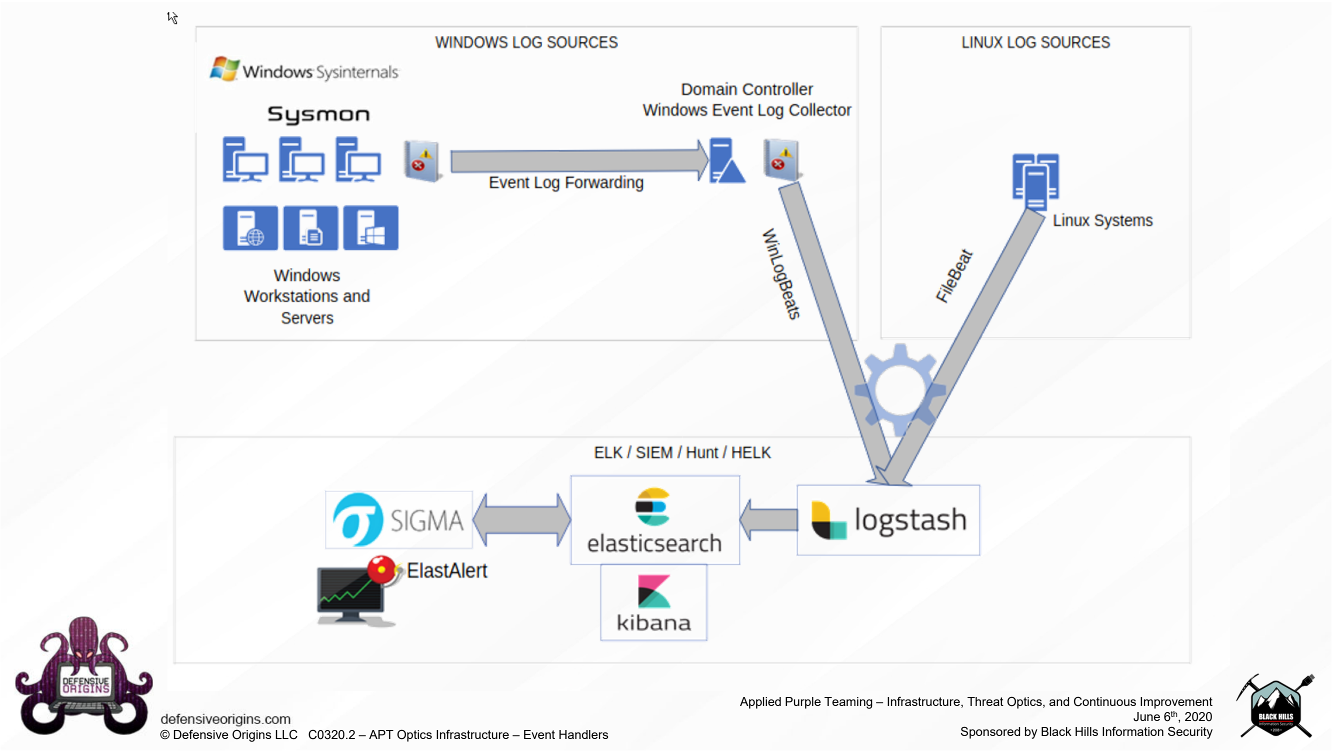
Applied Purple Teaming

Infrastructure, Threat Optics, and Continuous Improvement

June 6, 2020

LC0320

Event Handlers
WEC / WEF
Event Subscriptions



WINDOWS LOG SOURCES

Windows Sysinternals

Sysmon

Windows Workstations and Servers

Event Log Forwarding

Domain Controller
Windows Event Log Collector

WinLogBeats

LINUX LOG SOURCES

Linux Systems

FileBeat

ELK / SIEM / Hunt / HELK

SIGMA

ElastAlert

elasticsearch

kibana

logstash

https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection

What’s an Admin to do with all those Logs?

