WebLogic

Background

The WebLogic 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 WebLogic logs analysis App helps measure, troubleshoot, and optimize your servers integrity, stability and quality with the several visualization and investigation dashboards.

Steps:

1. The WebLogic App is running on Base Domain, AdminServer, DefaultAuditRecorder, access and WFCA_Access standard logs. When adding/editing the logs to XpoLog it is mandatory to apply the correct log type(s) to each of the logs:
    a. **weblogic** - all logs that the application will analyze must have **weblogic** as a log type.
    b. **basedomain** - only the Base Domain logs must also be configured to have **basedomain** as a log type.
    c. **adminserver** - only the AdminServer logs must also be configured to have **adminserver** as a log type.
    d. **audit** - only the DefaultAuditRecorder logs must also be configured to have **audit** as a log type.
    e. **access** - only the Access and the WFCA_Access log must also be configured to have **access** as a log type.
    f. **w3** - only the Access and the WFCA_Access log must also be configured to have **w3** 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 Linux App. Use the following patterns for each of the logs:
    a. Base_Domain:
    ####<{date:Date,MMM dd, yyyy hh:mm:ss a z}>
    <{priority:Priority,ftype=status;,TRACE;DEBUG;INFO;NOTICE;WARNING;ERROR;CRITICAL;ALERT;EMERGENCY}>
    <{text:Type,ftype=subsystem}> <{text:Machine_Name,ftype=machinename}> <{text:Server_Name,ftype=servername}>
    <{text:ThreadID,ftype=thread}>
    <{block,start,emptiness=true}<{block,end,emptiness=true}{text:UserID,ftype=username;,}>{block,start,emptiness=true}
    >{block,end,emptiness=true} <{text:Transaction_ID,ftype=transaction}>
    <{text:Diagnostic_Context_ID,ftype=diagcontext}> <{text:Raw_Time_Value,ftype=rawtime}>
    {block,start,emptiness=true}{regexp:Severity-Value,ftype=severityvalue;refName=Error
    Details,severity-value:\s([^\u005D]+).*}{regexp:RID,ftype=rid;refName=Error
    Details,rid:\s([^\u005D]+).*}{regexp:Partition-ID,ftype=partitionid;refName=Error
    Details,partition-id:\s([^\u005D]+).*}{regexp:Partition-Name,ftype=partitionname;refName=Error
    Details,partition-name:\s([^\u005D]+).*}<{text:Error Details,ftype=errordetails}>
    {block,end,emptiness=true}<BEA-{number:BEA,ftype=messageid}> <{string:Message,ftype=message}>{text}
    b. Admin_Server:
    ####<{date:Date,MMM dd, yyyy hh:mm:ss a z}>
    <{priority:Priority,ftype=status;,TRACE;DEBUG;INFO;NOTICE;WARNING;ERROR;CRITICAL;ALERT;EMERGENCY}>
    <{text:Type,ftype=subsystem}> <{text:Machine_Name,ftype=machinename}> <{text:Server_Name,ftype=servername}>
    <{text:ThreadID,ftype=thread}>
    <{block,start,emptiness=true}<{block,end,emptiness=true}{text:UserID,ftype=username;,}>{block,start,emptiness=true}
    >{block,end,emptiness=true} <{text:Transaction_ID,ftype=transaction}>
    <{text:Diagnostic_Context_ID,ftype=diagcontext}> <{text:Raw_Time_Value,ftype=rawtime}>
    {block,start,emptiness=true}{regexp:Severity-Value,ftype=severityvalue;refName=Error
    Details,severity-value:\s([^\u005D]+).*}{regexp:RID,ftype=rid;refName=Error
    Details,rid:\s([^\u005D]+).*}{regexp:Partition-ID,ftype=partitionid;refName=Error
    Details,partition-id:\s([^\u005D]+).*}{regexp:Partition-Name,ftype=partitionname;refName=Error
    Details,partition-name:\s([^\u005D]+).*}<{text:Error Details,ftype=errordetails}>
    {block,end,emptiness=true}<BEA-{number:BEA,ftype=messageid}> <{string:Message,ftype=message}>{text}
    c. DefaultAuditRecorder:
    First Pattern - #### Audit Record Begin <{date:Date,MMM dd, yyyy hh:mm:ss a}> <Severity
    ={text:Severity,ftype=status}> <<<Event Type = {text:Event Type,ftype=eventtype} ><Subject:
    {text:Subject,ftype=subject}{eol}>{regexp:ONCE,\u003CONCE\u003E}<<jndi>><type=<{text:jndi,ftype=type}>,
    application={text:Application,ftype=application}, path={text:Path,ftype=path},
    action={text:Action,ftype=action}>{string:End Of Record} Audit Record End ####
    Second Pattern - #### Audit Record Begin <{date:Date,MMM dd, yyyy hh:mm:ss a}> <Severity
    ={text:Severity,ftype=status}> <<<Event Type = {text:Event Type,ftype=eventtype}><Subject = Subject:
    {text:Subject,ftype=subject}{eol}{string:Principal,ftype=principal}>{string} type=<{text:jndi,ftype=type}>,
    {string:Message,ftype=message} Audit Record End ####
    d. **Access:**
    Default Pattern - {geoip:Client IP,ftype=remoteip} - {text:Remote User,ftype=remoteuser}
    [{date:Date,locale=en,dd/MMM/yyyy:HH:mm:ss z}] "{choice:Method,ftype=reqmethod;,GET;POST;HEAD}
    {url:URL,paramsFtype=querystring;ftype=requrl;paramsName=Query;,} {text:Request Protocol,ftype=reqprotocol;,}"

