

Higher Quality, Better Service!

KillTest

50% OFF
Coupon: off50

MICROSOFT CERTIFIED: IDENTITY AND ACCESS ADMINISTRATOR ASSOCIATE Exam

SC-300 Questions V16.02

**Microsoft Certified: Identity and
Access Administrator Associate
Topics - Microsoft Identity and
Access Administrator**

1. Topic 1, Litware, Inc

Overview

Litware, Inc. is a pharmaceutical company that has a subsidiary named fabrikam, inc. Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Identity Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled. Litware.com contains a user named User1 who oversees all application development. Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

On-premises Environment

The on-premises network contains the servers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.