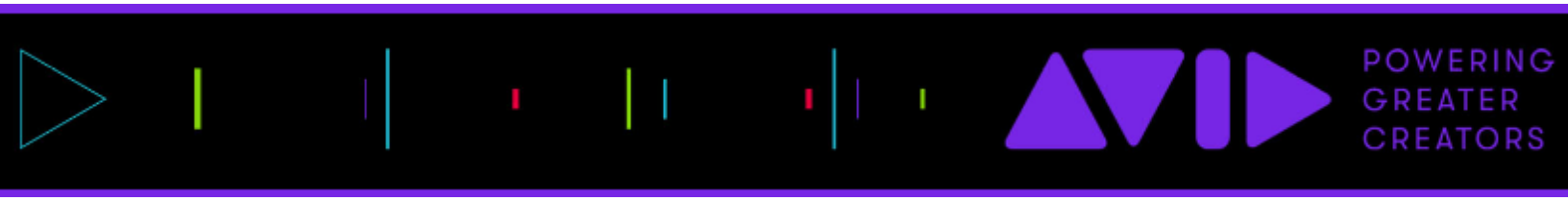
Avid Technology Cloud Team



Secure Cloud Editorial Production

Best Practices Guide

"Editorial in the Cloud"

20-Aug-20

Contents

Version	Comment	Date
1.0.1	Initial Release	8/20/20

1. Introduction.

1.1 Overview and Context.

Content production activities can be characterized into two core phases: **content creation** and **content distribution.**

Cloud based infrastructure and products are increasingly being used for content distribution which first began with media content that is essentially editorially complete and applying further processing to be able to then distribute that content to rights holders and more increasingly direct to end consumers. This shift has been transformational for business operations accompanied with a change from historically high capital expenditure (CAPEX) operational models towards an on-going operational expenditure model (OPEX) with resulting benefits of scalability, resilience, flexibility and agility.

By contrast, core content creation activities that feed into distribution depend on the ability to take content (e.g. footage) from multiple sources and create editorially complex media (e.g. programmes or films). This requires a Picture Editor to be able to seamlessly work with high-resolution and high-bitrate content with low latency in a secure fashion from any location. Once a futuristic notion, cloud hosted rich craft editorial applications are increasingly being used by some of the largest media companies around the world to securely edit content within scalable and high-performance environments across continents.

The cloud also allows the potential for greater collaboration while decreasing time to delivery for editing operations as more work can be done faster by disparate teams working together. It empowers media organizations to spin up additional resources to take on more projects without the capital expense required to set up and maintain on-premises environment. This has great potential to drive higher efficiency, leverage talent from any geographic region, and deliver content faster to distribution.

For content creation, the activity epicentre is focused around post-production activities and processes – especially video and audio editing. This poses a series of challenges, not least of which concerns **security**.

1.1 Use of this Guide.

It is important that this guide should be used in combination with additional sources of information, especially any existing organisational production operations and IT security policies or standards. For each prospective deployment it will be the business requirements in combination with appropriate security controls that will inform as to what extent the guidance given in this guide should be applied, adjusted or relaxed.

The guidance given in this guide should be thought of as a set of 'tools' from which to pick and choose which control should be applied for your particular situation. In some cases, it is likely that additional controls or measures may need to be implemented in addition to those described in this guide.

It is recommended that you initially read this guide in the order it is written in order to familiarise yourself with the content. Subsequently you can reference those topics or controls as required and apply or modify them as deemed appropriate.

Section 1 (this section) provides an introduction to the use and purpose of this guide.

Section 2 introduces the initial use case for further discussion and will be expanded upon in later sections.

Section 3 describes and examines various security topics and introduces the core controls with which each can be addressed.

Section 4 contains a selection of 'Playbooks' related to each of the topics introduced in earlier sections and the practical steps that should be taken or links provided to external information such as how-to or implementation guides.

1.2 Purpose of this Guide.

Through examination of a simple hypothetical **'Video Editorial in the Cloud'** deployment, this guide illustrates some general principles regarding security when using **Avid Products and Solutions** deployed in **Microsoft Azure**. This includes descriptions of **best practices** as well as **playbooks** for various scenarios in order to secure and harden a cloud editorial environment.

Although a hypothetical deployment is used as the basis for discussion, the example forms the core for similar real-world deployments used by post-production clients who are using a cloud hosted editorial system running in their own Enterprise Azure cloud subscriptions. Based on experience, these guidelines describe how users can plan and create a secure deployment of Avid Media Composer and the Avid NEXIS file system integrated with Azure cloud storage.

This setup will enable seamless editorial workflows, using the **Teradici** (PCoIP) client to access and edit content remotely and securely, and optionally may use a file transfer solution (for example **Signiant**, **Aspera** or **FileCatalyst**) to provide accelerated and secure file transfer from on-premise to an Avid NEXIS file system in Azure.

The guidelines below provide guidance for a technical audience, including media engineers with some Azure deployment experience. Prior experience with Azure deployments is highly recommended for a reasonable expectation of success.

This is a 'living' document that focuses on securing aspects relating specifically to Avid based editorial deployments and will be updated from time to time. Please check that you are using the latest version of this document.

Where possible Cloud industry best practices should be followed, and you should have some familiarity with the following principles:

- Use of strong network controls (Azure Virtual Networks)
- Virtual segmentation using Virtual Network Subnets
- Zero trust approach (use of mechanisms such as Network Security Groups and Application Security Groups)
- Principles and use of dedicated links (VPN, Azure ExpressRoute)
- Protocol exposure avoidance (RDP/SSH)

For additional information, please see the following guide: https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices

2.Architecture and Deployment Patterns.

There is often no single deployment model that will fulfil every production need especially where editorial teams using multiple products and more complex infrastructure is needed to support a wider set of collaboration and business activities and whose implementation will likely vary from one production to another.

There may also be need for additional capabilities such as connecting geographically distributed teams and workgroups due to business reasons or to exploit the best talent wherever they may be located. For high-value productions the pressure to ensure security and control over what can be accessed and from where is paramount and requires careful consideration of options before staging any environment for real-life use. In this document we will review some potential security concerns and mitigating patterns.

These security concerns and patterns can be thought of as **building blocks** which when implemented in combination can form the foundation for implementing a secure production environment in a virtual or cloud-based environment. In this way, even in the case of dissimilar target deployments, the same core concepts can still be understood and applied as needed.

2.1 Example Core Standalone Editorial Group.

The most basic building block is a single standalone editorial workgroup consisting of the following:

- Avid **Media Composer** editing application(s) using **Teradici** PCoIP technology used for remote edit desktop access.
- Avid **NEXIS** cloud storage.
- Additional components to support the editorial workgroup (e.g. a secure accelerated file transfer solution such as **Signiant Media Shuttle**, **Aspera**, **FileCatalyst** or equivalent).

Conceptually this deployment is illustrated below (**Core Standalone Editorial Workgroup – Figure 1**).