{number:ResponseStatus,ftype=respstatus} {number:Bytes Sent,ftype=bytesent}{eoe}
for more information see below the format Conversion Table:

Format String	Appear as	Description	XpoLog Pattern
Date + Time	date time	The date on which the activity occurred. The time, in coordinated universal time (UTC), at which the activity occurred.	`{date:Date,yyyy-MM-ddHH:mm:ss;yyyy-MM-dd HH:mm:ss}{tab}`
Client IP Address	c-ip	The IP address of the client that made the request.	{geoip:ClientIP,ftype=remoteip}{tab}
User Name	cs-username	The name of the authenticated user who accessed your server. Anonymous users are indicated by a hyphen.	{text:Remote User,ftype=remoteuser}
Server IP Address	s-ip	The IP address of the server on which the log file entry was generated.	{ip:ServerIP,ftype= localip}{block,start,emptiness=true}:{number:ServerPort,ftype=serverport}{block,end,emptiness=tru
Method	cs-method	The requested action, for example, a GET method.	{choice:Method,ftype=reqmethod;,GET;POST;HEAD}
Full-URI	cs-uri	The full requested URI	"{choice:Method,ftype=reqmethod;,GET;POST;HEAD} {url:URL,paramsFtype=querystring;ftype=requrl;paramsName=Query;,} {text:Request Protocol,ftype=reqprotocol;,}"
URI Stem	cs-uri-stem	The target of the action, for example, Default.htm.	{text:Request URL,ftype=requrl}
URI Query	cs-uri-query	The query, if any, that the client was trying to perform. A Universal Resource Identifier (URI) query is necessary only for dynamic pages.	{text:queryString,ftype= querystring}
HTTP Status	sc-status	The HTTP status code.	{number:ResponseStatus,ftype=respstatus}

Bytes Sent	bytes	The number of bytes that the server sent.	{number:Bytes Sent,ftype=bytesent}
Client Domain	c-dns	The domain name of the requesting client.	{text:Client Domain,ftype=clientdomain}
Server Domain	s-dns	The domain name of the requested server.	{text:Server Domain,ftype=serverdomain}
Comment	sc-comment	The comment returned with status code, for instance "File not found".	{text:Comment,ftype=comment}
Time Taken	time-taken	The length of time that the action took, in seconds.	{number:Time Taken,ftype=processrequestsecs}

e. WFCA_Access

Default Pattern - {geoip:ClientIP,ftype=remoteip}{tab}{ip:ServerIP,ftype=localip}{block,start,emptiness=true}:{number:ServerPort,ftype=serverport}{block,end,emptiness=true}{tab}{text:Remote User,ftype=remoteuser;,}{tab}{date:Date,yyyy-MM-ddHH:mm:ss;yyyy-MM-dd HH:mm:ss}{tab}{choice:Method,ftype=reqmethod;,GET;POST;HEAD}{tab}{url:URL,paramsFtype=querystring;ftype=requrl;paramsName=Query;,}{tab}{text:ResponseStatus,ftype=respstatus;,}{block,start,emptiness=true}{tab}{block,end,emptiness=true}{eoe}

for more information see below the format Conversion Table:

Format String	Appear as	Description	XpoLog Pattern
Date + Time	date time	The date on which the activity occurred. The time, in coordinated universal time (UTC), at which the activity occurred.	`[{date:Date,locale=en,dd/MMM/yyyy:HH:mm:ss z}]`
Client IP Address	c-ip	The IP address of the client that made the request.	{geoip:ClientIP,ftype=remoteip}{tab}
User Name	cs-username	The name of the authenticated user who accessed your server. Anonymous users are indicated by a hyphen.	{text:Remote User,ftype=remoteuser;,}{tab}

Server IP Address	s-ip	The IP address of the server on which the log file entry was generated.	{ip:ServerIP,ftype= localip}{tab}
Method	cs-method	The requested action, for example, a GET method.	{choice:Method,ftype=reqmethod;,GET;POST;HEAD}{tab}
Full-URI	cs-uri	The full requested URI	{url:URL,paramsFtype=querystring;ftype=requrl;paramsName=Query;,}{tab}
URI Stem	cs-uri-stem	The target of the action, for example, Default.htm.	{text:Request URL,ftype=requrl}{tab}
URI Query	cs-uri-query	The query, if any, that the client was trying to perform. A Universal Resource Identifier (URI) query is necessary only for dynamic pages.	{text:QueryString,ftype=querystring}{tab}
HTTP Status	sc-status	The HTTP status code.	{text:ResponseStatus,ftype=respstatus;,}{block,start,emptiness=true}{tab}{block,end,emptiness=tru
Bytes Sent	bytes	The number of bytes that the server sent.	{number:Bytes Sent,ftype=bytesent;,}{block,start,emptiness=true}{tab}{block,end,emptiness=true}
Client Domain	c-dns	The domain name of the requesting client.	{text:Client Domain,ftype=clientdomain;,}{tab}
Server Domain	s-dns	The domain name of the requested server.	{text:Server Domain,ftype=serverdomain;,}{tab}
Comment	sc-comment	The comment returned with status code, for instance "File not found".	{text:Comment,ftype=comment;,}{tab}
Time Taken	time-taken	The length of time that the action took, in seconds.	{number:Time Taken,ftype=processrequestsecs;,}{tab}