

AlienVault Unified Security Management™ Solution

Complete. Simple. Affordable

SQL Server Audit and USM

**Table of Contents**

SQL Server Audit and USM 1

1. INTRODUCTION 4

2. Configuring SQL server audit. 4

3. Installing NXlog 5

4. Apply MSSQLServer Plugin 7

5. To apply plugin to asset 8

6. Creating a SQL view 10

# INTRODUCTION

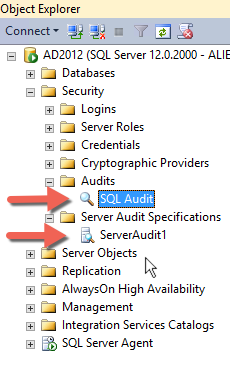
This document how to get SQL server audit event data from the Windows Event logs to AlienVault USM. To get the SQL audit events from Windows the NXlog Community Edition agent needs to be installed on the SQL server. The version of Windows and SQL this has been developed for is Windows 20012, with SQL 2014, however this may still work on earlier version of SQL.

# Configuring SQL server audit.

There are several different audit methods in SQL (C2, Common Criteria, Change Data Capture, and SQL Server Audit), but for this document we will be focusing on using SQL Server Audit to bring the audit trail from the Windows Event Logs to USM.

First you need to create an Audit. Make sure to specify Audit Destination to be the Application Log or the Security Log.

Then you need to create an Server Audit Specification, and a Database Audit Specification, both which will be tied to the Audit.



For more information on setting up SQL Server Audit see:

<https://msdn.microsoft.com/en-us/library/cc280386.aspx>

# Installing NXlog

To get the audit events from the Windows Event log to USM we will leverage NXlog to forward the events to the USM syslog server.

On the SQL server download and install NXlog Community Edition

<http://nxlog.org/products/nxlog-community-edition/download>

Download the Windows agent and then modify the nxlog.conf file located under %SYSTEMROOT%:\Program Files (x86)\nxlog\conf. So it looks like the following, make sure to modify the Host entry with your USM Sensor IP address.

|  |
| --- |
| ## Please set the ROOT to the folder your nxlog was installed into,  ## otherwise it will not start.  #define ROOT C:\Program Files\nxlog  define ROOT C:\Program Files (x86)\nxlog  Moduledir %ROOT%\modules  CacheDir %ROOT%\data  Pidfile %ROOT%\data\nxlog.pid  SpoolDir %ROOT%\data  LogFile %ROOT%\data\nxlog.log    <Extension charconv>  Module xm\_charconv  AutodetectCharsets utf-8, euc-jp, utf-16, utf-32, iso8859-2  </Extension>    <Extension syslog>  Module xm\_syslog  </Extension>    <Input in>  Module im\_msvistalog  # For windows 2003 and earlier use the following:  # Module im\_mseventlog    # We only forward relevant messages from the SQL Audit  Exec if not ($EventID == 33205) drop();  </Input>    <Output out>  Module om\_udp  Host 192.168.88.100  Port 514  Exec convert\_fields("AUTO", "utf-8");  Exec to\_syslog\_bsd();  </Output>    <Route 1>  Path in => out  </Route> |

After saving the nxlog.conf restart the nxlog service. The NXlog service will now forward all events with EventID 33205 to the USM syslog server (sensor).

# Apply MSSQLServer Plugin

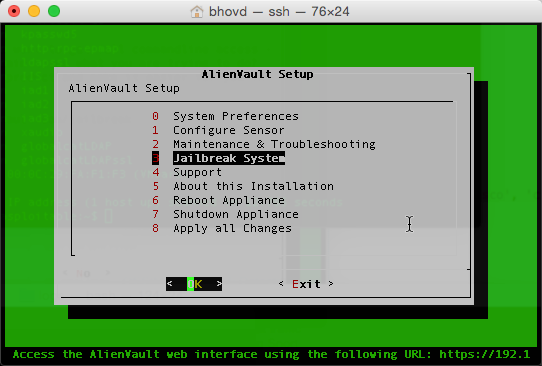
For USM to normalize the Audit events there needs to be a plugin that can extract the data we expect to see in the database. To Download the latest plugin go to:

<https://github.com/hovdb/Alien-Plugins/tree/master/SQL2014>

There will be a mssqlserver.cfg and a mssqlserver.sql file which you need to download.

copy the files over to /etc/ossim/agent/plugins on the USM sensor. Once the files are copied over the SQL file needs to be run to populate the plugins tables.

