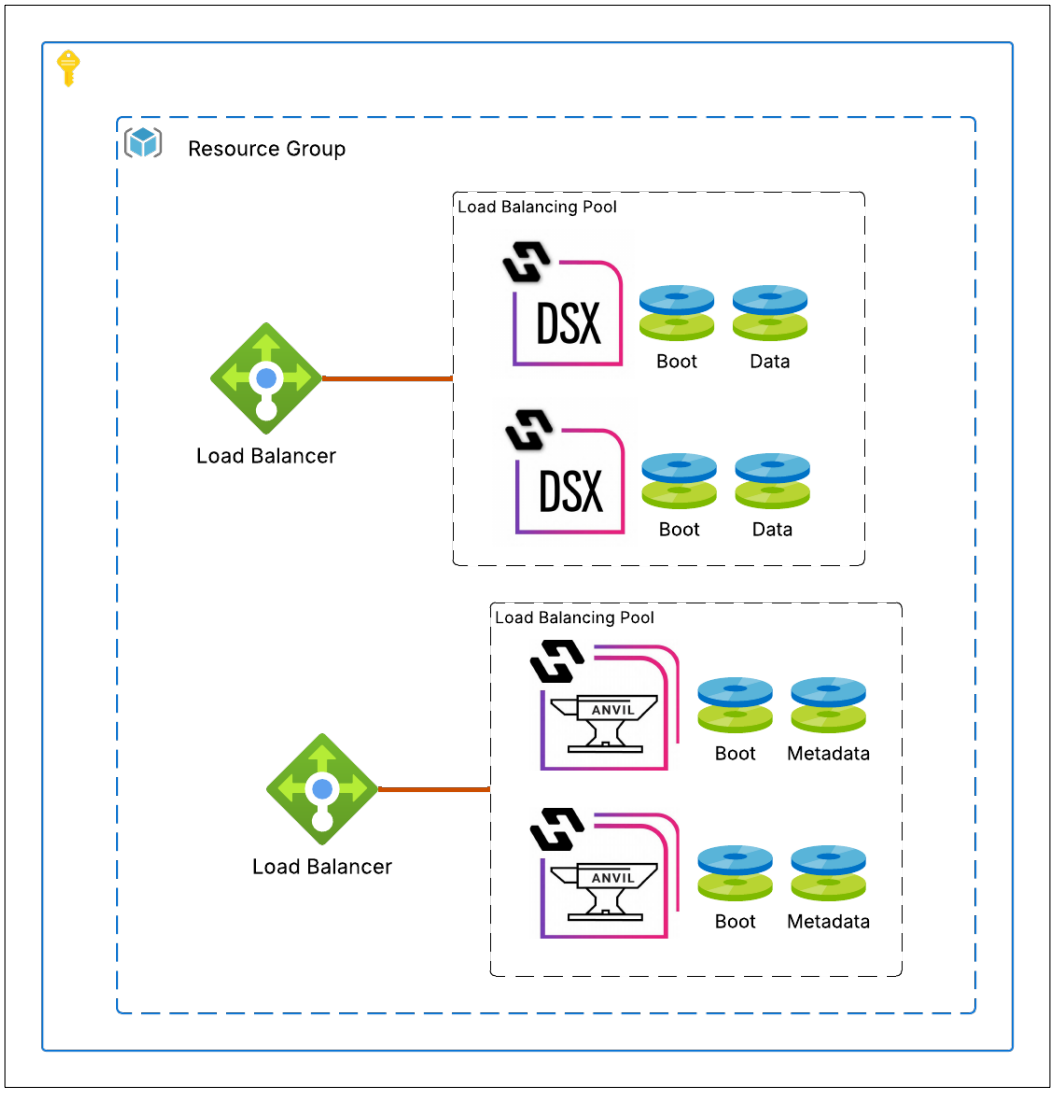

Figure 18

Data Path: SMB and NFSv3

The following image illustrates the read/write data path between an NFSv3 or SMB client and a minimal Hammerspace instance. The DSX node is the mount point and delivers the global namespace and global file system. The Anvil node controls metadata and data management, data orchestration, and all administrative functions. It also provides the Hammerspace Management GUI and Admin CLI.

