|  |  |
| --- | --- |
| **Azure Linux VM (Ubuntu 18.04) LVM on Encrypted Disks** | |
| **Azure CLI** | **Azure VM** |
| az login  # Manage Key Vault using the Azure CLI  # <https://docs.microsoft.com/en-us/azure/key-vault/key-vault-manage-with-cli2>  id=$(date +"%M%S")  #Deploy Ubuntu 18.04 VM and a key vault in the same resource group  vmName=u$id  rgName=da$id  #sku=win2016datacenter  sku=UbuntuLTS  location=southcentralus  # az vm list-sizes -l $location | more  vmSize=Standard\_B2ms  user=alice  pwd=thisP@ssw0rd  kvName=kv$id  keyName=key$id  volType=DATA  az group create --name $rgName --location $location  #az group delete --name $rgName  az vm create \  -g $rgName \  --name $vmName \  --image $sku \  --size $vmSize \  --admin-username $user \  --admin-password $pwd  #az vm open-port --port 80 --resource-group $rgName --name $vmName  diskSize=5  diskName=d5 # d51 d52  az vm disk attach \  --vm-name $vmName \  -g $rgName \  -n $diskName \  --size-gb $diskSize \  --new  az keyvault create \  -g $rgName \  -n $kvName \  --location $location \  --enabled-for-disk-encryption \  --output table  az keyvault key create \  --vault-name $kvName \  --name $keyName \  --ops decrypt encrypt sign unwrapKey verify wrapKey \  --output table |  |
|  | ssh user@vmIP  Lsblk -f  ls -l /dev/disk/azure/scsi1/lun\*  echo "y" | mkfs.ext4 /dev/disk/azure/scsi1/lun0  echo "y" | mkfs.ext4 /dev/disk/azure/scsi1/lun1  UUID0="$(blkid -s UUID -o value /dev/disk/azure/scsi1/lun0)"  UUID1="$(blkid -s UUID -o value /dev/disk/azure/scsi1/lun1)"  mkdir /data0  mkdir /data1  echo "UUID=$UUID0 /data0 ext4 defaults,nofail 0 0" >>/etc/fstab  echo "UUID=$UUID1 /data1 ext4 defaults,nofail 0 0" >>/etc/fstab  more /etc/fstab  mount -a  df -h /data\* |
| # Enable encryption using KEK  # Get the resource ID of the Key Vault  vaultResourceId=$(az keyvault show -g $rgName --name $kvName --query id -o tsv)  az vm encryption enable \  -n $vmName \  -g $rgName \  --disk-encryption-keyvault $vaultResourceId \  --key-encryption-keyvault $vaultResourceId \  --key-encryption-key $keyName \  --volume-type $volType  az vm encryption show --name $vmName --resource-group $rgName --query '[status,substatus]'  az vm encryption show -n $vmName -g $rgName |  |
|  |  |
|  | ssh ubuntuAdmin@vmIP  sudo su –  lsblk -f  df -h /data\*  umount /data0  umount /data1  fdisk -l | grep mapper  more /etc/crypttab  # Physical volumes  echo "y" | pvcreate /dev/mapper/???...???  echo "y" | pvcreate /dev/mapper/???...???  volGroup=’thisVG’  vgcreate $volGroup /dev/mapper/???...??? /dev/mapper/???...???  vgdisplay -v $volGroup    lvcreate -L 4G -n logicalVol0 $volGroup  lvcreate -L 4G -n logicalVol1 $volGroup  echo "yes" | mkfs.ext4 /dev/$volGroup/logicalVol0  echo "yes" | mkfs.ext4 /dev/$volGroup/logicalVol1  pvs  vgs  lvs  echo "/dev/mapper/$volGroup-logicalVol0/data0 ext4 defaults,nofail 0 0" >>/etc/fstab  echo "/dev/mapper/$volGroup-logicalVol0/data1 ext4 defaults,nofail 0 0" >>/etc/fstab  mount -a  df -h /data\*  reboot  df -h /data\* |