To insert the updates from the SQL file you copied over. Select option 3 Jailbreak System, and then type:

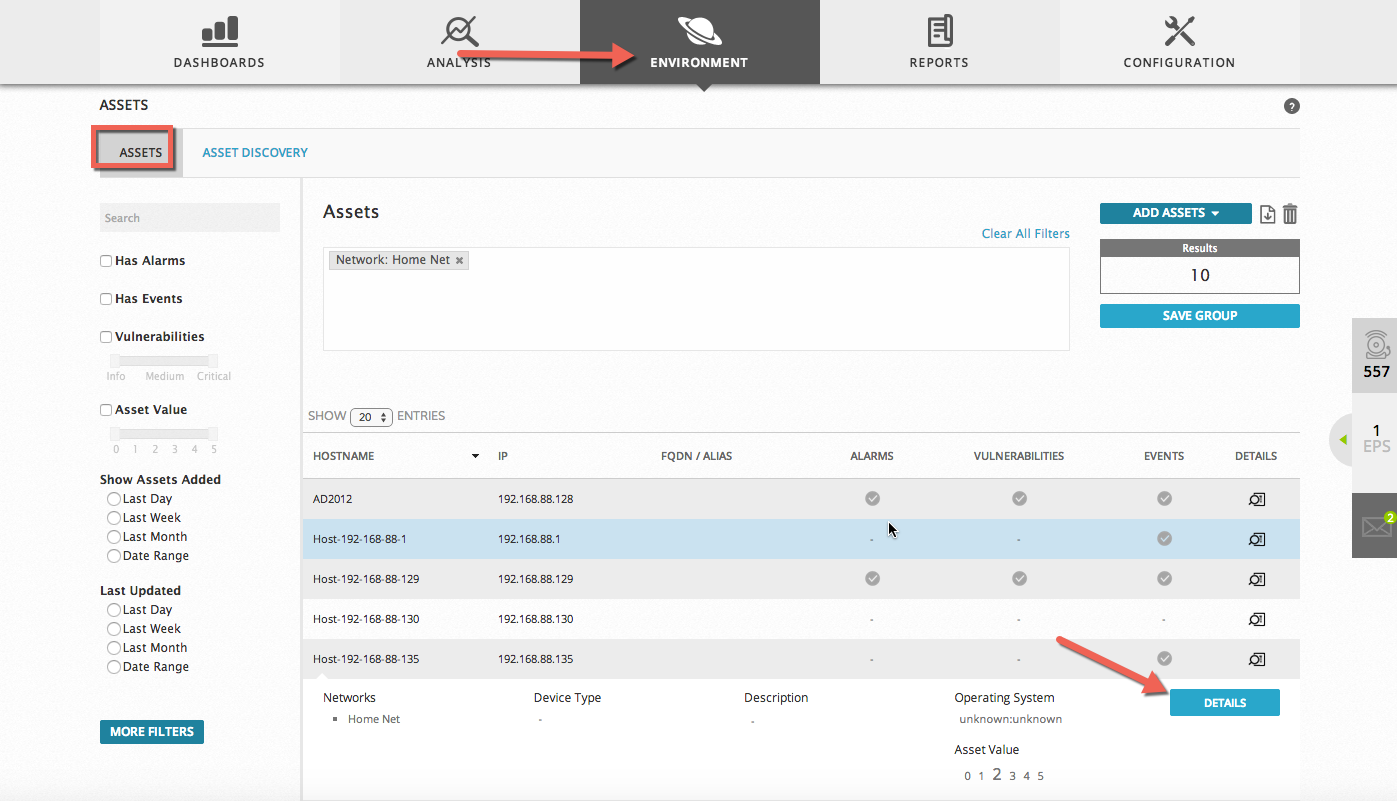


|  |
| --- |
| cat mssqlserver.sql | ossim-db |

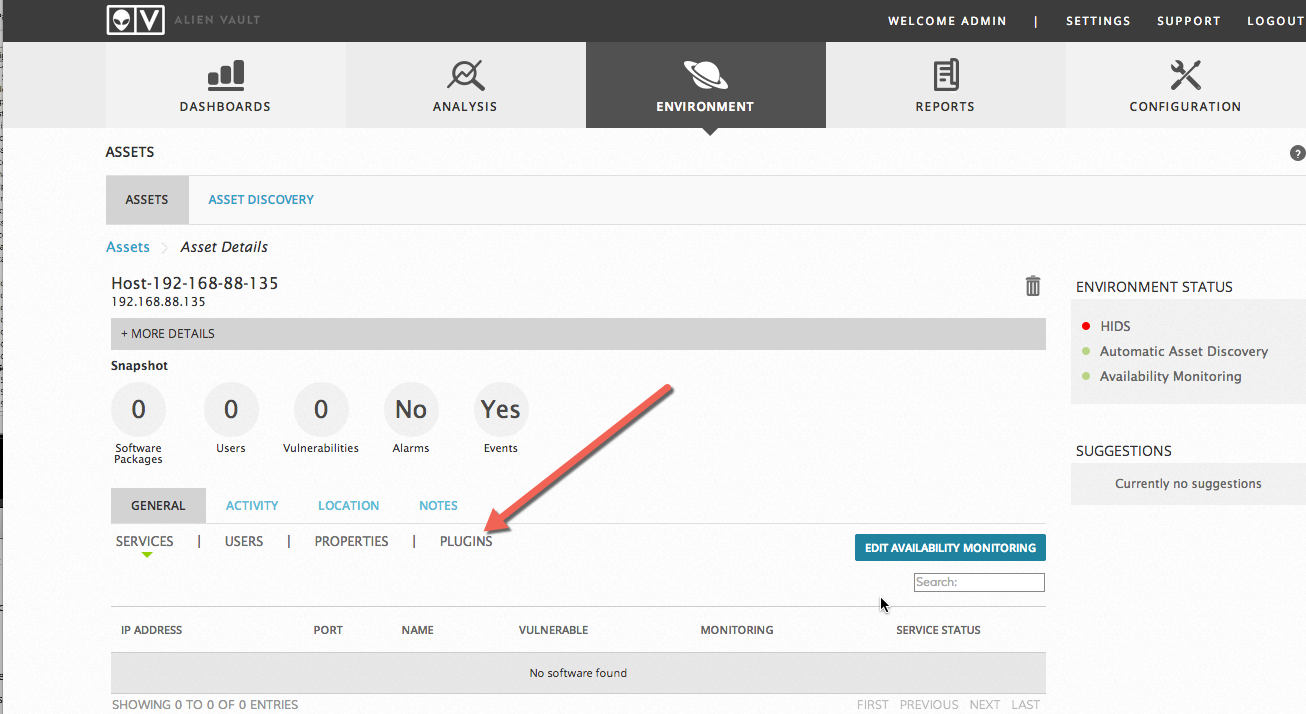
This will insert plugin information required in SQL.