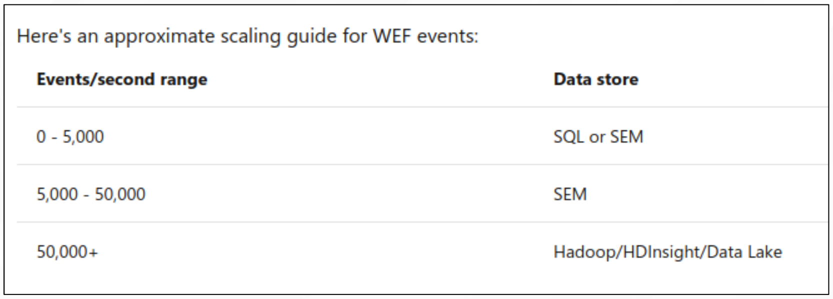
Windows Event Forwarding (WEF) to the rescue!

- Configuration tells an endpoint where to send its logs (Push)

OR

- Configuration tells an endpoint who is coming for them (Pull)

Pushed out via GPO



Here's an approximate scaling guide for WEF events:

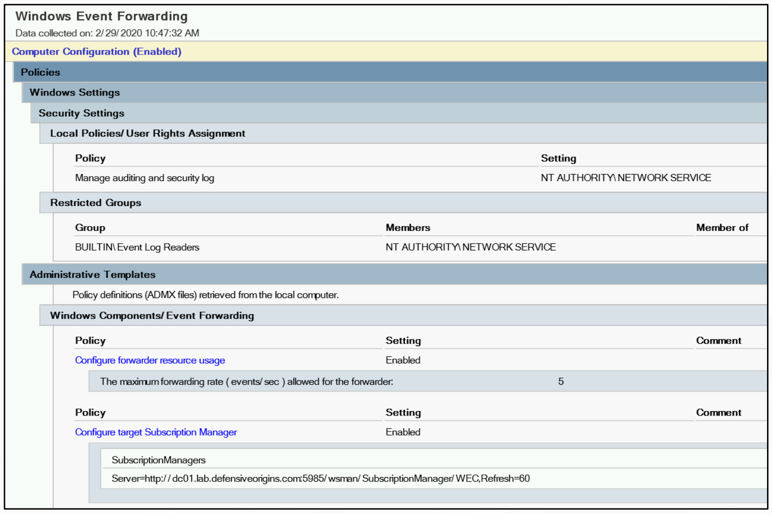
Events/second range	Data store
0 - 5,000	SQL or SEM
5,000 - 50,000	SEM
50,000+	Hadoop/HDInsight/Data Lake

Windows Event Forwarding

- Push or pull - not both
- Will queue events (size, see next bullet)
- Client buffer is size of windows event log
- Increase buffer by bumping log size
- Delivery timing options are configurable
- IPv4 / IPv6 ready
- Encrypted via Kerberos on domain
- WEF Servers can be HA'd

Deploy via GPO

- Define collector server[s]
- Provide necessary privileges
- Define resource usage (events/sec)



Windows Event Forwarding

Data collected on: 2/29/2020 10:47:32 AM

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Local Policies/User Rights Assignment

Policy	Setting
Manage auditing and security log	NT AUTHORITY\NETWORK SERVICE

Restricted Groups

Group	Members	Member of
BUILTIN\Event Log Readers	NT AUTHORITY\NETWORK SERVICE	

Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/Event Forwarding

Policy	Setting	Comment
Configure forwarder resource usage	Enabled	

The maximum forwarding rate (events/sec) allowed for the forwarder: 5

Policy	Setting	Comment
Configure target Subscription Manager	Enabled	

SubscriptionManagers

Server=http://dc01.lab.defensiveorigins.com:5985/wsman/SubscriptionManager/WEC,Refresh=60

https://social.technet.microsoft.com/wiki/contents/articles/33895.windows-event-forwarding-survival-guide.aspx
https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection
https://github.com/nsacyber/Event-Forwarding-Guidance

Who’s Listening? The Windows Event Collector (WEC)

Windows Event Collector to the rescue!

