Active Directory

Background

The Microsoft Active Directory Directory Servers logs analysis App automatically Collect - Read - Parse - Analyzes - Reports all machine generated log data of the server and presents a comprehensive set of graphs and reports to analyze machine generated data. Use a predefined set of dashboards and gadgets to visualize and address the system software, code written, and infrastructure during development, testing, and production. This logs analysis App helps measure, troubleshoot, and optimize your servers integrity, stability and quality with the several visualization and investigation dashboards.

Steps:

1. The Microsoft Active Directory App is running on Application, Security and System standard event logs (*.evtx).
   When adding/editing the logs to XpoLog it is mandatory to apply the correct log type(s) to each of the logs:
   a. **windows** - all logs that the application will analyze must have **windows** as a log type
   b. **activeDirectory** - all the logs must also be configured to have **activeDirectory** as a log type
   c. **application -** only the **Application** log must also be configured to have **application** as a log type
   d. **security -** only the **Security** log must also be configured to have **security** as a log type
   e. **system -** only the System log must also be configured to have **system** as a log type

2. Once the required information is set, on each log click next and edit the log pattern, this step is crucial to the accuracy and deployment of the Microsoft Active Directory App. Use the following patterns for each of the logs:
   a. Active Directory Application event log:
      {priority:Type,ftype=type,Error;Warning;Information;Success;Audit Failure;Audit Success}*;*{timestamp:Date,MM/dd/yyyy HH:mm:ss}{regexp:Account Name,refName=Description;ftype=account name,Account Name:\s+(\S+).*}{regexp:Account Domain,refName=Description;ftype=domain,Account Domain:\s+(\S+).*}*;*{text:Source,ftype=source}*;*{text:Category,ftype=category}*;*{number:Event,ftype=event}*;*{text:User,ftype=user}*;*{text:Computer,ftype=computer}*;*{string:Description,ftype=description}
   b. Active Directory Security event log:
      {priority:Type,ftype=type,Error;Warning;Information;Success;Audit Failure;Audit Success}*;*{timestamp:Date,MM/dd/yyyy HH:mm:ss}{regexp:Account Name,refName=Description;ftype=accountname,Account Name:\s+(\S+).*}{regexp:Account Domain,refName=Description;ftype=domain,Account Domain:\s+(\S+).*}*;*{text:Source,ftype=source}*;*{text:Category,ftype=category}*;*{number:Event,ftype=event}{map:Event Description,ftype=event description;refIndex=6,file:knowledge/repository/system/win/map/winEventsMap.prop}{map:Category Description,ftype=category description;refIndex=6,file:knowledge/repository/system/win/map/winEventsCategoryMap.prop}{map:Sub Category,ftype=sub category;refIndex=6,file:knowledge/repository/system/win/map/winEventsSubCategoryMap.prop}*;*{text:User,ftype=user}{regexp:Logon ID,refName=description;ftype=logon id,Logon ID:\s+(\S+).*}*;*{text:Computer,ftype=computer}*;*{regexp:Group Name,ftype=usergroup;refName=Description,Group Name:\s([^\n]+).*}{regexp:Object Name,ftype=object;refName=Description,(New Account:.*Account Name:\s+|Target Account:.*\tAccount Name:\s+|New Computer Account:.*Account Name:\s+|Target Computer:.*Account Name:\s+|Computer Account That Was Changed:.*\tAccount Name:\s+|Member:.*Account Name:\s+CN=|Member:.*Account Name:\s+cn=|New Logon:.*\tAccount Name:\s|Member:.*Account Name:\s|Account That Was Locked Out:.*\tAccount Name:\s|Account Whose Credentials Were Used:.*\tAccount Name:\s|Object Name:\s+)[XPLG_PARAM([^\n,]+)]}{regexp:Object Type,ftype=objecttype;refName=Description,Object Type:\s+([^\n]+).*}{regexp:Handle ID,ftype=handleid;refName=Description,Handle ID:\s+([^\n]+).*}{regexp:Source Address,ftype=sourceip;refName=Description,\tSource Address:\s([^\n]+)}{regexp:Destination Address,ftype=targetip;refName=Description,\tDestination Address:\s([^\n]+)}{string:Description,ftype=description}
   c. Active Directory System event log:
      {priority:Type,ftype=type,Error;Warning;Information;Success;Audit Failure;Audit Success}*;*{timestamp:Date,MM/dd/yyyy HH:mm:ss}{regexp:Account Name,refName=Description;ftype=account name,Account Name:\s+(\S+).*}{regexp:Account Domain,refName=Description;ftype=domain,Account Domain:\s+(\S+).*}*;*{text:Source,ftype=source}*;*{text:Category,ftype=category}*;*{number:Event,ftype=event}*;*{text:User,ftype=user}*;*{text:Computer,ftype=computer}*;*{string:Description,ftype=description}