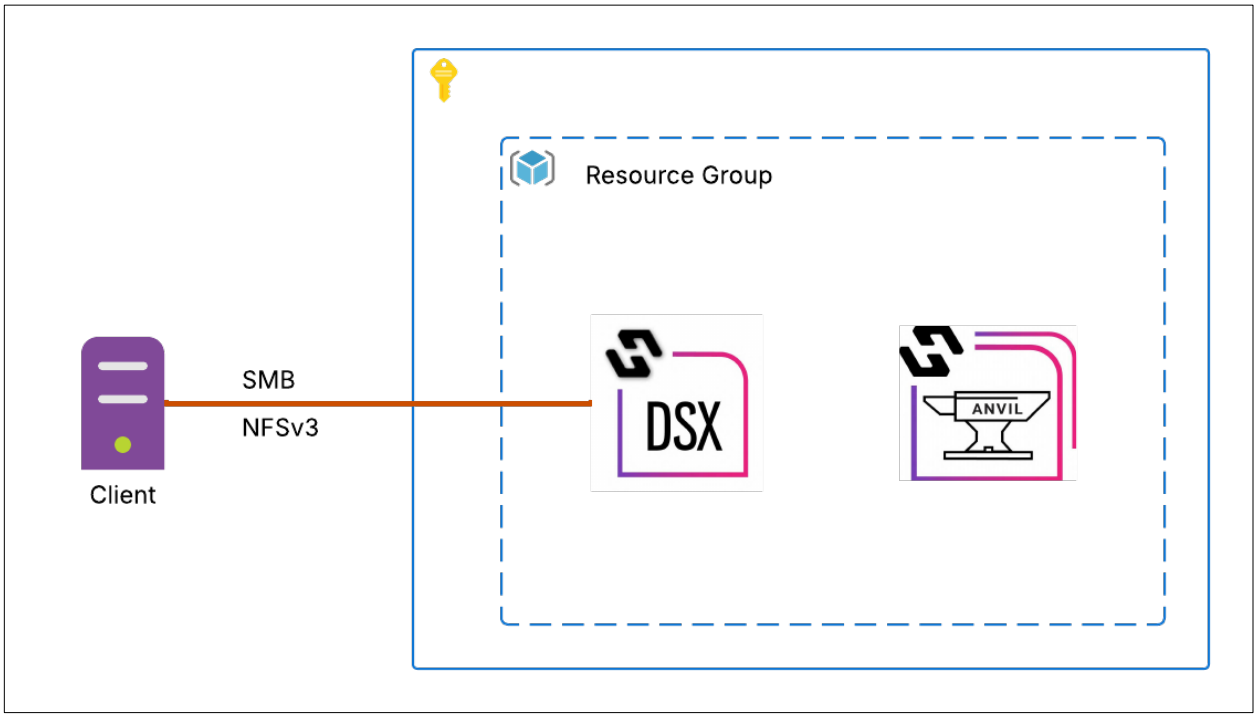

Figure 19

Data Path: Parallel NFS (NFSv4.2)

Parallel NFS is ideal for high-performance use cases. The data and control connections are separated for greater parallelization. They are suitable for the most demanding workloads, including AI training and inference, genomic sequencing, rendering, and other HPC scenarios requiring extreme performance.