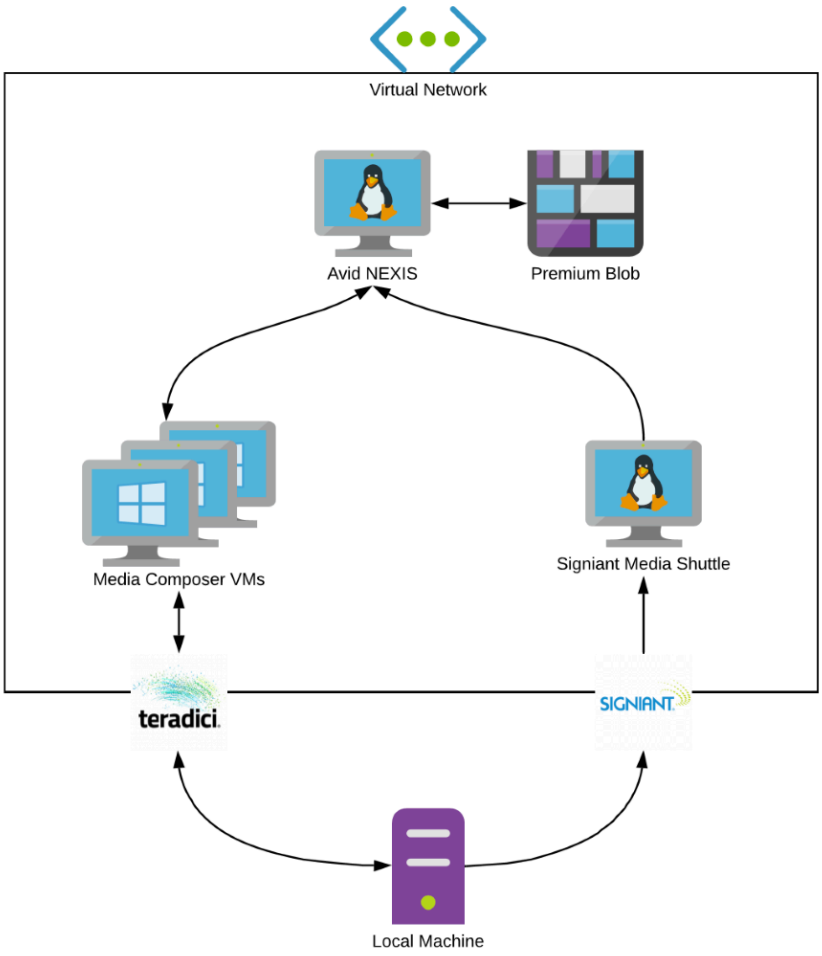


Figure 1 – Core Standalone Editorial Workgroup

Considered as a deployment in Microsoft Azure, this consists of several Virtual Machines (for Media Composer editor applications, Avid NEXIS and accelerated file transfer application VM) and associated Microsoft Azure infrastructure services such as Resource Groups, Virtual Networks (VNets) and Storage Accounts. This is illustrated below (Figure 2 - Core Standard Editorial Workgroup – Azure deployment).

When creating the respective resources using the Microsoft Azure administration portal, the level of public accessibility to those resources is dictated by a combination of the settings applied during creation and post configuration settings applied to the respective VM or virtual network subnet Network Security Group (NSG) filters, for example opening ports to allow external Teradici PCoIP remote desktop or RDP access to the VM's. However, some automated provisioning or orchestrated deployment solutions may make assumptions or apply defaults which may not be appropriate for the intended target scenario when we also consider additional security needs. For demo and test purposes these defaults may be acceptable but for production use we may want to consider what additional mechanisms we can bring to bear in order to enforce higher security and reduce the visible attack surface.

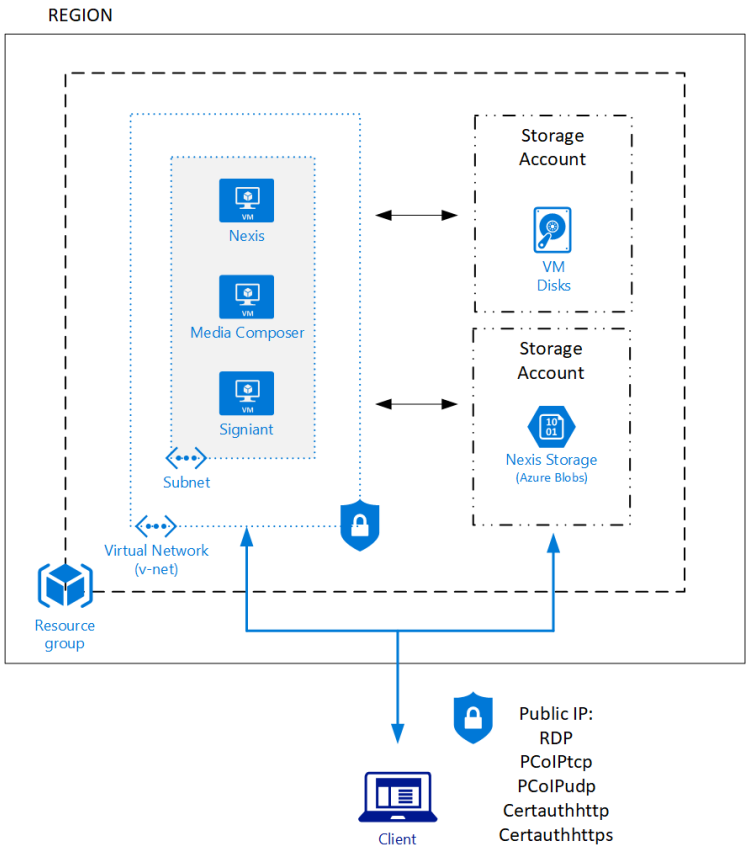


Figure 2 – Core Standard Editorial Workgroup – Azure deployment

Given the deployment scenario illustrated in Figure 2 (Core Standard Editorial Workgroup – Azure deployment), we will make the assumption that a user can currently access the environment providing they have been given valid connection and authentication credentials by an administrator. Let us assume a default deployment that allows users and administrators to publicly connect and access the VM's via **Remote Desktop Protocol (RDP), Secure Shell (SSH)** or via **Teradici PCoIP** protocol (in the case of the **Media Composer VM**) from any client device (laptop, workstation or Teradici Zero Client).

Some additional opportunities are now possible to further reduce the potential attack surface and strengthen security of the environment for production use, some examples are (not exhaustive):

- Implement secure VPN or Azure ExpressRoute connectivity
- Utilize a 'Jumpbox' or 'Bastion' device for separation of administrative and production user functions
- Re-configure Storage Accounts to be accessible only by the resources that rely on them.

These are only some of the potentially many optimisations that can be performed, and their applicability depends on the particular business use case and some may not be required or possible to implement for some situations.

Further information on staging a typical environment can be found in Section 4.1 - Playbook: Deploy Core Environment.

Adjustments can be applied to strengthen security and it is imperative that you choose and configure appropriate security options to align business operational needs with the official network and IT security policies of your organization.

