EASTWIND

Eastwind Active Directory Connector Setup Guide

The Challenge:

Enterprises today fight a complicated battle: there is a global army of hackers who never sleep and who are looking for new and creative ways to break into networks, whether hosted or on-premise. Eastwind arms security teams with comprehensive visibility.

The Solution:

EASTWIND
Active Directory

The Benefits:

- Complete cyber security and visibility of your SaaS solutions.
- Enhance your Breach Analytics with Eastwind for SaaS telemetry.

Overview

The Eastwind Active Directory (AD) Connector is designed to pair network traffic with AD domain users. Once activated, this information is sent to the Eastwind Breach Analytics Cloud for data enrichment. This document outlines the tasks required to connect the Eastwind Active Directory Connector to your domain controller.

In order to identify the users associated with network traffic (user-to-ip mapping), your Active Directory system integrates into the Eastwind Breach Analytics Cloud. This document describes the steps to connect an active directory system to the Eastwind Portal using the Eastwind Active Directory Connector. The following tasks are required to accomplish this:

- Setup domain authentication logging events on the active directory system.
- Create an Eastwind account to track the information.
- Install and configure the Eastwind Active Directory Connector.

We recommend running the Eastwind Active Directory Connector on a server that is not running the active directory components (primary or secondary domain controllers). Additionally, the Eastwind Active Directory Connector can run on a virtual machine(VM) or physical hardware.

Note: This document uses Windows Server 2016. Other Windows Server versions may vary slightly but the steps are the same.

Setup Domain Authentication Logging Events

The following steps configure the domain controller(DC) login settings for the Eastwind Active Directory Connector.

Note: This section needs to be completed on the primary domain controller.

Advanced Audit Policy Settings

To capture authentication events, the DC advanced audit policy must be configured to audit successful logon events.

To configure advanced domain logon audit policy settings, follow these steps:

1. Logon to the DC server using an account that has administrative privileges.
2. Select the Start button, click on the Windows Administrative Tools and then click on the Group Policy Management link.
3. In the console tree:
    a. Double click your forest e.g. eastwindnetworks.com.
    b. Double click Domains.
    c. Double click the DC (e.g. eastwindnetworks.com).
    d. Right click Default Domain Policy, and then click Edit.
4. Open the following items in this order:
    a. Double click the “Computer Configuration” folder.
    b. Double click the “Policies” folder.
    c. Double click the “Windows Settings” folder.
    d. Double click the “Security Settings” folder.
    e. Click on the “Advanced Audit Policy Configuration” folder.
    f. Click on the “Audit Policies” folder.

continued from previous section...

5. Click on the “Logon/Logoff” file.
6. In the right pane, double click on “Audit Logon” link.
7. Select the “Configure the following audit events” check box.
8. Select the “Success and Failure” check box.
9. Click the “OK” button.

Group Policy Configuration

The Eastwind Active Directory Connector uses remote WMI queries to verify whether a domain user is logged on or off. In this section, grant access to the Eastwind Active Directory Connector by configuring the Group Policy to enable Windows Management Instrumentation (WMI) access to a remote machine.

In the Group Policy Management Editor folder,

1. Open the following items in this order:
    a. Click on the “Administrative Templates” folder.
    b. Click on the “Network” folder.
    c. Click on the “Network Connections” folder.
    d. Click on the “Windows Firewall” folder.
    e. Click on the “Domain Profile” folder.
2. Double click on the “Windows Firewall: Allow inbounds remote administration exception” link.
3. Click the “Enabled” checkbox.
4. Click the “Ok” button.
5. Close the “Group Policy Management Editor” window pane.
6. Close the “Group Policy Management” control panel.
7. Close the “Windows Administrative Tools” control panel.

Update the Group Policy Settings

1. Select the “Start” link.
2. Type “cmd” in the field.
3. Right-click on “Command Prompt” and then click “Run as administrator” link.
4. Type “gpupdate” in the command prompt window and press enter.
5. Wait for the command to complete.

Verify that the Audit Policy Settings were Applied Correctly

1. Type the following exactly as follows: auditpol /get /category:“Logon/Logoff.
2. Verify that the setting for both Logon and Logoff is set to “Success and Failure”.
3. Close the Command Prompt window.

Create an Eastwind Networks Active Directory User

The Eastwind Active Directory Connector queries the domain controller event log configured above to obtain the user-to-ip mapping. To maintain security, create a “non-administrative” user with permissions to query the audit log. Perform the following steps to accomplish this.

- Create non-administrative domain user.
- Event log reading permission.
- WMI permission.
- DCOM permission.

Note: This section needs to be completed on the primary domain controller.

continued from previous section...

Create the Domain User Service Account

Please note: You must adjust these directions based on your organization's security policy

1. Click on the Start > Windows Administrative Tools address.
2. Double click on "Active Directory Users and Computers" folder.
3. On the left pane, right click on the "Users" link.
4. Select the "New" > "User" address.
5. Enter the following fields, Eastwind suggests:
    a. First name: Eastwind
    b. Last name: Audit
    c. User logon name: eastwindaudit (Note: you will need to enter this later)
6. Click the "Next" button.
7. Enter a secure password. (Note: you will need to enter this later)
8. Uncheck the "User must change password at next logon" box.
9. Check the "Password never expires" box.
10. Click the "Next" button.
11. Click the "Finish" button.

Grant User Audit Query

Add the user/group to the domain built in group: "Distributed COM Users" and "Event Log Readers".