Windows remote management is required (quick CLI config below)
winrm qc

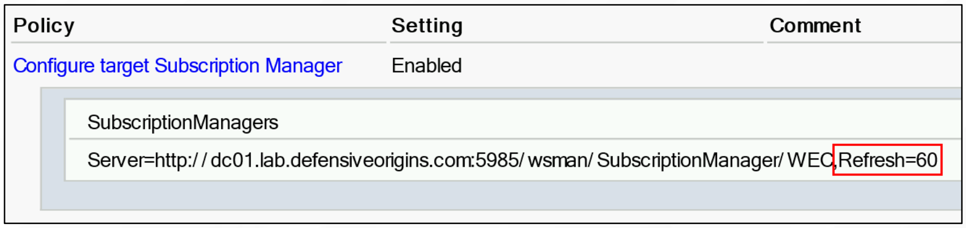
Windows event collector service allows creation and management of event subscriptions
wecutil qc

Remote systems must also support the WS-Management protocol!

https://docs.microsoft.com/en-us/windows/win32/wec/windows-event-collector

Log Forwarding Performance Considerations

- Frequency of connections **(Refresh)**
- Number of subscriptions
- Number of clients
- Operating system of the clients



Policy	Setting	Comment
Configure target Subscription Manager	Enabled	

SubscriptionManagers

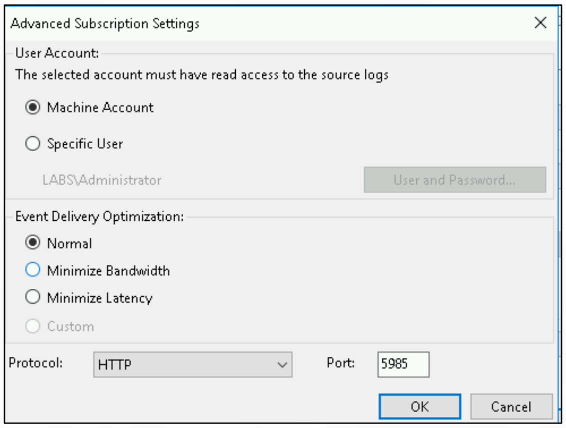
Server=http:/ / dc01.lab.defensiveorigins.com:5985/ wsman/ SubscriptionManager/ WEC,Refresh=60

https://support.microsoft.com/en-us/help/4494356/best-practice-eventlog-forwarding-performance

Log Forwarding Performance Considerations

Delivery Optimization (Subscription Parameter)

- Normal
- Minimize Bandwidth
- Minimize Latency



Advanced Subscription Settings

User Account:

The selected account must have read access to the source logs

● Machine Account

○ Specific User

LABS\Administrator

User and Password...

Event Delivery Optimization:

● Normal

○ Minimize Bandwidth

○ Minimize Latency

○ Custom

Protocol: HTTP

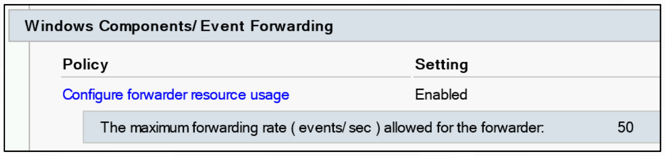
Port: 5985

OK

Cancel

Resource Restrictions

- Events per second

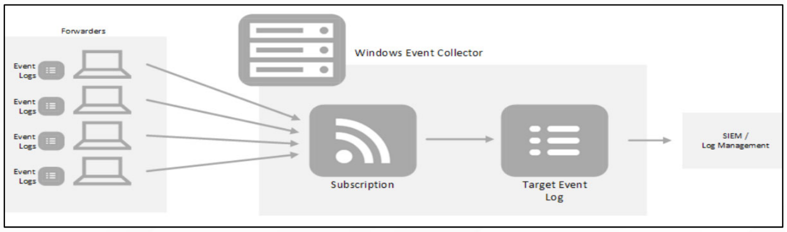


Windows Components/Event Forwarding

Policy	Setting
Configure forwarder resource usage	Enabled
The maximum forwarding rate (events/sec) allowed for the forwarder:	50

https://support.microsoft.com/en-us/help/4494356/best-practice-eventlog-forwarding-performance

Windows Event Collection



Maintains registry stamp of last heartbeat

No more than 10k WEF clients

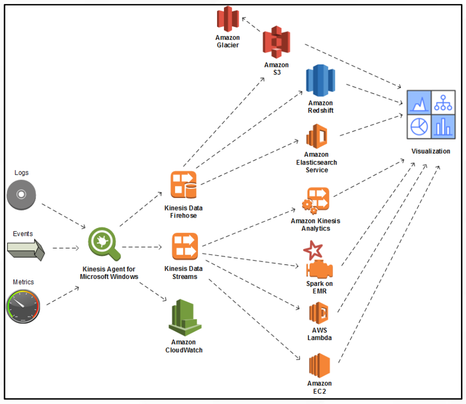
No more than 10k events/sec (remember EMR?)

