Integrating Azure

https://campus.barracuda.com/doc/96767412/

Barracuda XDR retrieves Audit Logs, Sign In Logs, and Activity Logs from Microsoft Azure. These items are read from the Azure Event Hub.

BarracudaCampus

Videolink:

https://campus.barracuda.com/

This video has no sound.

Requirements

- An Azure Premium **P1 or P2** license is required.

Integrating Microsoft Azure requires you follow these procedures, below:

- **Part 1: Setting Up Azure Event Hub**
  - To create Event Hub Namespaces
- **Part 2: Configuring Storage Accounts**
  - To initialize Storage Accounts
  - To set up Event Hub Entities
  - To set up an Event Hub Shared Access Policy
- **Part 3: Updating Diagnostic Settings**

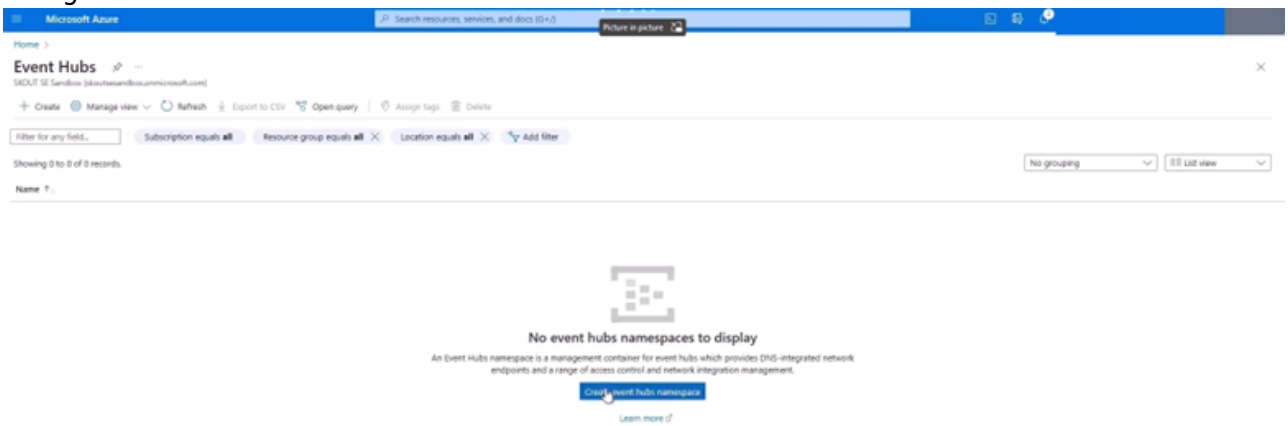
- To update diagnostic settings for the sign in log
- To update diagnostic settings for for the audit log and activity log
- To set up Microsoft Defender for Cloud

- **Part 4: Barracuda XDR Dashboard Setup for Azure**

Part 1: Setting Up Azure Event Hub

To create Event Hub Namespaces

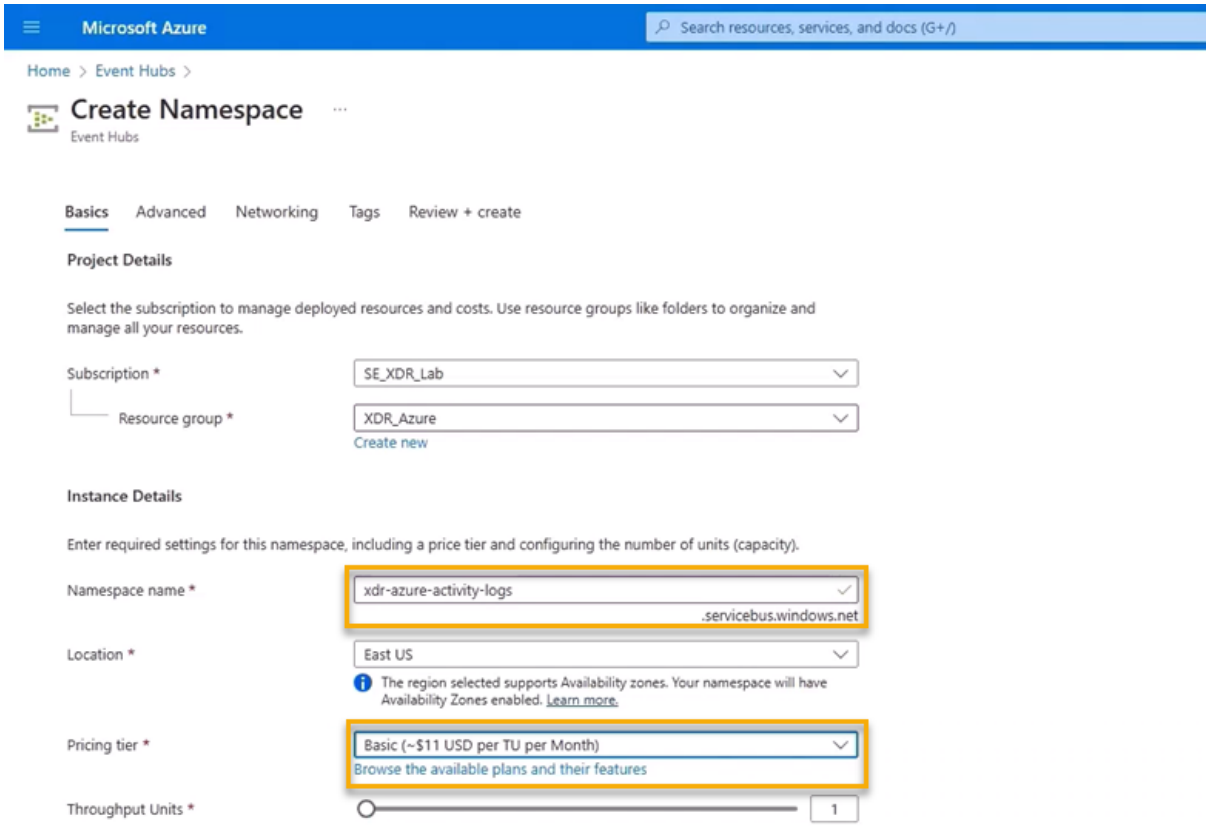
1. Navigate to the Azure Event Hub.



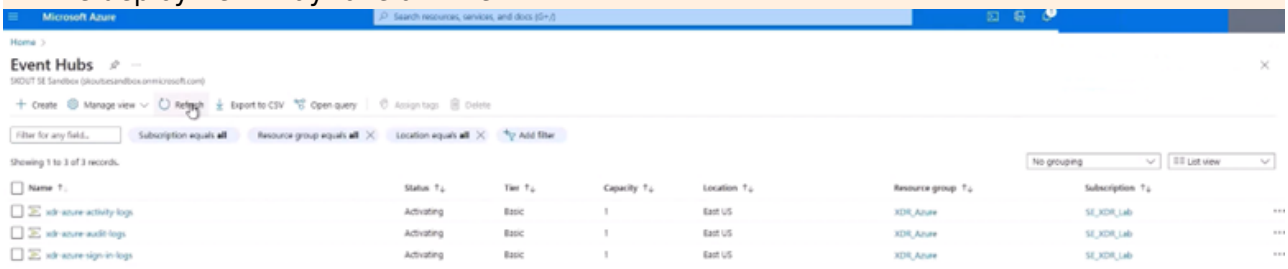
2. Create three event hub namespaces dedicated to each of the following:
    1. Audit Logs
    2. Sign In Logs
    3. Activity Logs

    The **Event Hub Namespace Name** must:
    - Contain at least eight characters.
    - Not contain special characters.

