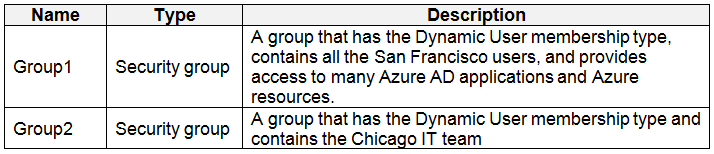
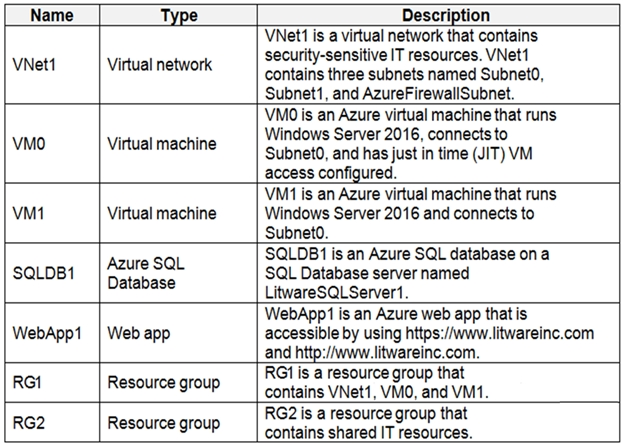
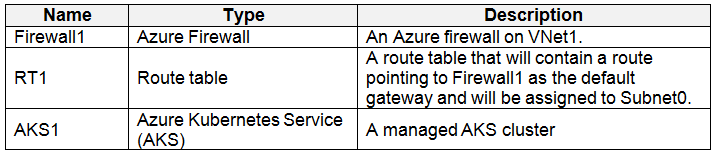
Overview -  
Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.  
  
Existing Environment -  
Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.  
Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the  
Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.  
The tenant contains the groups shown in the following table.  
  
The Azure subscription contains the objects shown in the following table.  
  
Identity and Access Requirements  
Azure Security Center is set to the Standard tier.  
  
Requirements -  
  
Planned Changes -  
Litware plans to deploy the Azure resources shown in the following table.  
  
Litware identifies the following identity and access requirements:  
All San Francisco users and their devices must be members of Group1.  
The members of Group2 must be assigned the Contributor role to RG2 by using a permanent eligible assignment.  
Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the usersג€™ behalf.  
Platform Protection Requirements  
Litware identifies the following platform protection requirements:  
Microsoft Antimalware must be installed on the virtual machines in RG1.  
The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.  
Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.  
Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.  
A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in RG1. Role1 must be available only for RG1.  
Security Operations Requirements  
Litware must be able to customize the operating system security configurations in Azure Security Center.  
Data and Application Requirements  
Litware identifies the following data and applications requirements:  
The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.  
WebApp1 must enforce mutual authentication.  
  
General Requirements -  
Litware identifies the following general requirements:  
Whenever possible, administrative effort must be minimized.  
Whenever possible, use of automation must be maximized.