MapReduce on AWS

Relatively Inexpensive and Auto-Scaling Option for Log Ingests

AWS Kinesis Agents

- Amazing data pipelining for almost anything
  - Video and data streams
  - Metric information
  - Logs of all types



  - **Picture here sourced from AWS Kinesis article below.**

https://aws.amazon.com/blogs/big-data/collect-parse-transform-and-stream-windows-events-logs-and-metrics-using-amazon-kinesis-agent-for-microsoft-windows/

https://docs.aws.amazon.com/kinesis-agent-windows/latest/userguide/directory-source-to-s3-tutorial.html

Windows Event Collection

Three considerations to achieve maximum numbers

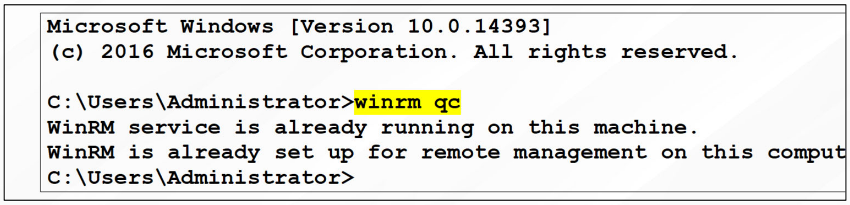
- Disk I/Ops
- Resilient network infrastructure
- Registry size (lifetime subscription numbers below)
  - >1,000 subscriptions event viewer will slow down noticeably
  - >50,000 subscriptions event viewer is no longer an option (wecutil.exe instead)
  - >100,000 subscriptions registry becomes unreadable

Windows Event Collection

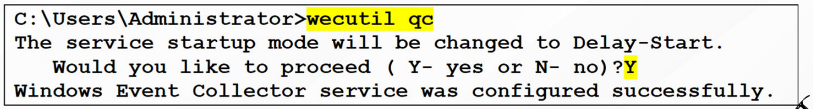
Two commands on the collector.

- **winrm qc** (remote mgmt quick config)
- **wecutil qc** (event collector utility)

(or pre-deploy winrm via GPO)



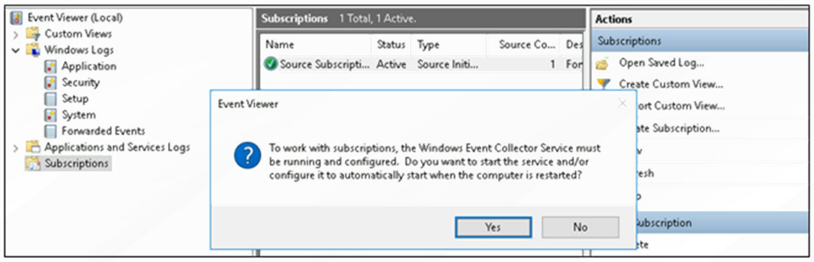
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>winrm qc
WinRM service is already running on this machine.
WinRM is already set up for remote management on this comput
C:\Users\Administrator>
```