2.2 Glossary of Terms.

Term	Definition
Subscription	A subscription refers to the logical entity that provides entitlement to deploy and consume Azure Resources. Your deployed Resources and Virtual Networks (VNet) are scoped to a subscription. You can implement multiple virtual networks within each Azure Subscription and Azure Region (see below).
Region	A region is a set of data centre's deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network. Microsoft Azure features 52 regions around the world, with plans announced for 6 additional regions. This gives customers the flexibility to deploy applications where they need to.
Location	A location is the Azure Region where the deployment will provision resources. It is recommended for this to be geographically close to the location where the editors will be.
Resource Group	A resource group is a logical container for the deployed resources (Vnet, VM's etc) inside of Azure. You can either select an existing resource group or create a new resource group for a deployment.
Storage Account	A storage account contains all of your Azure Storage data objects: blobs, files, queues, tables, and disks. The storage account provides a unique namespace for your Azure Storage data that is accessible from anywhere in the world over HTTP or HTTPS. Data in your Azure storage account is durable and highly available, secure, and massively scalable.
Subnet	Subnets ("Subnetworks") enable you to segment the virtual network into one or more sub-networks and allocate a portion of the virtual network's address space to each subnet. You can then deploy Azure resources in a specific subnet. Just like in a traditional network, subnets allow you to segment your VNet address space into segments that are appropriate for the organization's internal network. This also improves address allocation efficiency. You can secure resources within subnets using Network Security Groups.

Virtual Network (VNet)	A Virtual Network (VNet) is a representation of a deployed network in the cloud. It is a logical isolation of the cloud dedicated to your subscription. Similar to physical data networks, VNets provide the connectivity infrastructure used by deployed resources to talk to each other. VNets communicate with other VNets in Azure, or with your on-premises IT infrastructure (e.g. using VPN or ExpressRoute) to create secure hybrid or cross-premises environments. VNets contain Virtual Network Subnets that can be used to segregate resources and assign traffic access rules using Network Security Group (NSG) policies.
CIDR	Classless Inter-Domain Routing (CIDR) notation is a shorthand representation of an IP address space. The combination of address space and number of bits specified in CIDR notation represents the subnet mask.
Address Space	When creating a VNet, you must specify a custom private IP address space using public and private (RFC 1918) addresses. Azure assigns resources in a virtual network a private IP address from the address space that you assign. For example, if you deploy a VM in a VNet with address space, 10.0.0.0/16, the VM will be assigned a private IP like 10.0.0.4.
Virtual Machine	Virtual Machines (VM) is an emulation of a host computer system that provides the functionality of a physical computer. An Azure VM gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs it. However, you still need to maintain the VM by performing administrative tasks, such as configuring, patching, and installing the software that runs on it.
Endpoint	An endpoint provides remote access to the services running on a virtual machine or service in an Azure environment. It has a private (Azure) address and optionally a public address that is specified while creating the endpoint.
ExpressRoute	ExpressRoute is an Azure service that lets you create private connections between Microsoft data centres and infrastructure in your on-premise or co-location facility. ExpressRoute connections do not go over the public Internet, and offer higher security, reliability, and speeds with lower latencies than typical connections over the Internet.
VPN	Virtual Private Network. A VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet. You can also use a VPN gateway to send encrypted traffic between Azure virtual networks over the Microsoft network

3.Security Toolkit.

3.1 Secure VPN or Azure ExpressRoute Connections

The default core deployment allows the Virtual Machines (VM's) to be accessed via public configured endpoints. This allows any authorized user to connect and access the VM's from any location that is able to reach the configured public endpoint either by IP Address or the host's public Azure fully qualified domain name (FQDN). Although convenient in some situations, it may not be desirable to expose the connection endpoints in such a public way and create a potential security risk (e.g. allowing the opportunity for other hostile actors to attempt to gain or deny legitimate users access.)

Conventionally there are two primary methods that can help in securing connectivity:

- Implement a **Virtual Private Network (VPN)** to secure connection traffic over the public Internet
- Implement **Azure ExpressRoute** to facilitate secure private on-Premise to Azure connectivity

A VPN connection utilizes a deployed virtual network gateway to send encrypted traffic between an Azure virtual network and an on-premise or users' device over the public Internet. A VPN may also be applied to securely connect two virtual networks (in Azure) for example to facilitate geographically distributed setups where collaboration between teams are required.

A VPN can help to secure connections between Azure virtual network resources and an on-premise location (called Site-to-Site VPN) and this will require the customer to provide a suitably compatible hardware-based VPN gateway device at the on-premise location and deploy an Azure VPN gateway in the cloud environment. Alternatively, where the need is to secure connections for individual users who are not able to connect using an on-premise hardware based VPN device but instead directly from their own devices then a Azure VPN gateway is still deployed in the Azure virtual network and the user in this case installs and runs appropriate VPN software on their own device to connect to and secure the communications to the Azure virtual network (called Point-to-Site VPN).

Traffic over a Site-to-Site or Point-to-Site VPN connection will generally traverse the public Internet and may be subject to variations in bandwidth, jitter and latency depending on moment to moment path conditions. Where a more deterministic level of performance is required (with respect to bandwidth, jitter, latency) and again to guarantee a secure private connection between an Azure virtual network and an on-premise facility, then Azure ExpressRoute is the recommended connectivity option. This utilizes a private circuit arranged by a Telco with an appropriate peering arrangement with Microsoft's cloud infrastructure. For

some production usage scenario's an ExpressRoute connection may be the only valid option and guidance should, in the first instance, be sought from your local Avid representative.

A virtual network in an Azure Resource Group can accommodate either a single VPN Gateway, single ExpressRoute Gateway or one of each. The VPN Gateway and ExpressRoute Gateways must each be deployed into their own subnets within the Virtual Network; the basic core deployment configuration places the Avid applications into a separate subnet within the Azure Virtual Network. Therefore, **advance planning** of the respective subnet addresses and ranges must be considered to ensure that any address ranges do not overlap or conflict with any existing on-premise or pre-configured cloud (subnet) network ranges.

A possible deployment pattern where some remote users (e.g. working from home) connect via a virtual VPN Gateway to access the production system using Point-to-Site connectivity over the public Internet, and other users working in a facility wanting secure private connectivity over Azure ExpressRoute is illustrated in **Figure 3 – Connect using VPN Gateway & ExpressRoute Gateway.**