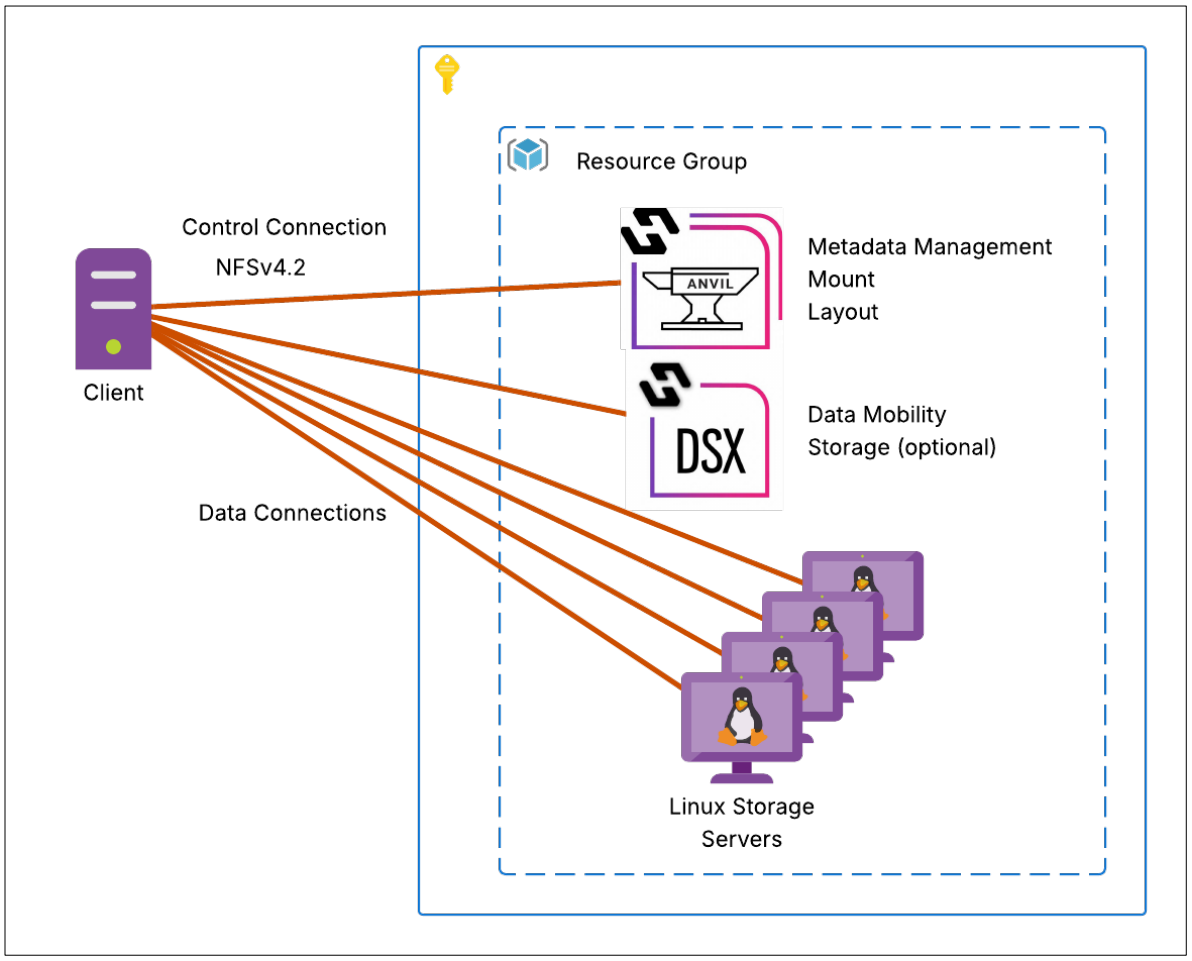

Figure 20

Appendix D: Documentation and Support

Azure References

Getting Started

https://azure.microsoft.com/en-us/get-started

Networking

https://learn.microsoft.com/en-us/azure/networking/

Compute

https://learn.microsoft.com/en-us/azure/virtual-machines/

https://learn.microsoft.com/en-us/azure/?product=compute

Storage

https://learn.microsoft.com/en-us/azure/?product=storage

Security

https://learn.microsoft.com/en-us/azure/?product=security

Azure Load Balancer

https://learn.microsoft.com/en-us/azure/load-balancer/

https://learn.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-internal-portal

IAM Permissions

https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations

Hammerspace Resources

https://hammerspace.com/azure/

https://hammerspace.com/resources/

https://hammerspace.com/support/

support@hammerspace.com