    In **Pricing Tier**, select **Basic**.
    In **Networking**, select **Public Access**.
    We recommend the following naming convention:
    - xdr-azure-activity-logs
    - xdr-azure-audit-logs
    - xdr-azure-sign-in-logs



3. Click **Review and Create**.
   The deployment may take a while.



Part 2: Configuring Storage Accounts

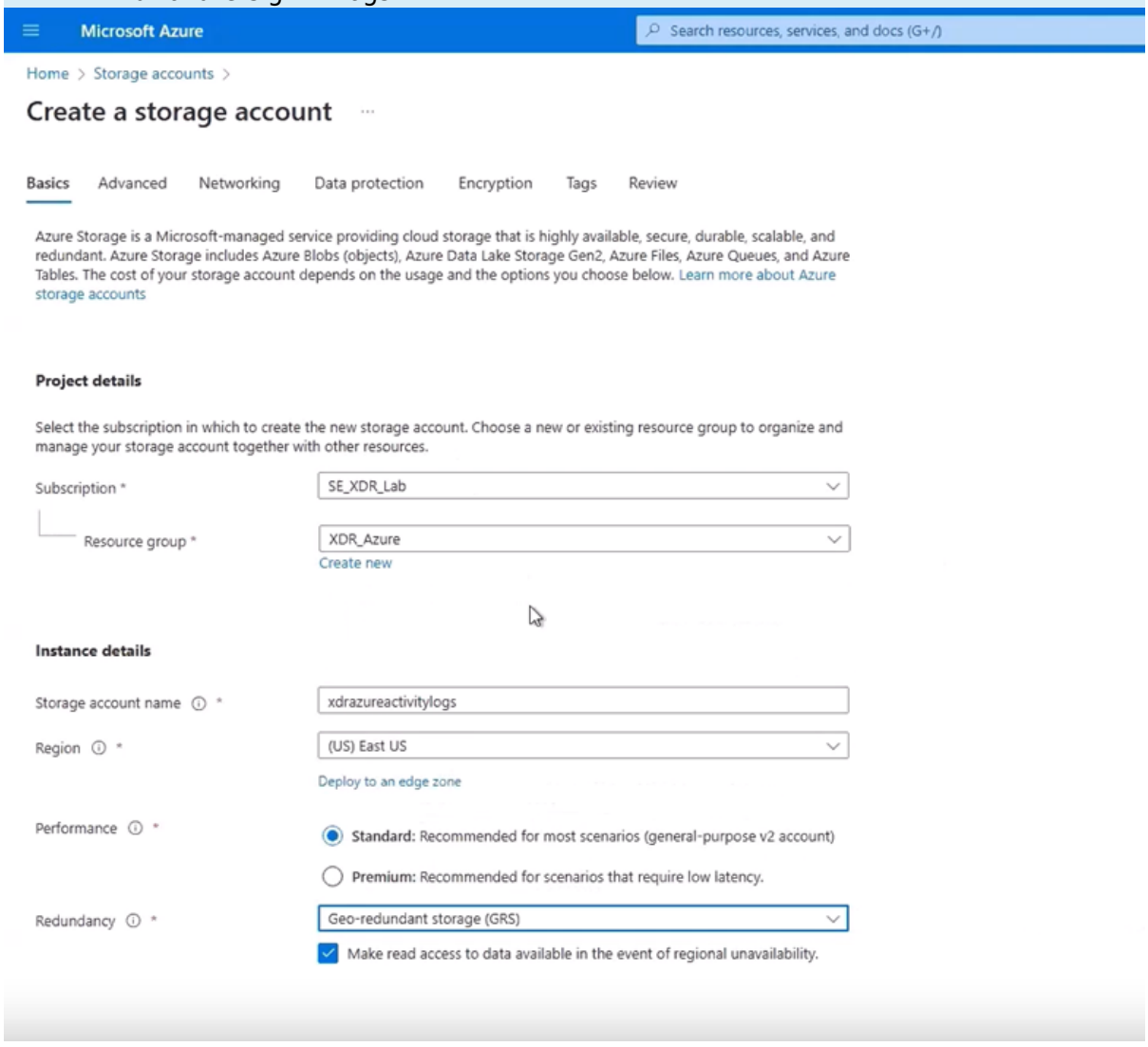
Configuring storage accounts requires the following procedures, below:

- To initialize Storage Accounts
- To set up Event Hub Entities
- To set up an Event Hub Shared Access Policy

To initialize storage accounts

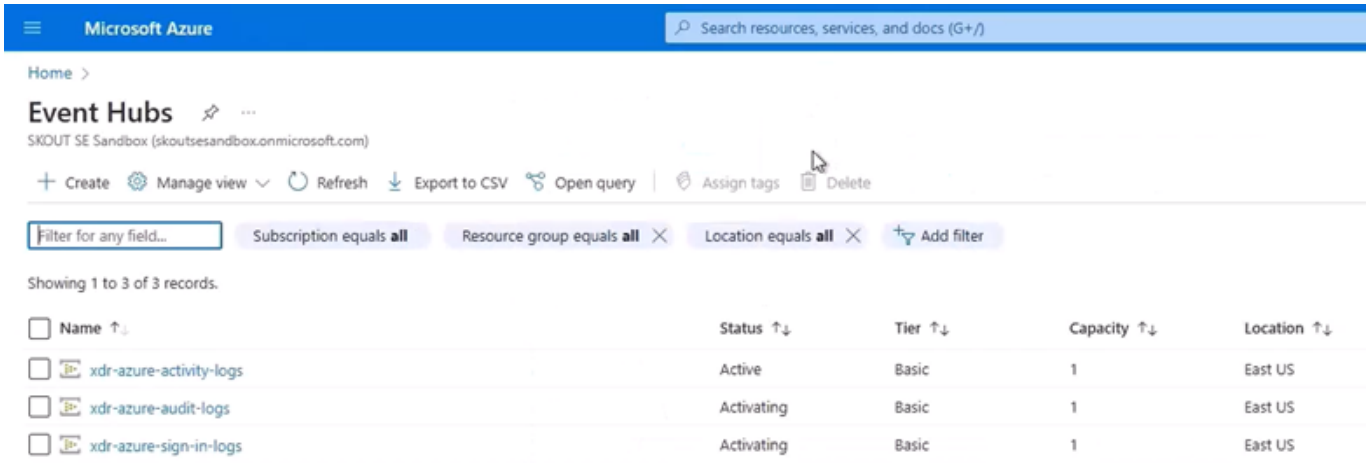
1. Navigate to **Storage Accounts**.
    - Audit Logs
    - Sign In Logs
    - Activity Logs

    We recommend the following naming convention:
    - xdr-azure-activity-logs
    - xdr-azure-audit-logs
    - xdr-azure-sign-in-logs



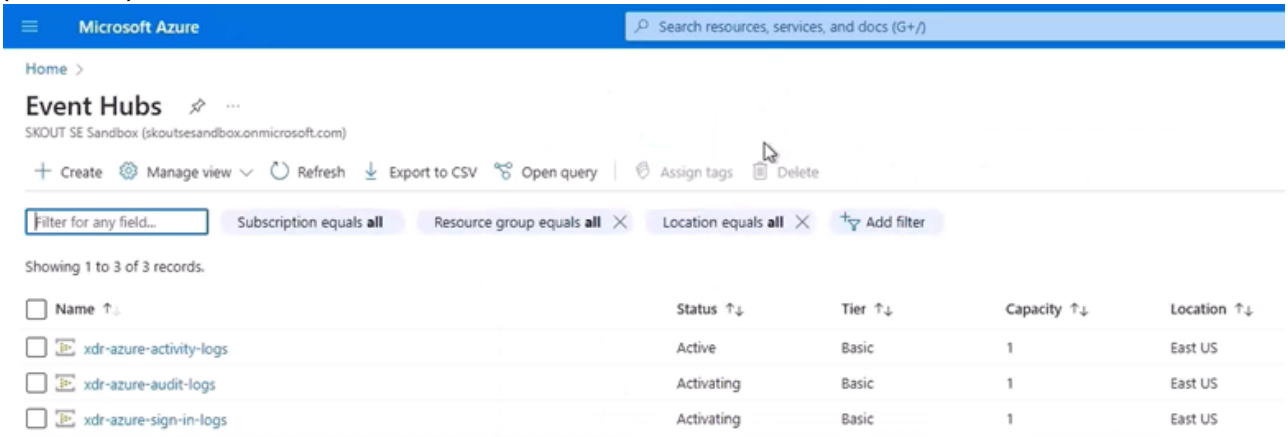
2. Click **Review and Create**.