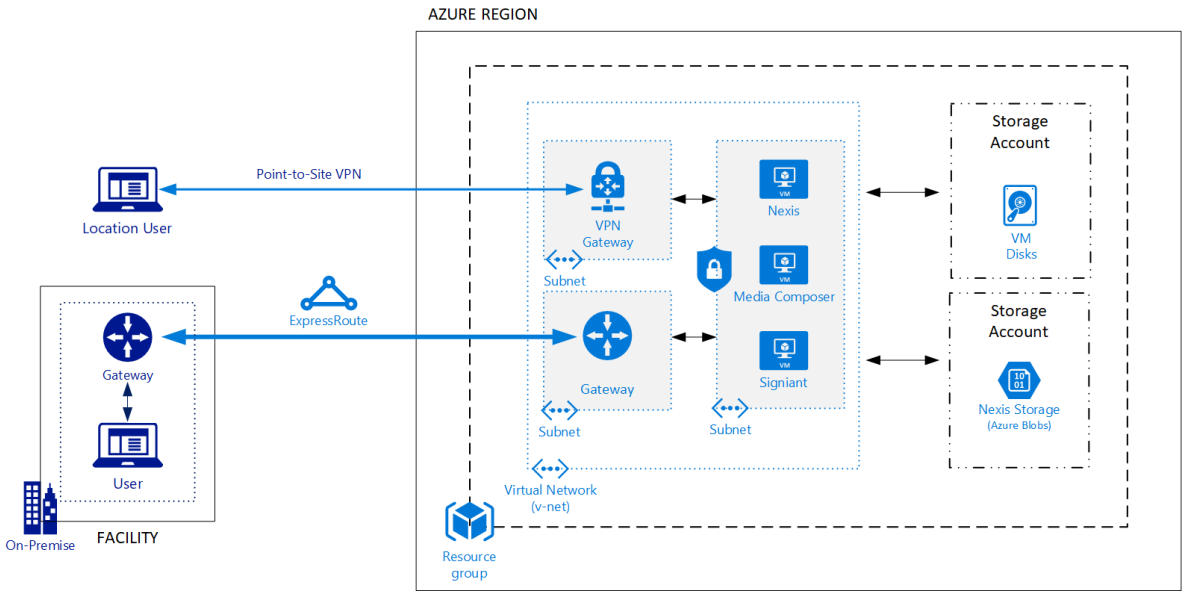


Figure 3 – Connect using VPN Gateway & Azure ExpressRoute Gateway

Alternative configurations and variations are also possible, for example using a VPN for Site-to-Site connectivity or enabling brokered VPN authentication using Azure Active Directory but these depend on local circumstances, consult with your IT department for additional guidance.

As it stands, after setup and configuration of the gateways, the VM's can still be accessed via their public IP addresses (or public Azure FQDN's), and in addition now also by their Azure private IP addresses (or private Azure FQDN's) in the case of users connecting over VPN or ExpressRoute. Where appropriate, public IP addresses can now be disabled or removed from VM's so that they are no longer accessible via public endpoints. This may also involve adjusting Network Security Group (NSG) configurations to remove rules allowing public (Internet) originating traffic to the subnet.

Once public IP addresses have been disabled on the production environment VM's and with suitably modified NSG changes then the production components (NEXIS, Media Composer, etc.) can only be accessed directly by users (IT administrators, ops admin and end users) connecting through either VPN or ExpressRoute gateways.

General, technical and how-to information for Azure VPN and ExpressRoute connections can be found at Microsoft VPN Gateway documentation and Azure ExpressRoute documentation.

Information on setup and configuration of Azure VPN Gateway can be found in Section 4.2 - Playbook: Set Up Azure VPN.

Information on setup and configuration of Azure ExpressRoute and Azure ExpressRoute Gateway can be found in Section 4.3 - Playbook: Setup Azure ExpressRoute.

3.2 Implement a Jumpbox or Bastion Strategy.

The Production VM's can be accessed by any user using a workstation or device that can connect via VPN or ExpressRoute Gateways and access the virtual network that the VM's are deployed in. User's can then utilize different tools and remote connection protocols such as **Secure Shell (SSH), Remote Desktop Protocol (RDP) or Teradici PCoIP** depending on that specific user's need and incoming traffic could be from a potentially wide pool of connecting devices. Ideally, we want to segregate user access such that administrative functions can only be performed by users connecting from known trusted workstations or devices and reduce the ability for other (non-administrative) users to be able to connect to production resources using SSH or RDP protocols.

One possible way to achieve this is to implement 'Jumpbox' devices/workstations or utilize the 'Azure Bastion' service, both of which facilitate privileged connections to resources for performing administrative functions using SSH or RDP. A possible implementation showing both options is illustrated in **Figure 4 – Jumpbox & Azure Bastion Example.**

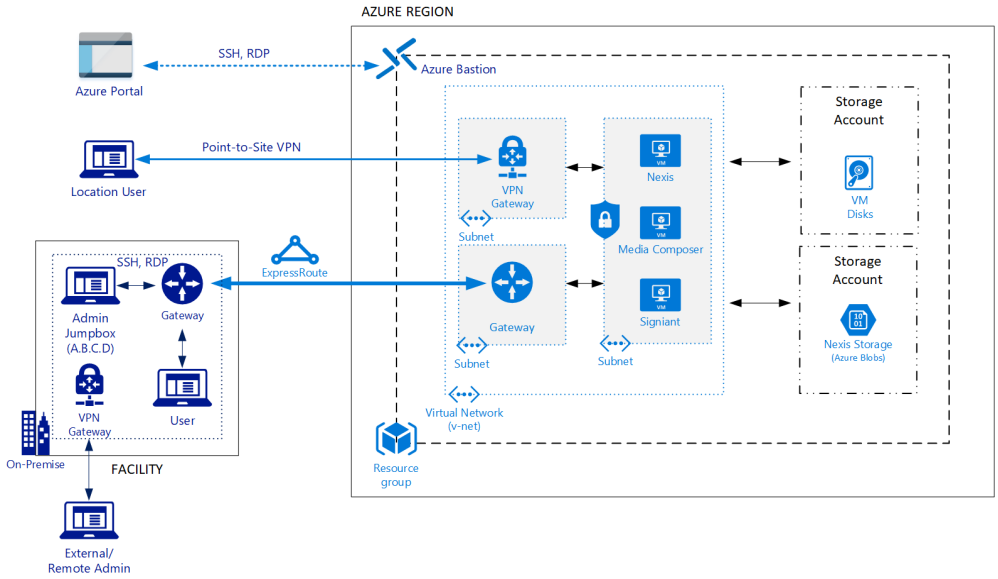


Figure 4 – Jumpbox & Azure Bastion Example

Designated workstation(s) (e.g. called 'Admin Jumpbox' in Figure 4) within the on-premise facility are used for performing system administration functions. Administrators can, using the designated workstation(s), now connect to any of the production resources via SSH, RDP or PCoIP protocol. The Network Security Group (NSG) of the production subnet is also adjusted so that SSH and RDP protocol traffic originating only from the designated Jumpbox workstation(s), or on-premise subnet that the Jumpbox workstations are located in, is allowed. This restriction means a user attempting to connect from a different workstation using SSH or RDP protocol will be denied access. Restricting the range or number of source devices that can be used to access and perform administrative functions helps to control access to the production environment and improve security.

Normal end users (e.g. Editorial, Assistants) can still access the Media Composer VM's but now only using Teradici PCoIP protocol and will not be able to access the production VM's using either SSH or RDP protocols. A further level of functional segregation can be implemented by restricting normal end users with logins only granting 'PowerUser' level privileges on Media Composer VM's, whereas Administrator logins can be granted full access administrator privileges.

The principle of a Jumpbox can be further extended such that any user wanting administrative access to the production environment must first authenticate and connect to the Jumpbox device or workstation and only then be able to initiate a connection session to the target production VM's. In this way organizational security policies can be further applied to restrict initial access to the Jumpbox device or workstation and create user logon audit trail.