1. In the right pane, right click the created "user" link.
2. Select the "Add to a group" button.
3. Click on the "Advanced" tab.
4. Click on the "Find Now" button.
5. In the bottom list, select the "Distributed COM Users" link.
6. Click the "OK" button.
7. Click on the "Advanced" button.
8. Click on the "Find Now" button.
9. In the bottom list, select the "Event Log Readers" link.
10. Click the OK button to close the advanced dialogue window.
11. Click the OK button to close the "Select Groups" window.
12. Close the "Active Directory Users and Computers" window.
13. Close the Windows Administrative window.

Grant Activation and Access Permissions

Give the user/group DCOM remote launch, activation permission, and remote access permission. To grant DCOM remote launch and activation permissions for a user/group, follow these steps.

1. Select the "Start" link.
2. Type "DCOMCNFG" in the box and press the Enter.

In the "component services" dialog box in the left pane:

1. Double click the "Component Services" link.
2. Double click the "Computers" link.
3. Right click the "My Computer" folder.
4. Select the "Properties" tab.

In the "My Computer properties" dialog box:

1. Click the "COM Security" tab.
2. Under "Launch and Activation Permissions" tab, click on "Edit Limits" link.
3. Click on the" Distributed COM Users" link and ensure that the following are set to "Allow":
    - Local Launch, Remote Launch, Local Activation, Remote Activation
4. Click the "Ok" button.

continued from previous section...

To grant DCOM Remote Access permissions for user/group, follow these steps.

11. In the “My Computer properties” dialog box, click the “COM Security” tab.
12. Under “Access Permissions”, click the “Edit Limits” button.
13. Click on the “ANONYMOUS LOGON” link and ensure that the following are set to “Allow”
    - Local Access, Remote Access
14. Click on the “Ok” button.
15. Click on the “Ok” button again.

Allow Remote Access WMI

1. Select the “Start” link and type “wmimgmt.msc”.
2. Press the “Enter” link to open the Windows Management Instrumentation Dialogue.
3. In the left pane, right click the “WMI Control” link and select the “Properties” tab.
4. Select the “Security” tab, expand “Root”.
5. Expand the “CIMV2” root.
6. Click the “Security” button.
7. Click the “Add” button to add the Eastwind Active Directory user created above.
8. Click on the “Advanced” link.
9. Click on the “Find Now” button and double click the user created above from the bottom list.
10. Click the “OK” button.
11. Ensure that the “Enable Account” permission and the “Remote Enable” permission are selected.
12. Click the “Advanced” button, then click select the domain user.
13. Click on the “Edit” link.
14. From the “Applies to” dropdown menu confirm it is set to the following: “this namespace and subnamespaces”.
15. Select the “OK” button to save changes.
16. Select the “OK” button to close all the windows in the WMI dialogue.

Restart WMI service via services.msc

1. Click the “Start” button.
2. Open the “Windows Administrative Tools” link.
3. Double click the “Services” link.
4. Right click and restart the “Windows Management Instrumentation” link.

Install and Configure the Active Directory Connector

The Eastwind Active Director Connecter msi installs and configures the following:

- The Windows service, which sends the user-to-ip mapping to the Eastwind Networks cloud.
- A GUI configurator application to configure the service.

Note: This section should be completed on a different server than the Domain Controller.

Download the Eastwind Active Director Connector

To get started, download the Eastwind Active Directory Connector software by logging into the Eastwind Portal at https://portal.eastwindnetworks.com. Once downloaded, install and configure the service using the configurator. You can launch configurator from the Start menu or from the installed directory.

1. Logon to the Eastwind Portal at https://portal.eastwindnetworks.com using the supplied credentials.
2. Click on the “Data Sources” link in the left navigation panel.
3. Click on the “AD Correlation” menu link in the top navigation panel.
4. Click on the “Download Installer” button.

continued from previous section...

Install the Eastwind Active Directory Connector

1. Once downloaded, install the software then locate the downloaded EWNADCorrelationSetup installer.
2. Double click on the “Installer” button. When it is complete it will exit silently.
3. Configure the Eastwind Active Directory Connector using the Eastwind Configuration Utility
    a. Browse to the following directory C:>Program Files (x86)>Eastwind Networks.
4. Double click on the “EWNADConfigurator” link.
5. Activate the service by entering the “Setup Token” found on the “AD Correlation” page on the Eastwind Portal.
6. Click the “Next” button after entering the AD Setup Token to configure the AD Correlation service.
7. Add the domain name, IP of the primary domain controller, username, and the password.
8. Click on the “Next” button.
9. The configurator will try to discover other domain controllers too (if there are any).

Note: You can also add manually.

10. Click on the “Apply” button.
11. Click on the “Close” button.

Once these steps are completed, the active directory user-to-ip correlation data will be sent to the Eastwind Breach Analytics Cloud.

Verify the Eastwind Active Directory Connector Connection

To verify the Eastwind Active Directory Connector connection, browse to the following folder:

C:>Program Files (x86)>Eastwind Networks

and open the EWNADConfigurator Text Document. This document logs transactions between the Eastwind Active Directory Connector and the Domain Controller (user/IP pairings).

Note: These files will need to be monitored to ensure they do not fill up disk space. The files do not need to be preserved although the Eastwind Support team may need access to the logs for support purposes.

EASTWIND

For more information on Eastwind Active Directory Connector,
please see eastwindnetworks.com