The deployment may take a while.



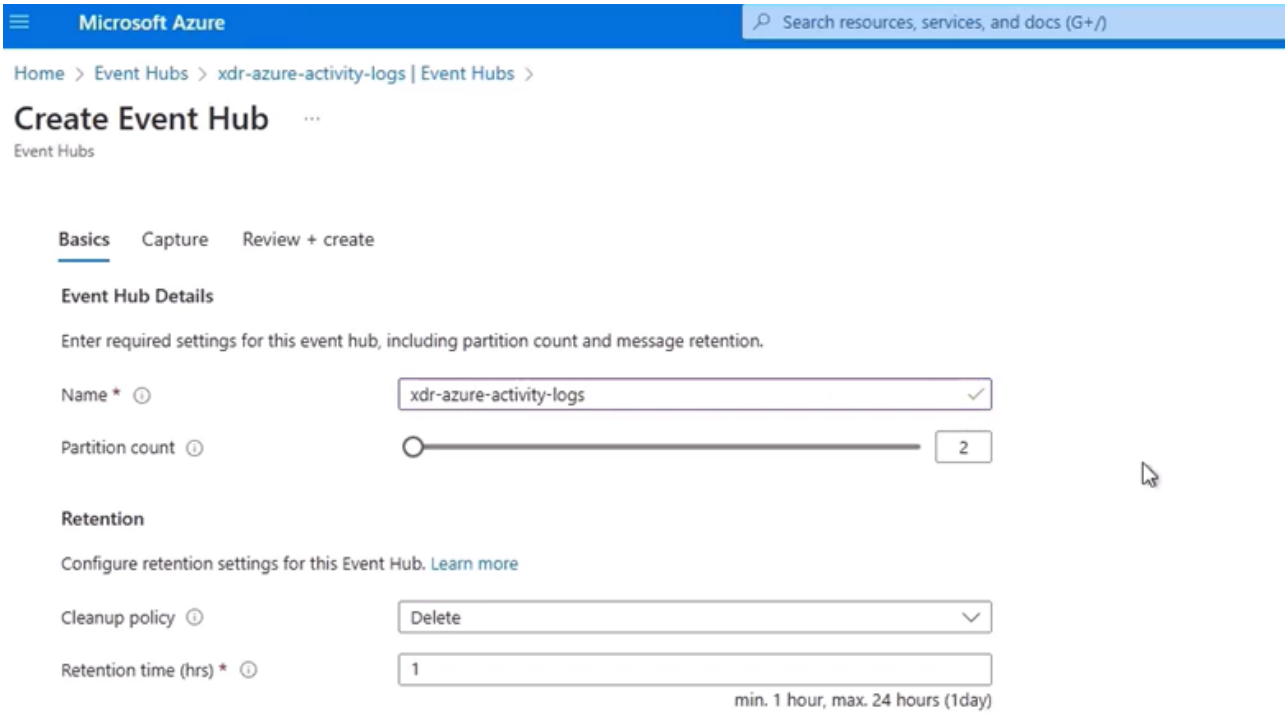
To set up Event Hub Entities

1. In Microsoft Azure, navigate to **Event Hubs**.
2. In **Event Hubs**, select the check box of an **Event Hub Namespace** that you created in the previous procedure.

