aardio 范例: 查询系统日志

```
//查询系统日志
import console.int;
import com.wmi;
import sys.acl;

for event in com.wmi.eachProperties(`SELECT * FROM Win32_NTLogEvent WHERE
     Logfile = "System" AND ( EventCode=7001 OR EventCode=7002 OR EventCode=6005 OR EventCode=6006 )` ) {
/*
    console.log( "Category: ", event.Category);
    console.log( "Computer Name: ", event.ComputerName);
    console.log( "Event Code: ", event.EventCode);
    console.log( "Message: ", event.Message);
    console.log( "Record Number: ", event.RecordNumber);
    console.log( "Source Name: ", event.SourceName);
    console.log( "Event Type: ", event.Type);
    console.log( "User: ", event.User);
    console.dumpTable(event)
*/

    var tm = time.utc( event.TimeWritten ).local();

    if(event.EventCode==7001 && event.SourceName=="Microsoft-Windows-Winlogon"){
        var idx,sid = table.find(event.InsertionStrings,lambda(v) string.startWith(v,"S-"));
        var userName = sys.acl.sidStringToUserName(sid);

        console.log(tm,userName + " 登录成功")
    }
    if(event.EventCode==7002 && event.SourceName=="Microsoft-Windows-Winlogon"){
        var idx,sid = table.find(event.InsertionStrings,lambda(v) string.startWith(v,"S-"));
        var userName = sys.acl.sidStringToUserName(sid);

        console.log(tm,userName, " 已注销" )
    }
    elseif(event.SourceName=="EventLog") {
        console.log(tm,event.Message,event.SourceName,event.EventCode)
        if(event.EventCode == 6005) console.more(1)
    }
}
```

Markdown 格式