Filename: microsoft-ms101-6-1-2-azure-atp-architecture-and-components-overview
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Implement Threat Management
EpisodeName: Azure ATP Architecture and Components - Overview
Description: Adam and Wes discuss the architecture and components of the Azure ATP solution.

Azure ATP Architecture and Components - Overview

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 - Overview

Azure ATP consists of the following components:

```
• Azure ATP portal - allows creation of your Azure ATP instance, displays the
```

data received from Azure ATP sensors, and enables you to monitor, manage, and investigate threats in your network environment.

```
    NOTE: If no sensor is installed on your Azure ATP instance within 60 days,
the instance may be deleted and you will need to recreate it.


    Logging into the Azure ATP portal:

    You can enter the Azure ATP portal either by logging in to the portal
    https://portal.atp.azure.com and selecting your instance, or browsing to
    the instance URL: https://instancename.atp.azure.com


• Azure ATP sensors - installed directly on your domain controllers. The sensor
```

directly monitors domain controller traffic, without the need for a dedicated server, or configuration of port mirroring.

```
• Azure ATP cloud service - connected to Microsoft's intelligent security graph.
```

Azure ATP Sensor features

The Azure ATP sensor supports Event Tracing for Windows (ETW) which provides the log information for multiple detections. ETW-based detections include Suspected DCShadow attacks attempted using domain controller replication requests and domain controller promotion.

Domain synchronizer process

Responsible for synchronizing all entities from a specific Active Directory domain proactively (similar to the mechanism used by the domain controllers themselves for replication). One sensor is automatically chosen at random from all of your eligible sensors to serve as the domain synchronizer.

NOTE: If the domain synchronizer is offline for more than 30 minutes, another sensor is automatically chosen instead.

Resource limitations

The Azure ATP sensor includes a monitoring component that evaluates the available compute and memory capacity on the domain controller on which it's running.

The monitoring process runs every 10 seconds and dynamically updates the CPU and memory utilization quota on the Azure ATP sensor process.

The monitoring process makes sure the domain controller always has at least 15% of free compute and memory resources available.

If the monitoring process causes the Azure ATP sensor to run out of resources, only partial traffic is monitored and the monitoring alert "Dropped port mirrored network traffic" appears in the Azure ATP portal Health page.

Windows Events

To enhance Azure ATP detection coverage related to NTLM authentications, modifications to sensitive groups and creation of suspicious services, Azure ATP needs to analyze the logs of the following Windows events:
• 4776
• 4732
• 4733
• 4728
• 4729
• 4756

• 4757
• 7045
• 8004

These events are read automatically by Azure ATP sensors with correct advanced audit policy settings.

NOTE: To make sure Windows Event 8004 is audited as needed by the service, review your NTLM audit settings.

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.