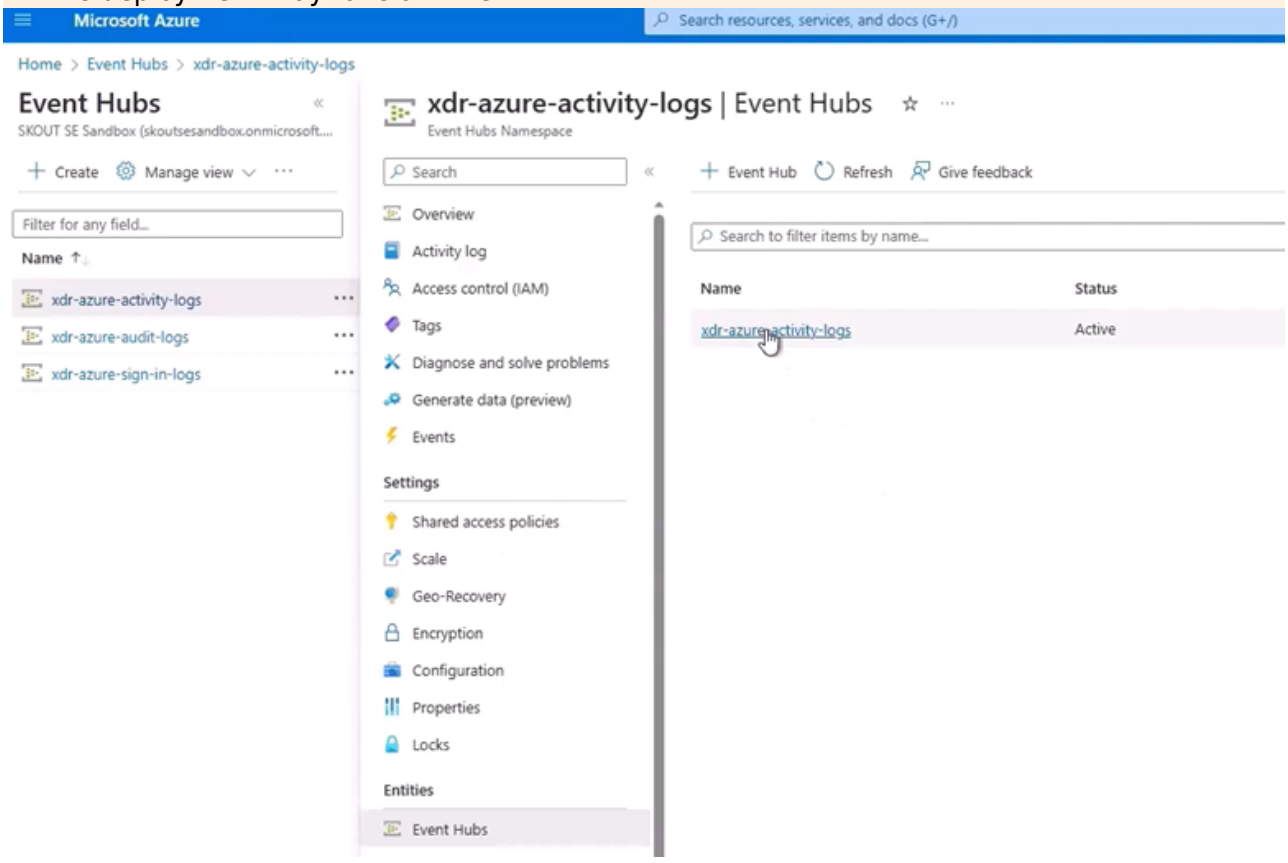


3. Click **Create Event Hub**.

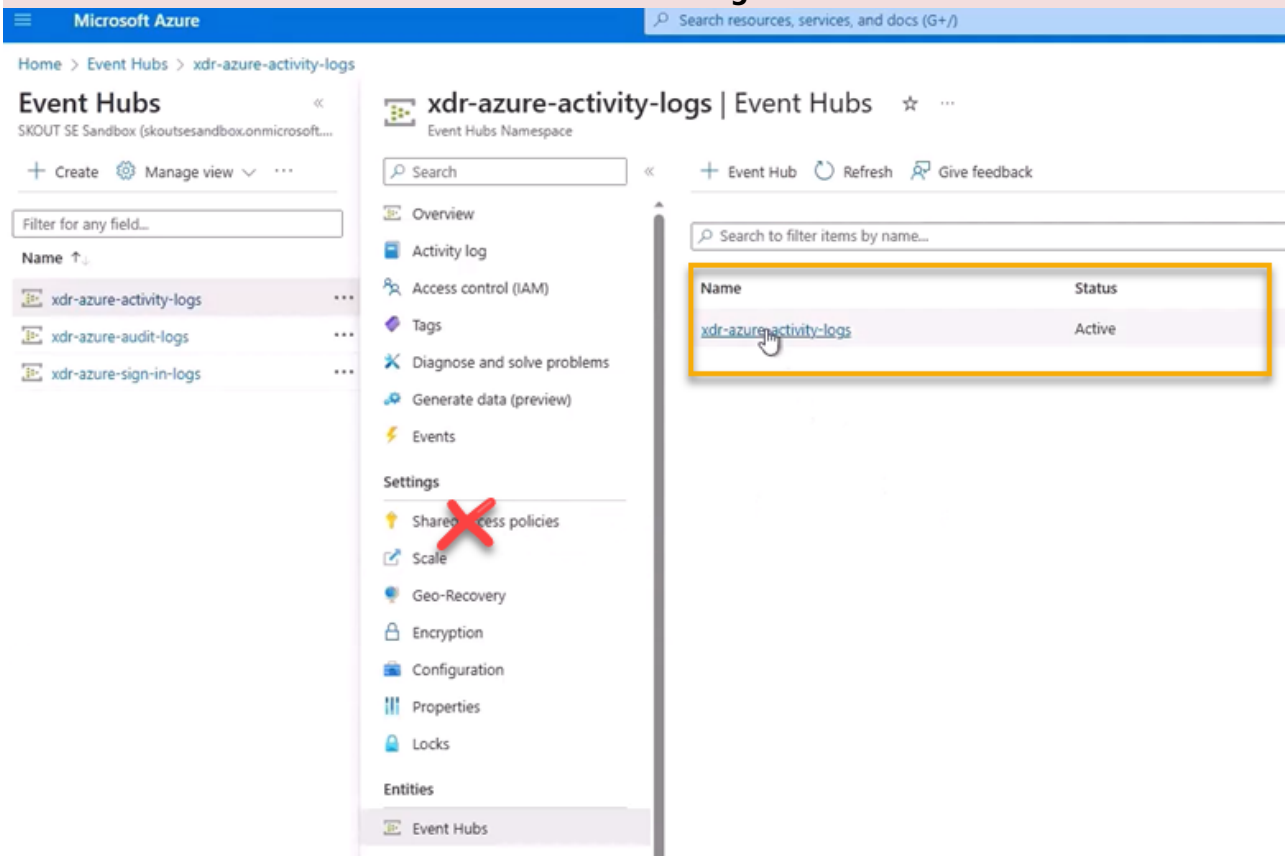
   We recommend the following naming convention:
   - xdr-azure-activity-logs
   - xdr-azure-audit-logs
   - xdr-azure-sign-in-logs



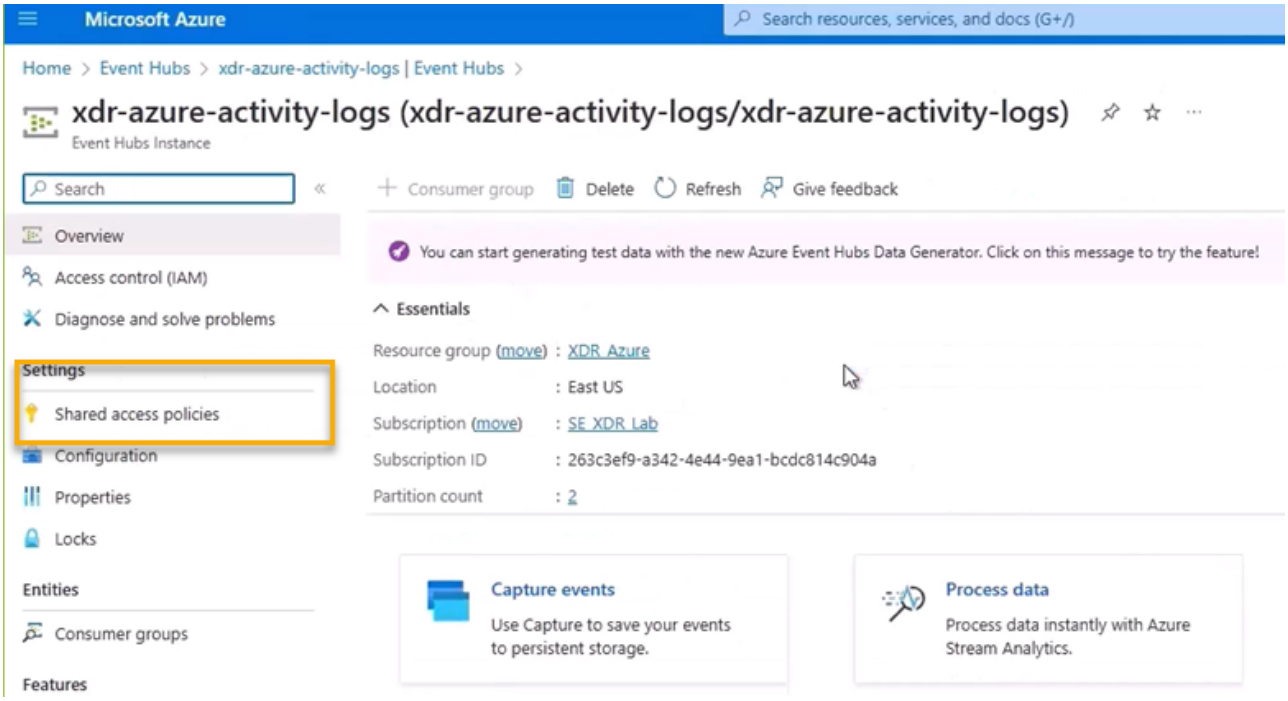
4. Repeat steps 2-3 for the rest of the namespaces.
5. Click **Review and Create**.
   The deployment may take a while.



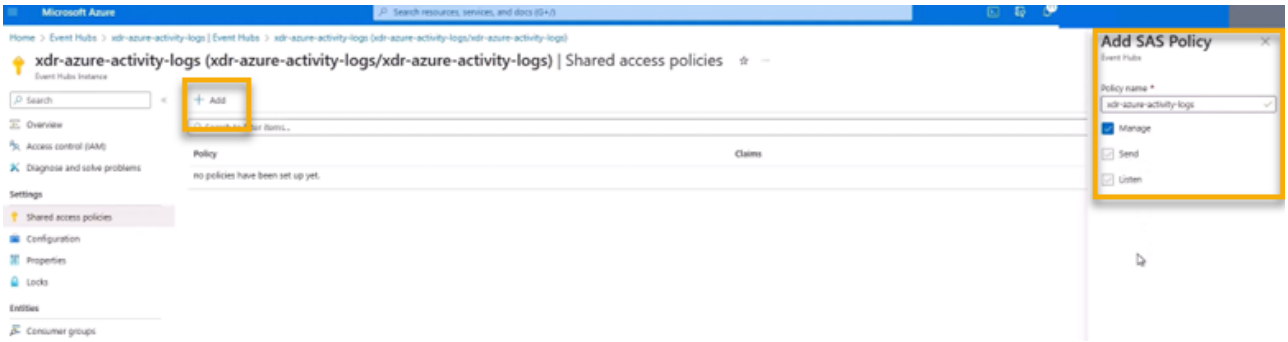
To set up an Event Hub Shared Access Policy

1. In **Event Hubs**, on the right, click the link **Event Hub Namespace** that you created in the previous procedure.
   Do *not* click **Shared Access Policies** under **Settings**.