```
C:\Users\Administrator>wecutil qc
The service startup mode will be changed to Delay-Start.
   Would you like to proceed ( Y- yes or N- no)?Y
Windows Event Collector service was configured successfully.
```

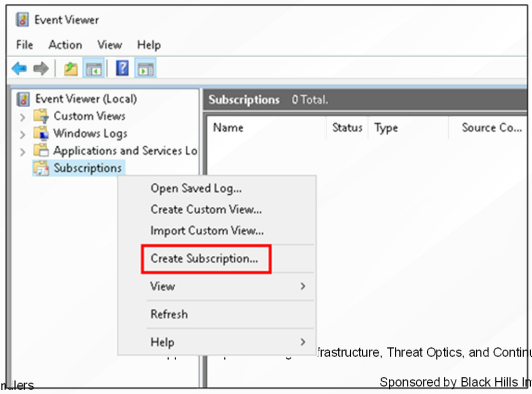
Windows Event Collection

If prompted, as seen here, click **Yes.**



To work with subscriptions, the Windows Event Collector Service must be running and configured. Do you want to start the service and/or configure it to automatically start when the computer is restarted?

From the Event Viewer window, right (alternate) click on **Subscriptions** and click to **Create Subscription...**



Working with Event Subscriptions

Security Insight Baselines – Optics Configurations

Audit Policy – Which events on the domain are we going to capture?

Windows Event Forwarding Configuration

- Baseline WEF config on all systems
- Suspect WEF config on targeted / high risk systems

Subscriptions then define the following:

- Event IDs grouped in meaningful ways (example on next slide) we wish to collect
- Source computer groups

Event Channels

Or, just "channels"

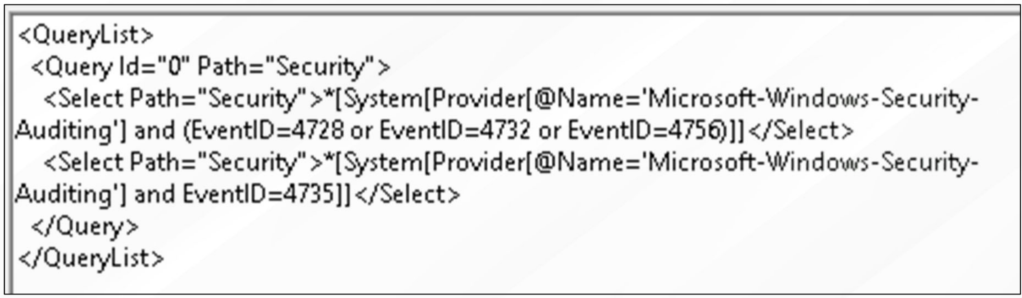
Event channel = log bucket

Working with Event Subscriptions

Grouping event IDs in meaningful ways.

This XML filter, when applied to a subscription:

- Check the security logs for 4728 ***or*** 4732 ***or*** 4756 ***and*** 4735
- Identifies users added to privileged groups
- Called an "XPath query" and can be constructed as a custom event log "view"