An alternative deployment of a Jumpbox is illustrated in **Figure 5 (Using Jumpbox in Azure Virtual Network).**

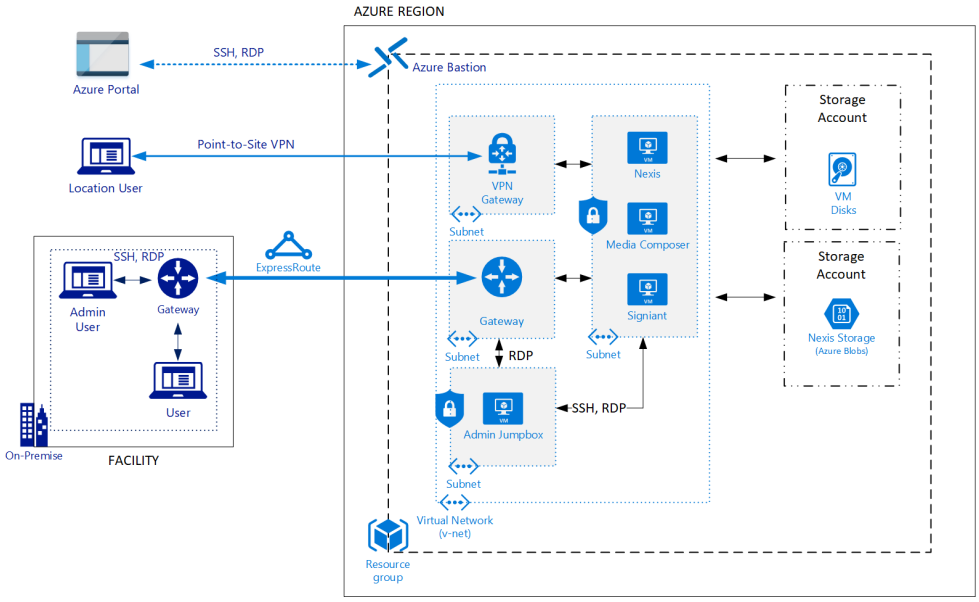


Figure 5 - Using Jumpbox in Azure Virtual Network

In this example, an administrator that is located in the on-premise facility now connects to the Jumpbox VM deployed in the Azure environment via RDP, and once connected is then able to connect using SSH or RDP to the various production VM's. The NSG for the production virtual network subnet is configured to only accept SSH and RDP traffic from the Jumpbox VM subnet. The Jumpbox subnet NSG is also configured to accept connections only from the on-premise environment over the ExpressRoute gateway. When using a Jumpbox, consideration should be given to where it will be situated and what further configuration changes may also be required in the environment.

Microsoft Azure has a service option that functions in a similar manner to a Jumpbox and is called a 'Bastion' service. The 'Bastion' service allows administrative users to be able to connect to production VM's using SSH or RDP over their current web browser session when they are logged into the Azure Portal. This option may be useful for small or isolated editorial production setups and avoids needing to setup and configure additional VPN gateways and VM's to act as the Jumpbox device. The 'Bastion' service is limited to only those users with credentials to access the Azure portal.

Irrespective of whether a 'Jumpbox' or 'bastion' is used for access, it is important to check that the respective publicly accessible VM endpoints (public IP addresses and interfaces) are blocked or disabled and Network Security Group policies are adjusted appropriately.

Information on configuring an environment for a 'Jumpbox' access device/workstation can be found in Section 4.4 - Playbook: Configure Environment for Jumpbox Device.

Information on setup and configuring an environment to use Azure 'Bastion' service can be found in Section 4.5 - Playbook: Setup and Configure Environment for Azure Bastion Service.

3.3 Securing Storage Accounts.

Azure Storage Accounts are a type of Microsoft Azure service and when created, by default, can be accessed publicly by authorized users. This default allows access using Microsoft tools such as Azure Storage Explorer without needing granted access to a specific Resource Group. Storage accounts are used for many file and data storage needs and can be associated with more than one Azure Resource Group. They are used for provisioning Virtual Machine disks (OS primary and secondary) as well as providing different storage types (e.g. Files, Blob, Table etc.) that can be used for general file and data storage.

Although only authenticated users and Azure resources can access Azure Storage Accounts, the fact that traffic by default traverses a public endpoint may be undesirable or conflicts with organizational security policies. This may be important where high-value media content should not un-necessarily be exposed and it may be desirable to adjust the environment so that only the dependent Azure resources can access the respective storage accounts (and underlying stores), in such a manner that no traffic traverses a public endpoint or that the storage accounts should not be accessible from any other virtual networks within the Azure environment.

Without further action, resources (e.g. VM's) accessing storage accounts will utilize the Azure public endpoint addresses of the storage account even if the resources are within the Azure environment and irrespective of the Azure Storage Account private address endpoints. What is required is to re-configure the environment such that any consuming resources will by default only utilize the Azure Storage Account private endpoint address.

Apart from Storage Accounts there are also many other Microsoft Azure Services that therefore are by default, accessed by their respective public endpoint addresses. A 'Service Endpoint' when configured on a Virtual Network Subnet can be used to force network traffic to instead use the Azure private endpoint address of the target Microsoft Azure Service and not the public endpoint address. A separate Service Endpoint when configured creates a one-to-one link between the virtual network subnet and the target Microsoft Azure service instance and therefore if access to multiple services need to be secured, (e.g. when using multiple Storage Accounts) from the same virtual network subnet then a Service Endpoint for each one will need to be created.

In typical Production environment deployments, there are at least two Microsoft Azure Storage Accounts, one for provisioning VM OS boot and data disks and one for provisioning the backing storage for NEXIS Cloud filesystem. Normally media files would be stored on the Nexis storage and without further action the underlying backing storage could be directly accessed by any user with suitable credentials from anywhere. A measure that can be taken to secure the underlying Azure Storage access is to re-configure the environment to use 'Service Endpoints'.

Re-configuration requires a two-step process:

- Define one or more 'Service Endpoints' on each Virtual Network subnet that will reserve a static private address from the subnet range for each one.

- Associate the configured 'Service Endpoint' with the respective Storage Account.