2. Click **Shared Access Policies**.



3. Click **Add**.

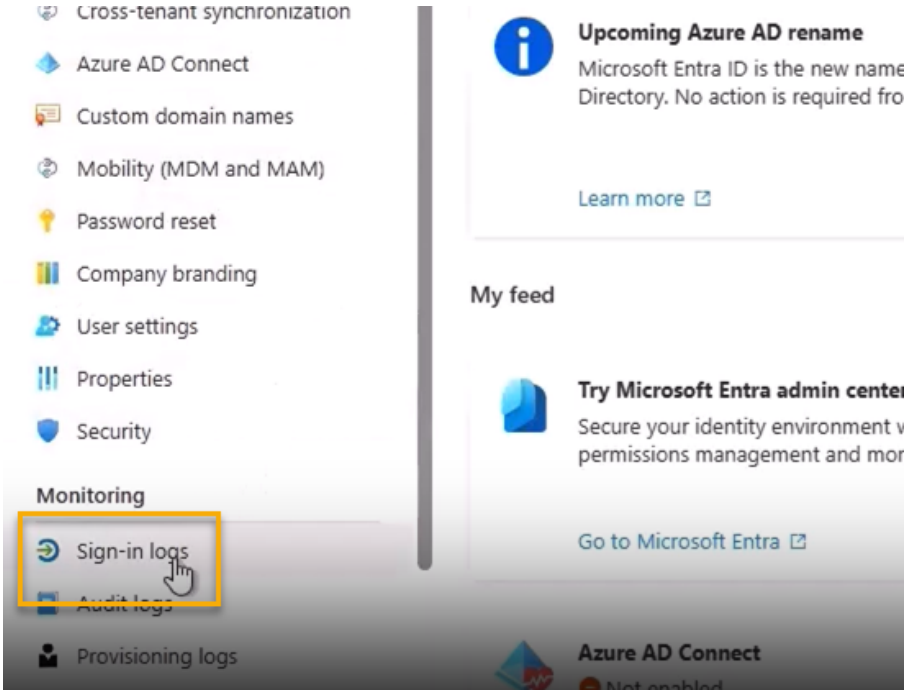


4. In **Add SAS Policy**, in **Policy Name**, type the name of the namespace.
5. Select the **Manage** checkbox.
6. Repeat steps 1-5 for the rest of the namespaces.

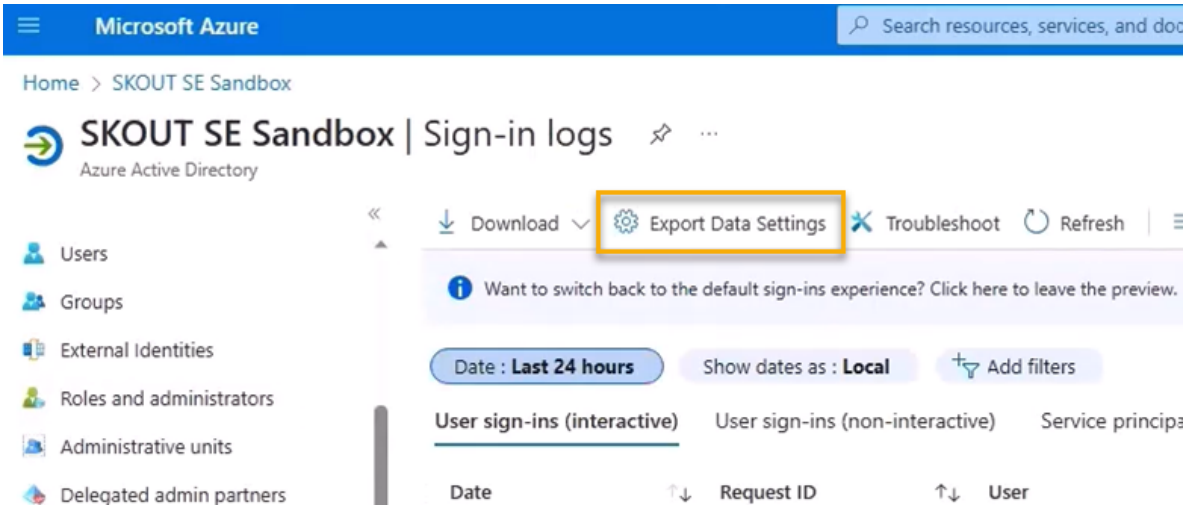
Part 2: Updating Diagnostic Settings

To update diagnostic settings for the sign in log

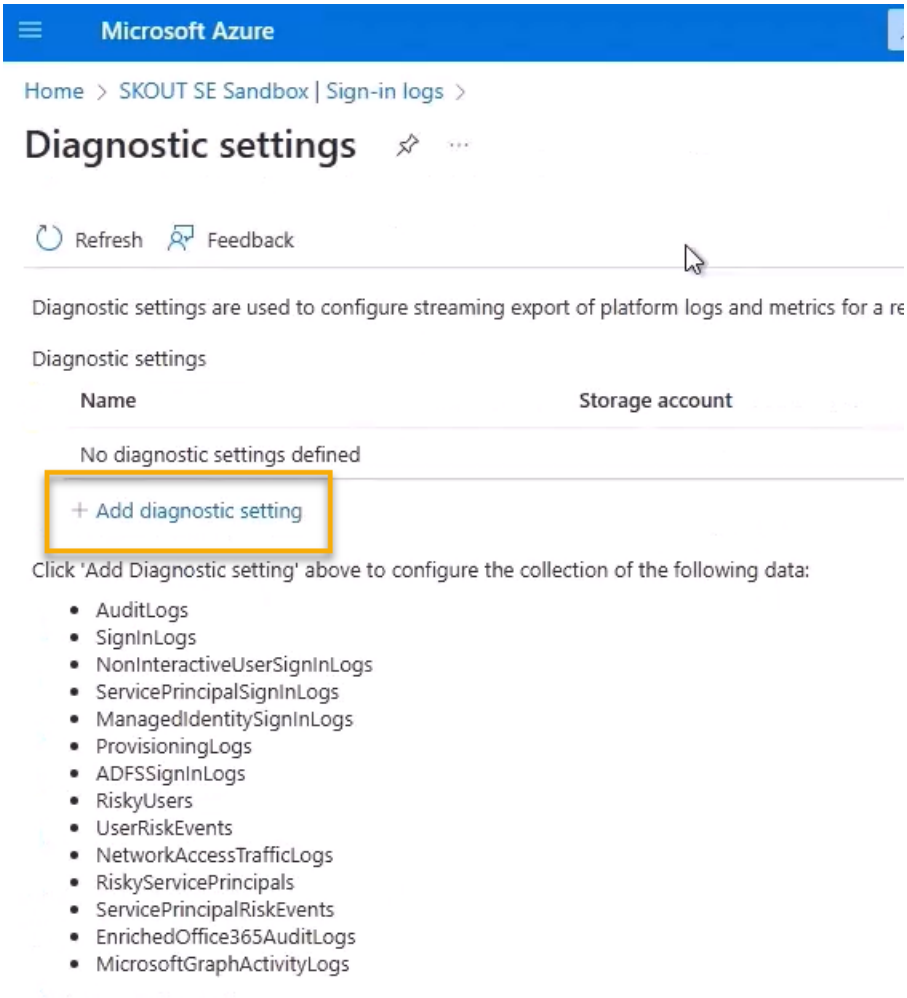
1. Navigate to **Azure Active Directory**.
2. In the **Monitoring** section, click **Sign-in logs**.