```
<QueryList>
  <Query Id="0" Path="Security">
    <Select Path="Security">*[System[Provider[@Name='Microsoft-Windows-Security-
Auditing'] and (EventID=4728 or EventID=4732 or EventID=4756)]]</Select>
    <Select Path="Security">*[System[Provider[@Name='Microsoft-Windows-Security-
Auditing'] and EventID=4735]]</Select>
  </Query>
</QueryList>
```

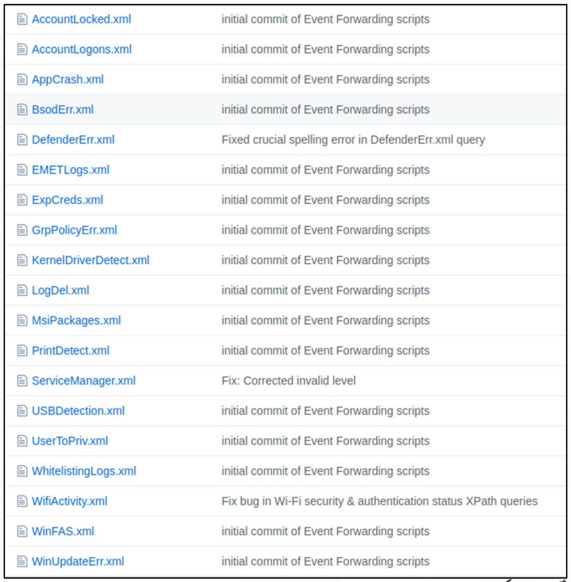
https://github.com/palantir/windows-event-forwarding
https://github.com/nsacyber/Event-Forwarding-Guidance/tree/master/Subscriptions/NT6

Working with Event Subscriptions
Security Insight Baselines

You want event subscription xml templates?
The NSA has your subscriptions XMLs linked below.

- Account Lockouts
- Problems with Defender
- Group Policy Errors
- USB Drives Plugged In
- Users Added to Privileged Groups
- Problems with Windows Updates
- Each of these is just an XPath query
- Palantir's Event Baselines are used for APT lab

This is just a baseline.



AccountLocked.xml	initial commit of Event Forwarding scripts
AccountLogons.xml	initial commit of Event Forwarding scripts
AppCrash.xml	initial commit of Event Forwarding scripts
BsodErr.xml	initial commit of Event Forwarding scripts
DefenderErr.xml	Fixed crucial spelling error in DefenderErr.xml query
EMETLogs.xml	initial commit of Event Forwarding scripts
ExpCreds.xml	initial commit of Event Forwarding scripts
GrpPolicyErr.xml	initial commit of Event Forwarding scripts
KernelDriverDetect.xml	initial commit of Event Forwarding scripts
LogDel.xml	initial commit of Event Forwarding scripts
MsiPackages.xml	initial commit of Event Forwarding scripts
PrintDetect.xml	initial commit of Event Forwarding scripts
ServiceManager.xml	Fix: Corrected invalid level
USBDetection.xml	initial commit of Event Forwarding scripts
UserToPriv.xml	initial commit of Event Forwarding scripts
WhitelistingLogs.xml	initial commit of Event Forwarding scripts
WifiActivity.xml	Fix bug in Wi-Fi security & authentication status XPath queries
WinFAS.xml	initial commit of Event Forwarding scripts
WinUpdateErr.xml	initial commit of Event Forwarding scripts

Working with Event Subscriptions
Audit Policy

Microsoft recommends the following:

- Anti-Malware
- Process Creation
- Registry Changes
- OS Startup / Shutdown
- Service Installs
- CA Audit Events
- User Profile Events
- Service Start / Failure
- Network Share Events (*sans* IPC$ events)
- RDS Session Events
- EMET Events

...and so much more...***as a baseline***...plus the "suspect system/server" baselines

A Few Important Event IDs

4624 and 4634 (Logon / Logoff)
4662 (ACL'd object access - Audit req.)
4688 (process launch and usage)
4698 and 4702 (tasks + XML)
4740 and 4625 (Acct Lockout + Src IP)
5152, 5154, 5156, 5157 (FW - Noisy)
4648, 4672, 4673 (Special Privileges)
4769, 4771 (Kerberoasting)
5140 with \\*\IPC$ and so many more….

https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings
https://techcommunity.microsoft.com/t5/microsoft-security-baselines/security-baseline-sept2019update-for-windows-10-v1903-and/ba-p/890940

Working with Event Subscriptions

Audit Policy

You must have Audit Process Creation auditing enabled
You must enable the policy setting:

- Include command line in process creation events

> "When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings." (cit. *MSFT, see links)

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing
https://github.com/MotiBa/Sysmon/
https://github.com/SwiftOnSecurity/sysmon-config
https://www.malwarearchaeology.com/cheat-sheets
https://adsecurity.org/?p=3458
http://www.stuffithoughtiknew.com/2019/02/detecting-bloodhound.html

Working with Event Subscriptions

Audit Policy Baselines

Y

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing
https://github.com/MotiBa/Sysmon/
https://github.com/SwiftOnSecurity/sysmon-config
https://www.malwarearchaeology.com/cheat-sheets
https://adsecurity.org/?p=3458
http://www.stuffithoughtiknew.com/2019/02/detecting-bloodhound.html

RECAP.

Sysmon. Enable WEC. Deploy WEF. Event Subscriptions. Configure Auditing.

Enable Windows Collection

- Plan appropriately for scaling

Deploy Windows Event Forwarding configuration

- Use GPO to configure security privileges for event log reading by network service
- And to define the Windows Event Collector's destination URL

Configure Event Subscriptions

- Group event IDs in meaningful ways and create a subscription

Plan, configure, and deploy Audit Policies

- This is critical to the success of this project
- You cannot see that which you do not audit