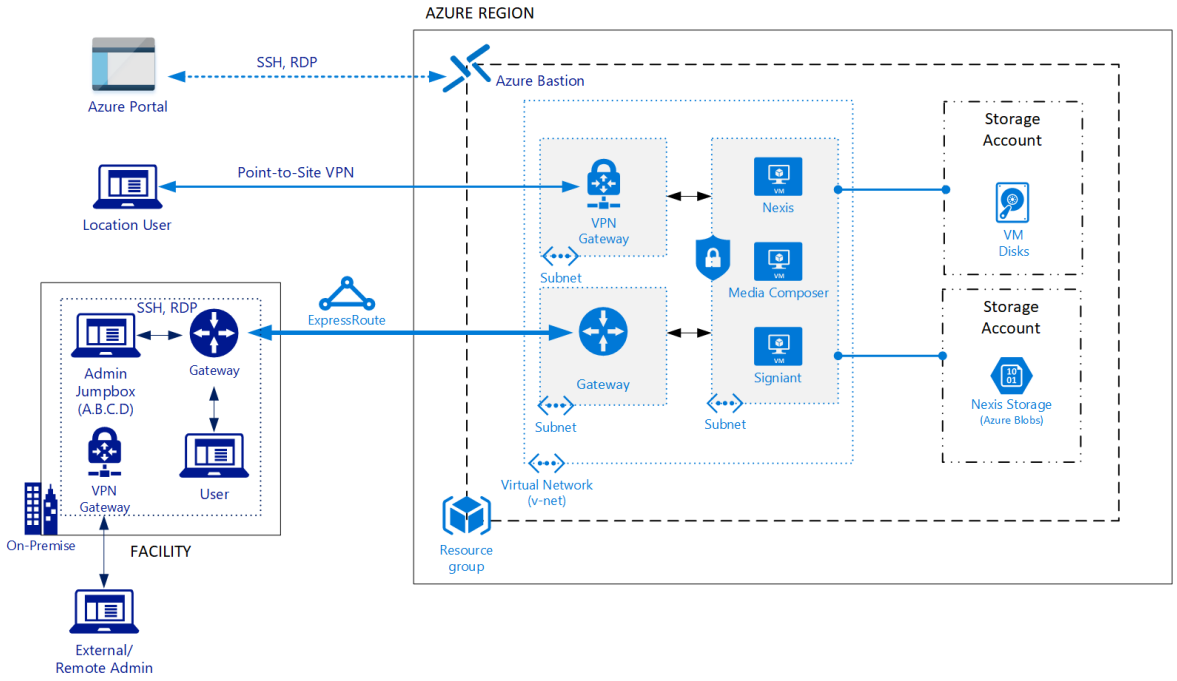


Figure 6 - Service Endpoints and Storage Accounts

Great care must be taken when performing these steps as network packet source and destination addresses will be re-written such that they will now only reference Azure private addresses and therefore the storage accounts will no longer be able to be accessed except from those specific Azure Network subnets using those private addresses.

As illustrated (**Figure 6 – Service Endpoints and Storage Accounts**) there are two Storage Accounts, one for VM Managed Disks and the other as the backing store for NEXIS Cloud storage (using Premium Blobs for online storage or Standard Blobs for nearline storage).

In the Virtual Network subnet containing the production VM's, there are now two configured Service Endpoints, one for each of the two Storage Accounts and these are shown associated with their respective Storage Accounts. After configuration only the resources within the Virtual Network subnet can access the respective storage accounts.

Users or administrators wanting file level access to the stores can only do so via virtual machines that are in the Virtual Network subnet with Service Endpoints associated with the respective storage accounts.

Information on setup and configuration of Service Endpoints for securing access to Storage Accounts can be found in Section 4.6 - Playbook: Secure Storage Accounts using Service Endpoints.

4.Playbooks for Setup and Configuration.

The following sections describe pathways ("Playbooks") for setup and configuration for the various topics discussed in previous sections. It is advisable to review the plays and any further associated resources and information before making adjustments to your own environments.

4.1 Playbook: Deploy Example Core Environment

Pre-requisites:

You will require an active **enterprise** or **pay-as-you-go Azure subscription** with proper rights and quotas to create Azure resources.

An open source deployment script can be used as the basis to help stage a typical core environment that consists of the following components:

- Avid NEXIS | Cloud
- Avid Media Composer | Ultimate
- Avid Media Composer VM Option
- File Transfer using Signiant Media Shuttle
- Teradici Graphics Agent (PCoIP)

Documentation and the necessary **deployment template** and scripts can be found here: https://github.com/Azure/VideoEditorialInTheCloud .

Note: The respective product or component licenses are not included and will need to be obtained from each vendor as appropriate and there may be additional costs involved. The open source scripts are provided 'as-is' and without warranty or support. Additional post-provisioning steps or configuration may also be required depending on individual situations. If in doubt contact your local Avid representative.

4.2 Playbook: Set Up Azure VPN.

Information on Azure VPN Gateway can be found at Microsoft Azure VPN Gateway documentation.

Pre-requisites:

- Determine the subnet and range that the Azure VPN Gateway will be deployed into. This must be a subnet range within the Virtual Network and must not overlap any other subnet ranges that may be present. Do not deploy into the same subnet that is used for the editorial production components or other existing subnets.
- Determine the Azure VPN Gateway SKU to be applied. The Gateway SKU determines the performance characteristics of the Azure VPN Gateway that will be provisioned. Note that the performance characteristics of the path from your location to the Azure VPN Gateway access point may be different to the throughput characteristics of the Azure VPN Gateway.
- For Point-to-Site style connections, determine the security protocols to be supported; OpenVPN, SSTP or IKEv2 (latter used typically for MacOS clients). You will also need to determine an appropriate authentication mechanism, using either native Azure certificate authentication or Azure Active Directory (if configured). See About Point-to-Site VPN for further information.

Plays:

- Create a route-based VPN gateway using the Azure portal
- Create a Site-to-Site connection in the Azure portal (for facility to Cloud connections)
- (or) Configure a Point-to-Site VPN connection to a VNet using native Azure certificate authentication (for end user to Cloud connections)
- Test connecting to production VM's (e.g. Avid NEXIS, Media Composer) using the Azure private IP address (not using DNS or computer name) of the VM (test SSH, RDP and PCoIP)
- Disable the public IP addresses of the appropriate production VM's
- Modify the production subnet's Network Security Group (NSG) to remove non-relevant public access policies that may be present (e.g. entries for public access RDP, SSH, PCoIP from the Internet)

4.3 Playbook: Set Up Azure Express Route.

Pre-requisites:

Determine the subnet and range that the Azure ExpressRoute Gateway will be deployed into. This must be a subnet range within the Virtual Network and which must not overlap any other subnet ranges that may be present. Do not deploy into the same subnet that is used for the editorial production components or other existing subnets.

Information on Azure ExpressRoute can be found at Microsoft Azure ExpressRoute documentation.

Plays:

- Planning ExpressRoute prerequisites & checklist
- Create and modify an ExpressRoute circuit
- Connect a virtual network to an ExpressRoute circuit
- Test connecting to production VM's (e.g. Avid NEXIS, Media Composer) using the Azure private IP address (not DNS or computer name) of the VM (test SSH, RDP and PCoIP)
- Disable the public IP addresses of the appropriate production VM's
- Modify the production subnet's Network Security Group (NSG) to remove any non-relevant public access policies (e.g. entries for public access RDP, SSH, PCoIP from the Internet)

4.4 Playbook: Configure Environment for Jumpbox Device.

Pre-requisites:

Decide and plan accordingly based on where the 'Jumpbox' will be deployed (on-premise or cloud).

Plays – On-Premise:

- Acquire and setup the Jumpbox system. This may be on a physical host or a virtualized appliance located on-premise.
- Configure the Jumpbox to allow administrators to logon or connect to it.

- Modify the cloud production subnet's Network Security Group (NSG) to only allow RDP/SSH connections from the Jumpbox system.
- Modify the cloud production subnet's Network Security Group (NSG) to remove any rules allowing RDP/SSH connections from other sources.
- Test that PCoIP connections are still possible from allowed locations.
- Test that RDP/SSH connections are not possible from any locations other than the Jumpbox system.
- Check and remove any non-relevant public access policies (e.g. entries for public access RDP, SSH, PCoIP from the Internet) from any NSG if not done already and re-test.