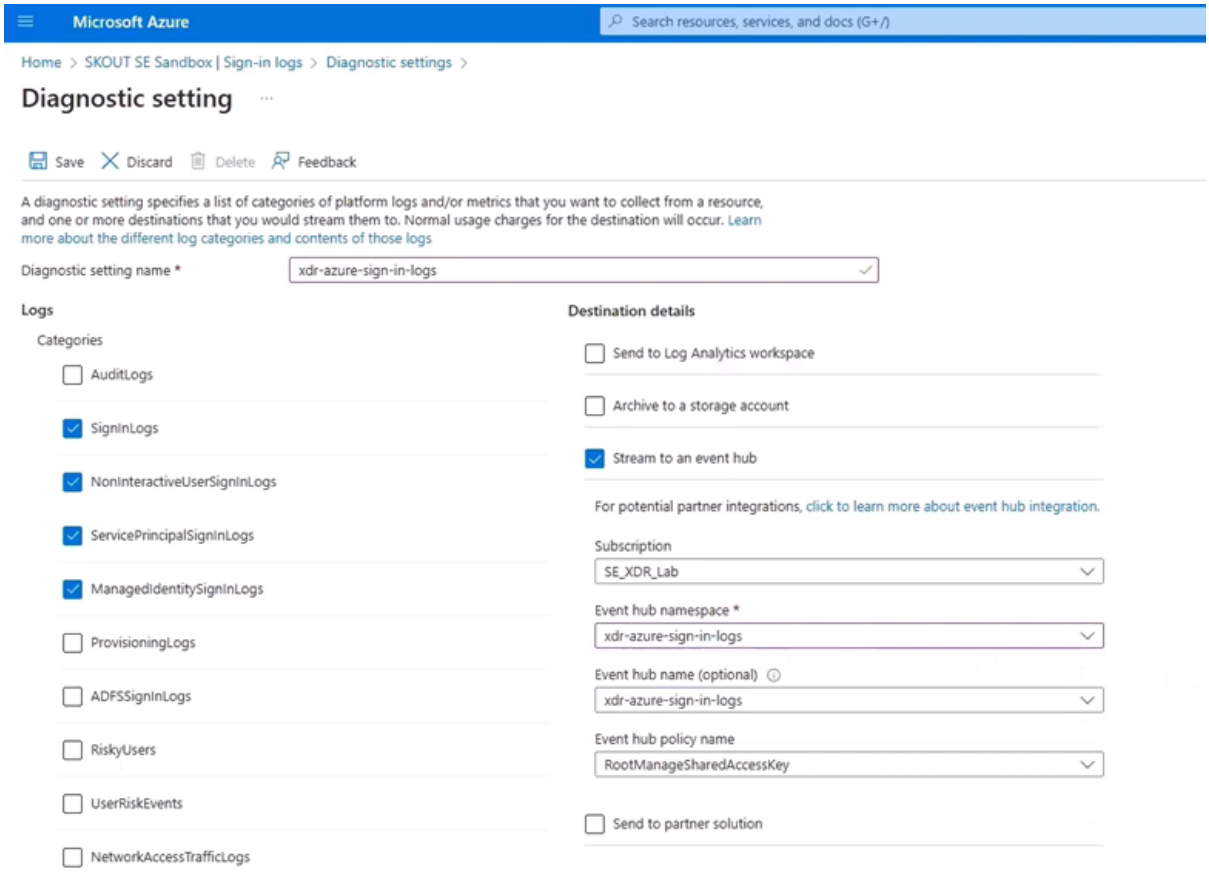
3. Click **Export Data Settings**.



4. Click **Add diagnostic setting**.



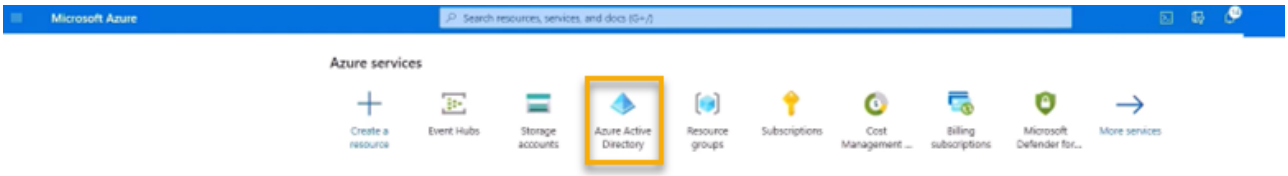
5. Do the following:
    - In **Diagnostic setting name**, type the name of your sign in log.
    - Select the following checkboxes:
        - **SignInLogs**
        - **NonInterctiveUserSignInLogs**
        - **ServicePrincipleSignInLogs**
        - **ManagedIddentitySignInLogs**
        - **Stream to an event hub**
    - Select the correct **Subscription and Event hub namespace** (Ex: xdr-azure-sign-in-logs).



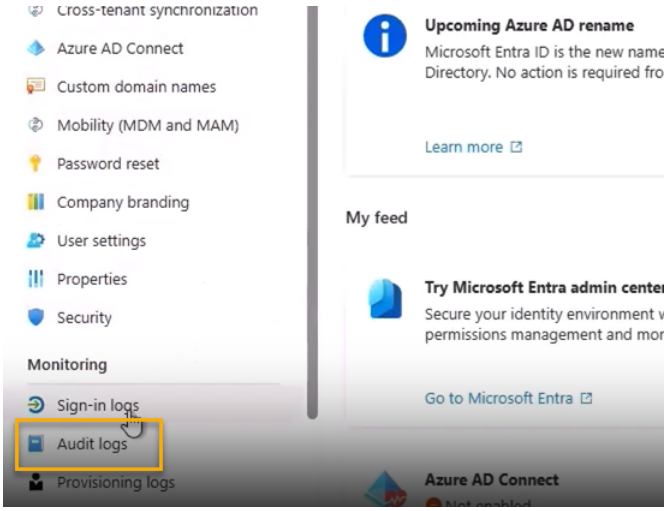
6. Click **Save**.

To update diagnostic settings for for the audit log and activity log

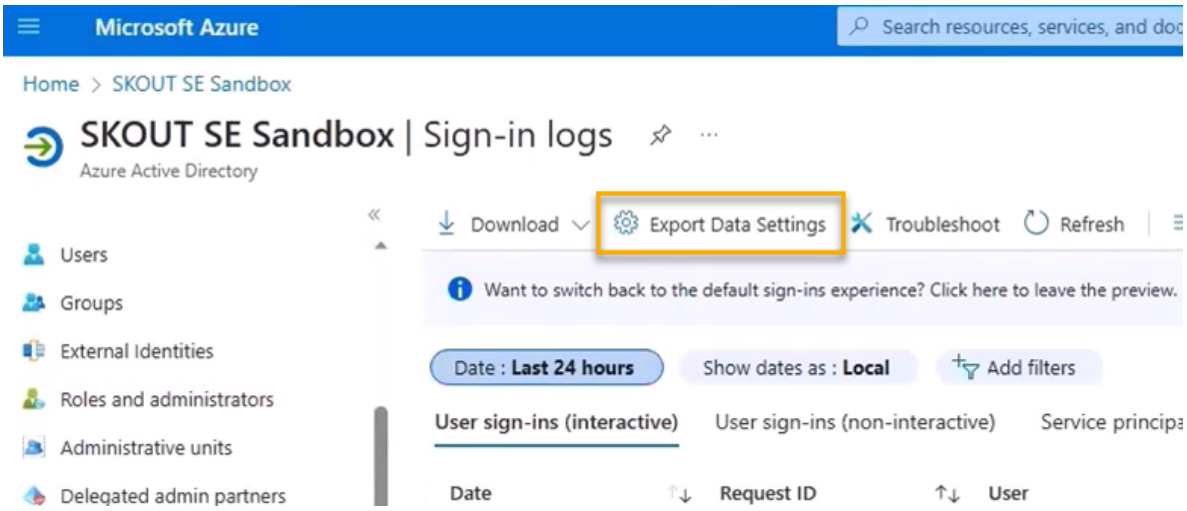
1. Navigate to **Azure Active Directory**.



