Filename: microsoft-ms101-6-1-3-azure-atp-architecture-and-components-prerequisites
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Implement Threat Management
EpisodeName: Azure ATP Architecture and Components - Prerequisites
Description: Adam and Wes discuss the prerequisites of the Azure ATP solution.

Azure ATP Architecture and Components - Prerequisites

Implement Microsoft 365 Security and Threat Management (30-35%)

Implement Threat Management
• Plan a Threat Management Solution
• Design Azure Advanced Threat Protection (ATP) Policies
• Design Microsoft 365 ATP Policies
• Configure Azure ATP Policies
• Configure Microsoft 365 ATP Policies
• Monitor Advanced Threat Analytics (ATA) incidents

==========

Azure ATP Architecture and Components - Prerequisites

Azure ATP Advanced Audit Policy check:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-advanced-audit-policy

Azure Advanced Threat Protection Sizing Tool:
https://gallery.technet.microsoft.com/Azure-Advanced-Threat-a11343c4

Plan capacity for Azure ATP:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning

Azure ATP Prerequisites:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-prerequisites

Before you start

```
1. To create your Azure ATP instance, you will need an AAD tenant with at
```

least one global/security administrator. Each Azure ATP instance supports a
multiple Active Directory forest boundary and Forest Functional Level (FFL)
of Windows 2003 and above.

```
2. A license for Enterprise Mobility + Security 5 (EMS E5), or use the Cloud
```

Solution Partner (CSP) licensing model, or Standalone Azure ATP licenses are
also available.

```
3. Verify the domain controller(s) you intend to install Azure ATP sensors on
```

have internet connectivity to the Azure ATP Cloud Service. The Azure ATP sensor
supports the use of a proxy.

```
4. An on-premises AD user account and password with read access to all objects
```

in the monitored domains.

NOTE: If you have set custom ACLs on various Organizational Units (OU) in your
domain, make sure that the selected user has read permissions to those OUs.

```
5. If you run Wireshark on Azure ATP standalone sensor, restart the Azure
```

Advanced Threat Protection sensor service after you have stopped the Wireshark
capture. If you do not restart the sensor service, the sensor stops capturing
traffic.

```
6. If you attempt to install the Azure ATP sensor on a machine configured with
```

a NIC Teaming adapter, you will receive an installation error.

If you want to install the ATP sensor on a machine configured with NIC teaming,
follow these instructions:

```
If you have not yet installed the sensor:

    a. Download Npcap from https://nmap.org/npcap/
    b. Uninstall WinPcap, if it was installed
    c. Install Npcap with the following options: loopback_support=no & winpcap_mode=yes
    d. Install the sensor package

If you already installed the sensor:

    a. Download Npcap from https://nmap.org/npcap/
    b. Uninstall the sensor
    c. Uninstall WinPcap
    d. Install Npcap with the following options: loopback_support=no & winpcap_mode=yes
    e. Reinstall the sensor package


7. Deleted Objects container Recommendation: User should have read-only
```

permissions on the Deleted Objects container. Read-only permissions on this
container allows Azure ATP to detect user deletions from your Active Directory.

```
8. Optional Honeytoken: A user account of a user who has no network activities.
```

This account is configured as an Azure ATP Honeytoken user.