Plays – Cloud:

- Deploy a Windows based VM in the virtual network, typically into a separate subnet with its own Network Security Group (NSG).
- Configure the production subnet's NSG to deny RDP/SSH from any source other than the Jumpbox subnet.
- Configure the production subnet's NSG to allow PCoIP from permitted sources.
- Configure the Jumpbox subnet's NSG to allow RDP connections from permitted sources.
- Configure the Jumpbox VM to allow administrators to logon or connect to it.
- Test that PCoIP connections are still possible from allowed locations.
- Test that RDP/SSH connections are refused when trying to connect directly to production VM's (e.g. Media Composer, NEXIS) from any sources other than from the Jumpbox VM.
- Test that RDP connections can be made by administrators to the Jumpbox VM and subsequently RDP/SSH connections from the Jumpbox VM to the production VM's (e.g. Media Composer, NEXIS).
- Check and remove any non-relevant public access policies (e.g. entries for public access RDP, SSH, PCoIP from the Internet) from any NSG if not done already and re-test.

Other Considerations: The exact setup and configuration will be highly dependent on the implementation of the choice of Jumpbox system location and the steps as illustrated may need to vary as a consequence. You should work with your local IT to ensure that the appropriate setup and configuration is aligned with local security guidelines.

4.5 Playbook: Configure Environment for Azure Bastion Service.

Information on Azure Bastion can be found at Microsoft Azure Bastion documentation

Pre-requisites:

For further information about the Azure Bastion service see : What is Azure Bastion?

Plays:

- Create an Azure Bastion host
- Connect to a Windows virtual machine using Azure Bastion
- Connect using SSH to a Linux virtual machine using Azure Bastion
- Disable the public IP addresses of the appropriate production VM's
- Modify the production subnet's Network Security Group (NSG) to remove any non-relevant public access policies (e.g. entries for public access RDP, SSH, PCoIP from the Internet)

4.6 Playbook: Secure Storage Accounts Using Service Endpoints.

Prerequisites:

Information about Service Endpoints can be found at: Virtual Network service endpoints.

Additional information on using Service Endpoints with Azure Storage can be found at: Use Private Endpoints for Azure Storage.

- Assumes that you can directly connect and browse the Storage Account from outside of the desired secure locations (e.g. using Azure Storage Explorer)

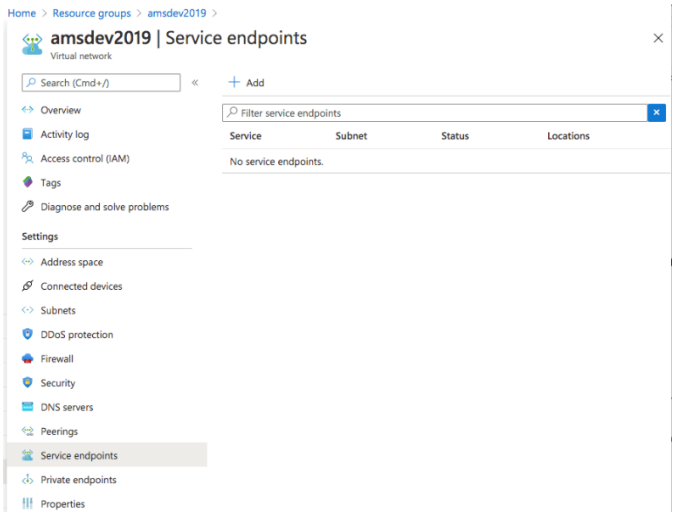
Plays:

- Configure Service Endpoint on Virtual Network Subnet for VM Disk Storage Account
- Configure Service Endpoint on Virtual Network Subnet for Media Storage Account
- Test that from the production VM's the Storage Account can still be accessed

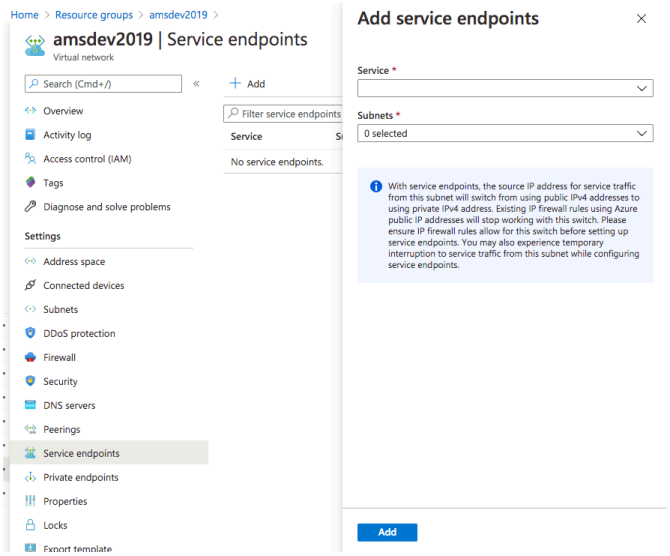
- Re-test and confirm that you are no longer able to connect and browse the Storage Account from the locations that you tested in 'prerequisites' above (e.g. using Azure Storage Explorer)

The following describe the steps to setup and apply Azure Service Endpoints with Storage Accounts using Azure Portal:

1. Navigate to the Resource Group where you want to securely access the Storage Account and select the Virtual Network resource...

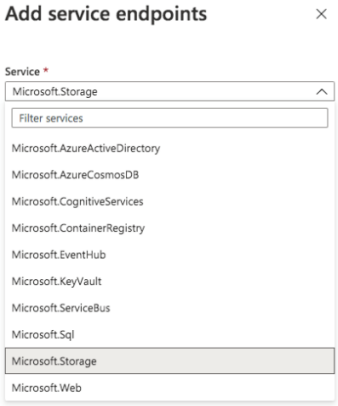


Then select 'Service endpoints' and click on '+Add'...



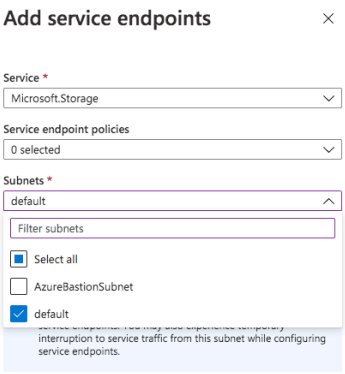
The 'Add service endpoints' side panel appears.

2. From the 'Service' dropdown on the 'Add service endpoints' side panel select the service type for which you want to create a Service Endpoint, e.g. Azure Storage Accounts



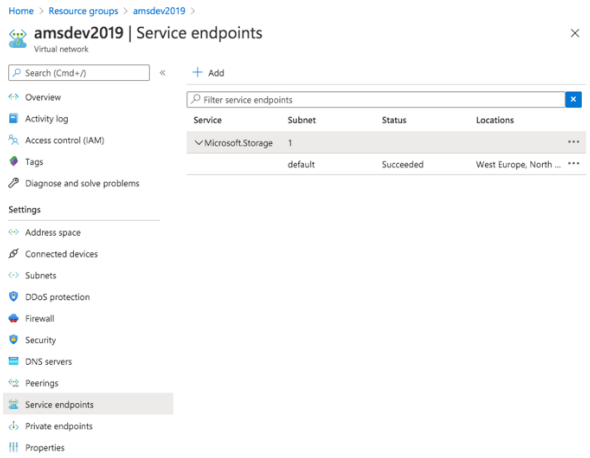
choose 'Microsoft.Storage'...