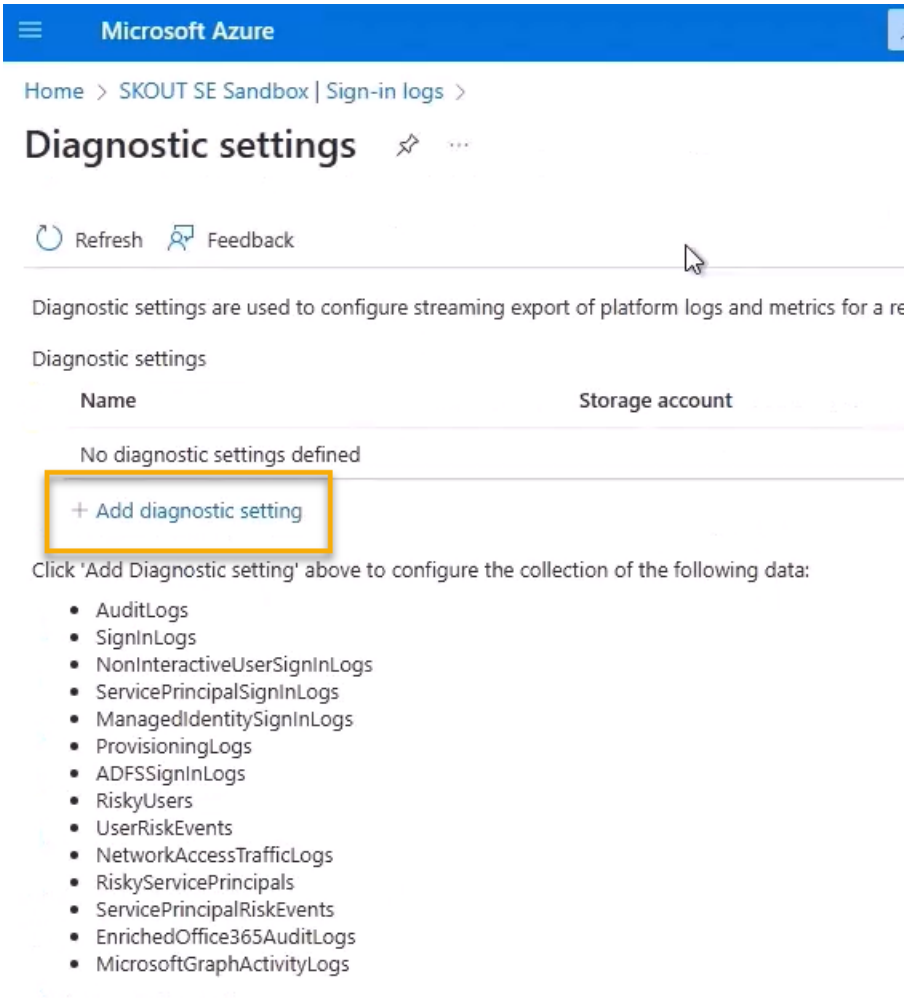
2. In the **Monitoring** section, click **Audit logs**.



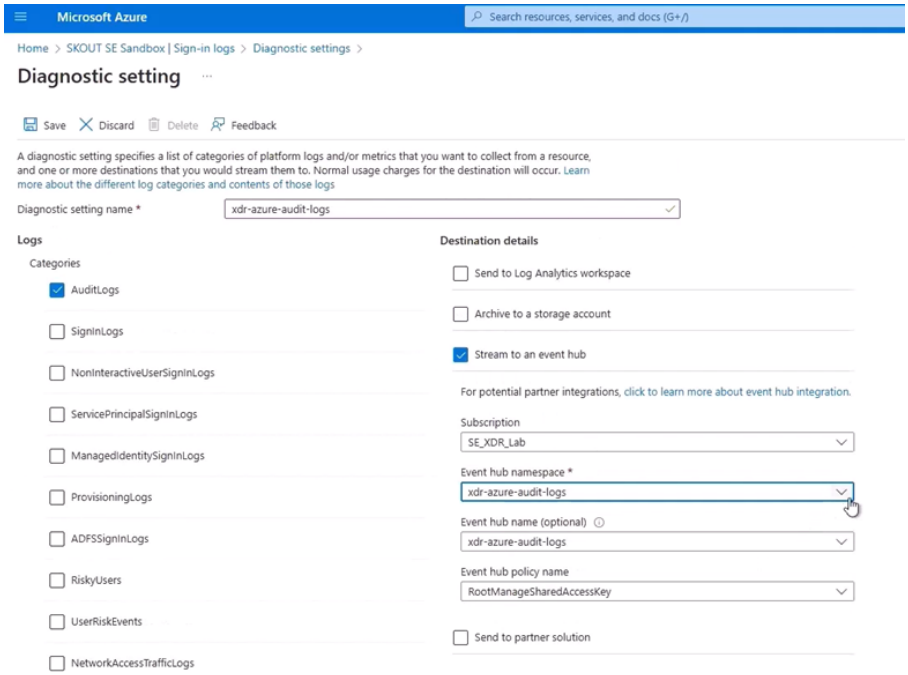
3. Click **Export Data Settings**.



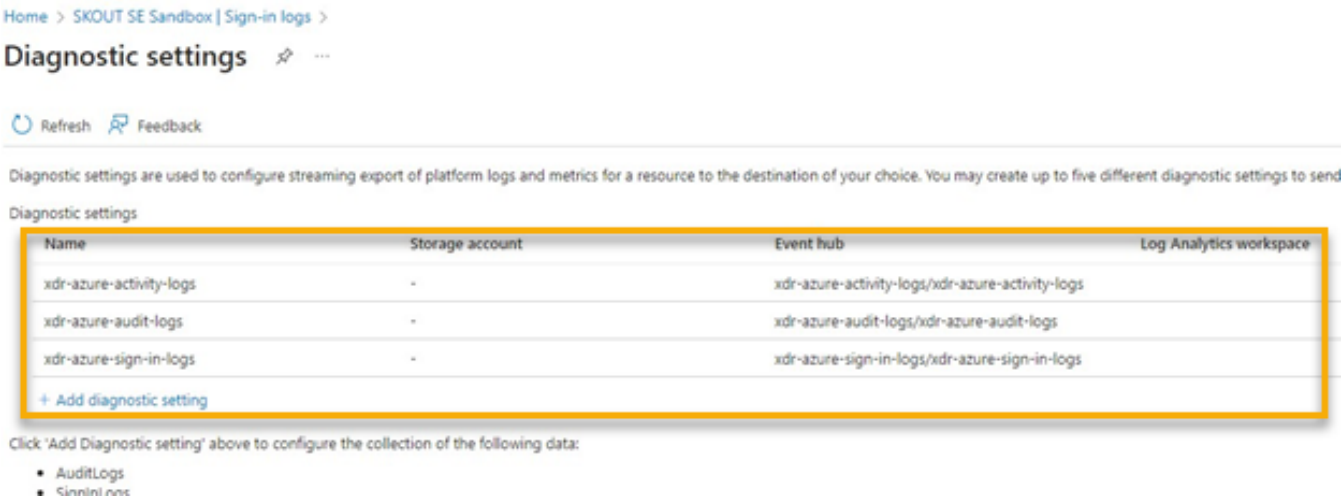
4. Click **Add diagnostic setting**.



5. Do the following:
    - In **Diagnostic setting name**, type the name of your audit log namespace.
    - Select the following checkboxes:
        - **AuditLogs**
        - **Stream to an event hub**
    - Select the correct S**ubscription and Event hub namespace** (Ex: xdr-azure-audit-logs).