3. From the 'Subnets' dropdown on the 'Add service endpoints' side panel select the subnet for which you want to create a Service Endpoint. This would typically be the subnet containing resources that need secure access to the Storage Account...

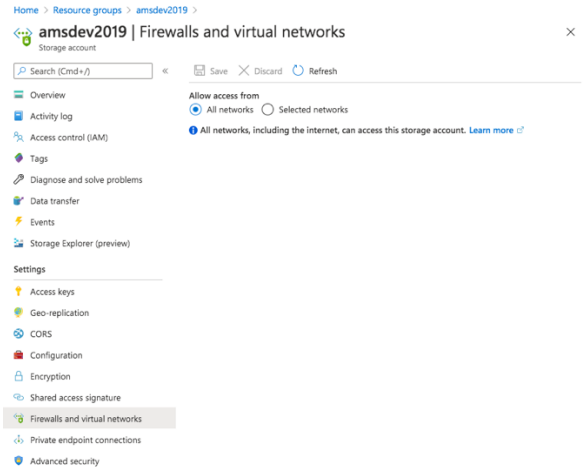


Then click on 'Add' to create the Service Endpoint.

4. The Service Endpoint will be provisioned and when completed will appear in the Virtual Network under 'Service endpoints'...

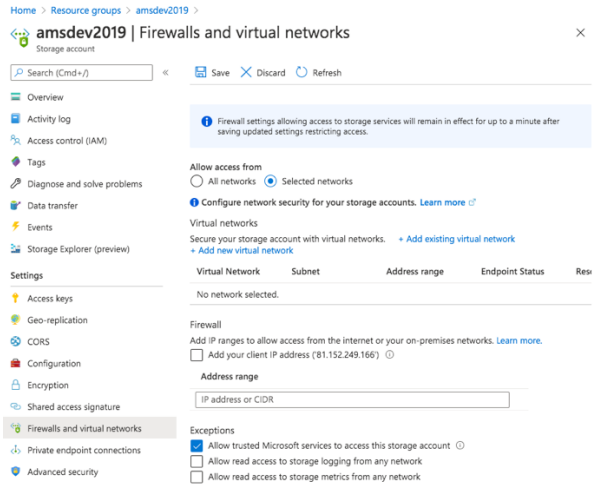


5. Then navigate and select the Storage Account you want to associate the Service Endpoint with and choose the 'Firewalls and virtual networks' option for the Storage Account...



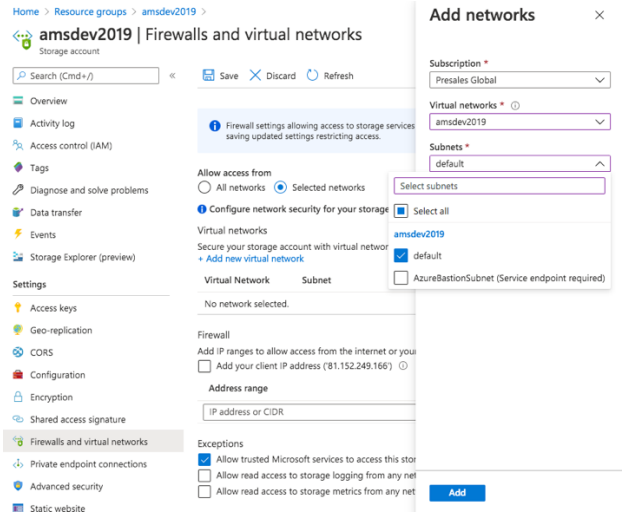
From the 'Allow access from' sub-section, click on 'Selected networks'...

6. Options will then appear to configure network security for your storage account...



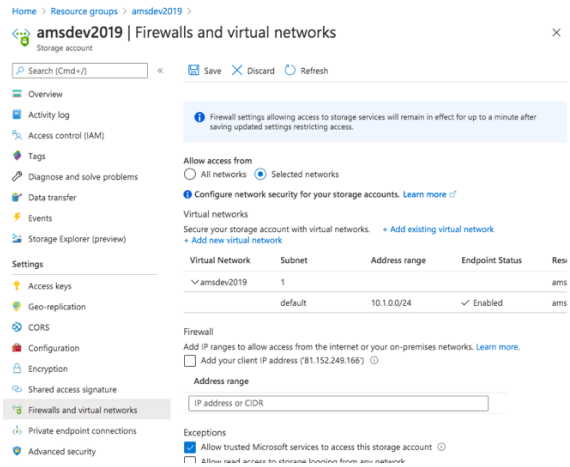
Then from the 'Virtual networks' sub-section, click on '+Add existing virtual network'...

7. The 'Add networks' side panel will appear...



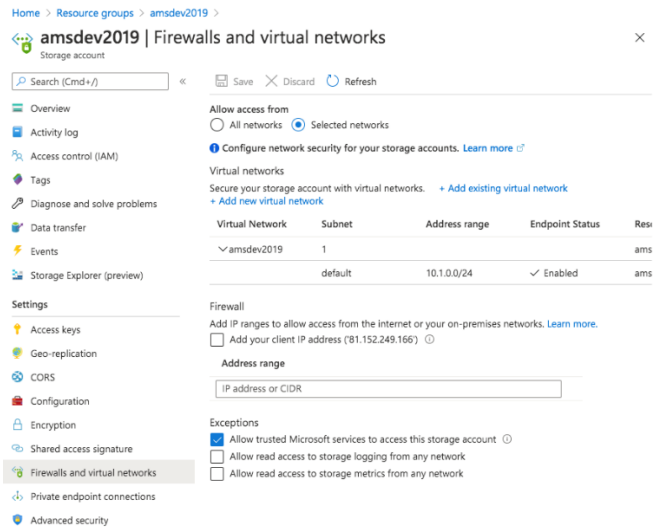
Ensure that you choose the correct Subscription, Virtual Network and Subnet that you previously created the Service Endpoint for. Note that if you choose incorrectly, the subnet choice(s) may be annotated with 'Service endpoint required' if no Service Endpoints exist on that subnet. When done click on 'Add'...

8. The Service Endpoint will be added to the Storage Account...



When ready, apply the changes by clicking on the 'Save' icon at the top of the Storage Account, Firewalls and virtual networks panel...

9. The changes will then be applied to the Storage Account...



From now on only those deployed resources in the Subnet on which the Service Endpoint was created will be able to access the Storage Account.

Repeat the above steps to create and associate Service Endpoints for any other subnets containing resources that need to access the same Storage Account.

Other Considerations: Note that the Storage Account (storage) will only be able to be accessed from those subnets on which you have created Service Endpoints, therefore you may need to repeat this 'Playbook' if the same Storage Account needs to be accessed from resources in different subnets (or subnets in different Resource Groups).

To be able to access the Storage Account storage you now need to connect to a suitable VM within the subnet that is associated with the Storage Account (e.g. a subnet containing a Jumpbox workstation or Media Composer/NEXIS VM's).

If additional access is required from specified IP address ranges (e.g. on-premise access via ExpressRoute), then you should also consider adding Firewall IP address ranges on the Storage Account (Firewalls and virtual networks pane) in addition to applying Service Endpoints. Further details can be found at: Grant access from an internet IP range.