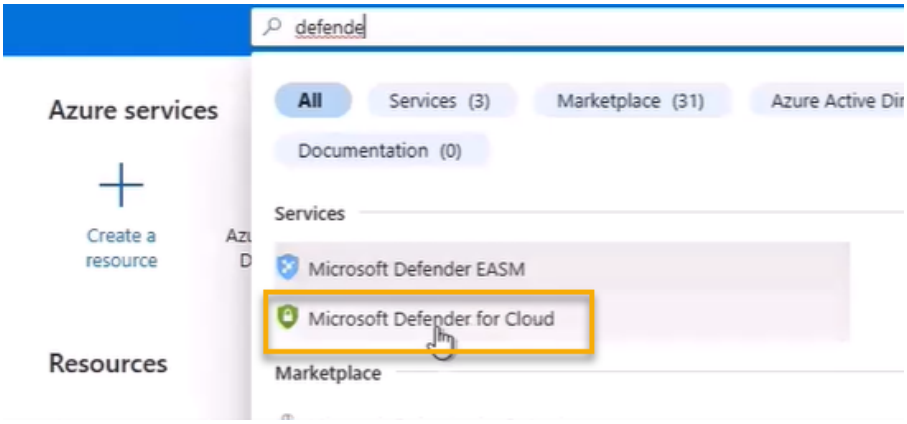


6. Click **Save**.
7. Repeat steps 1-6 for the activity log.

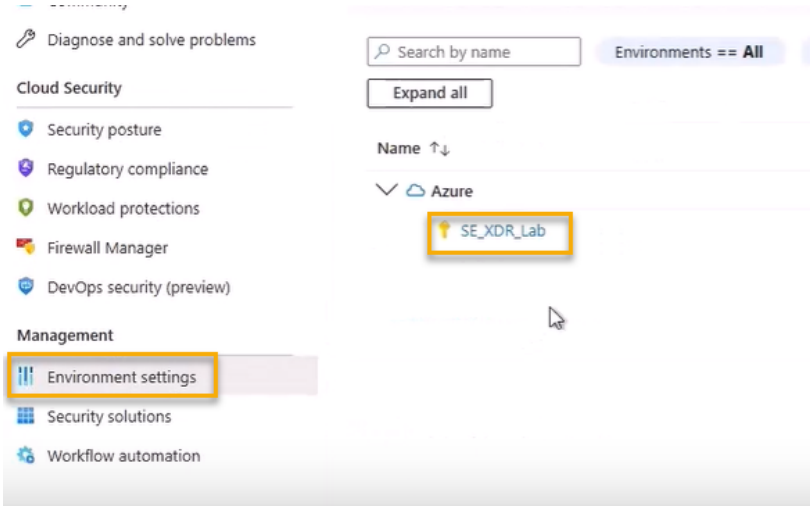


To set up Microsoft Defender for Cloud

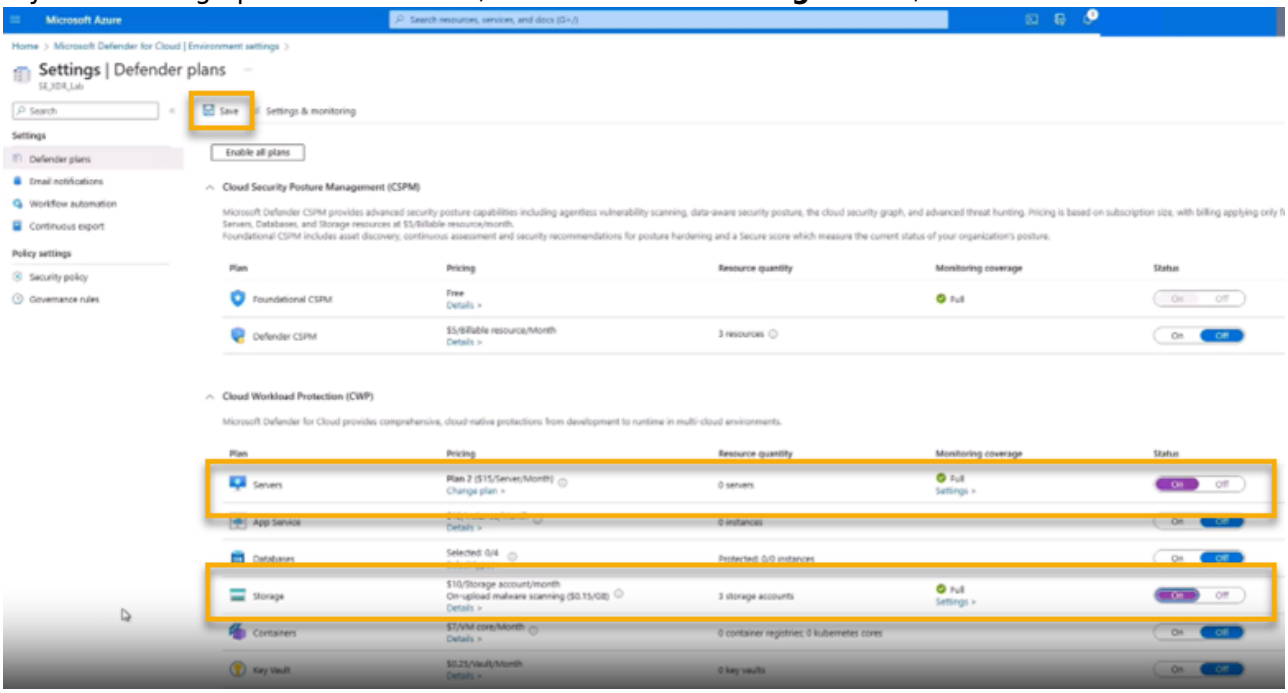
1. Navigate to **Microsoft Defender for Cloud**.



2. Under **Management**, click **Environment settings**.

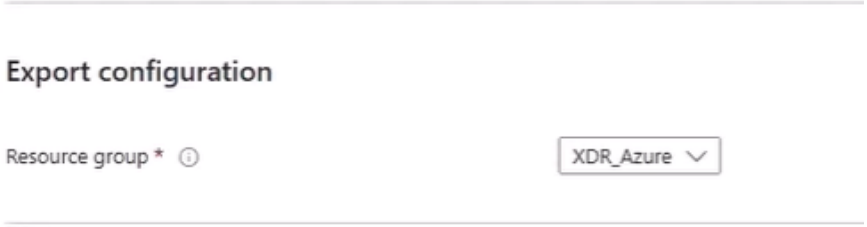


3. Select your subscription.
4. If you're setting up for the first time, set **Severs** and **Storage** to **On**, then click **Save**.



Enabling Microsoft Defender for Servers while another EDR is active can lead to performance issues.

5. Under the **Settings** section, click **Continuous Exports**.
6. Do the following:
7. Select the **Security recommendations** checkbox, and select **All recommendations**.
8. In **Security Alerts**, select **Low, Medium, High, Informational**.
9. Turn **Streaming Updates** on.
10. Turn **Snapshots** off.
11. In **Export configuration**, select your subscription.



12. In **Export Target**, do the following:
    - In **Subscription**, select your subscription
    - In **Event Hub namespace**, select the name of your activity log.
    - In **Event Hub name**, select the name of your activity log.
    - In **Event hub policy name**, select the name of your activity log.

13. Click **Save**.

Part 3: Barracuda XDR Dashboard Setup for Microsoft Azure

To set up Barracuda XDR Dashboard Setup for Microsoft Azure

1. In Azure, click **Event Hubs**, then click one of the activity logs.
2. Click **Event Hubs**, then lick the link of the log.
3. Click **Shared access policies**.
4. In the right side, copy the **Connection string-primary key**.
5. Open another browser tab and start **Barracuda XDR Dashboard**.
6. In **Barracuda XDR Dashboard**, click **Setup** > **Integrations**.

7. On the **Microsoft Azure** card, click **Setup**.
8. Select the **Enabled** checkbox.
9. In the **Activity Log** section, do the following:
10. In **Event Hub**, type the name of the **Activity Log**.
11. In **Connection String**, paste the **Connection string-primary key**.
12. In **Azure**, click **Home**, **Storage Accounts**.
13. Click the link of the Activity Log.
14. Copy the name of the Storage Account.
15. In **Barracuda XDR Dashboard**, in **Storage Account**, paste the name of the Storage Account.
16. In **Azure** , click **Access Keys**.
17. In the **key1** section, copy the Key.
18. In **Barracuda XDR Dashboard**, in **Storage Account Key**, paste the key.
19. Repeat steps 1-19 for the rest of the logs.
20. Click **Save**.

Figures