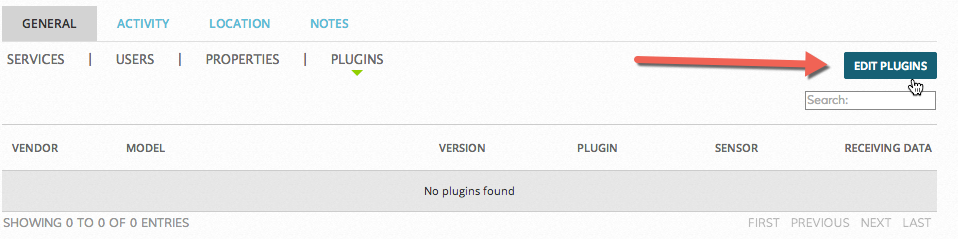
# To apply plugin to asset

To apply a plugin for an asset. Navigate to ENVIRONMENT>ASSETS. Once you locate the asset you want to have the plugin click on DETAILS and it will display the GENERAL tab of the asset.

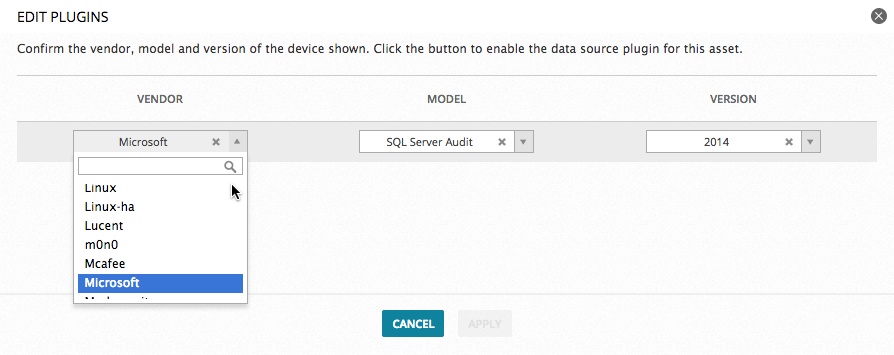


Click on PLUGINS >EDIT PLUGINS





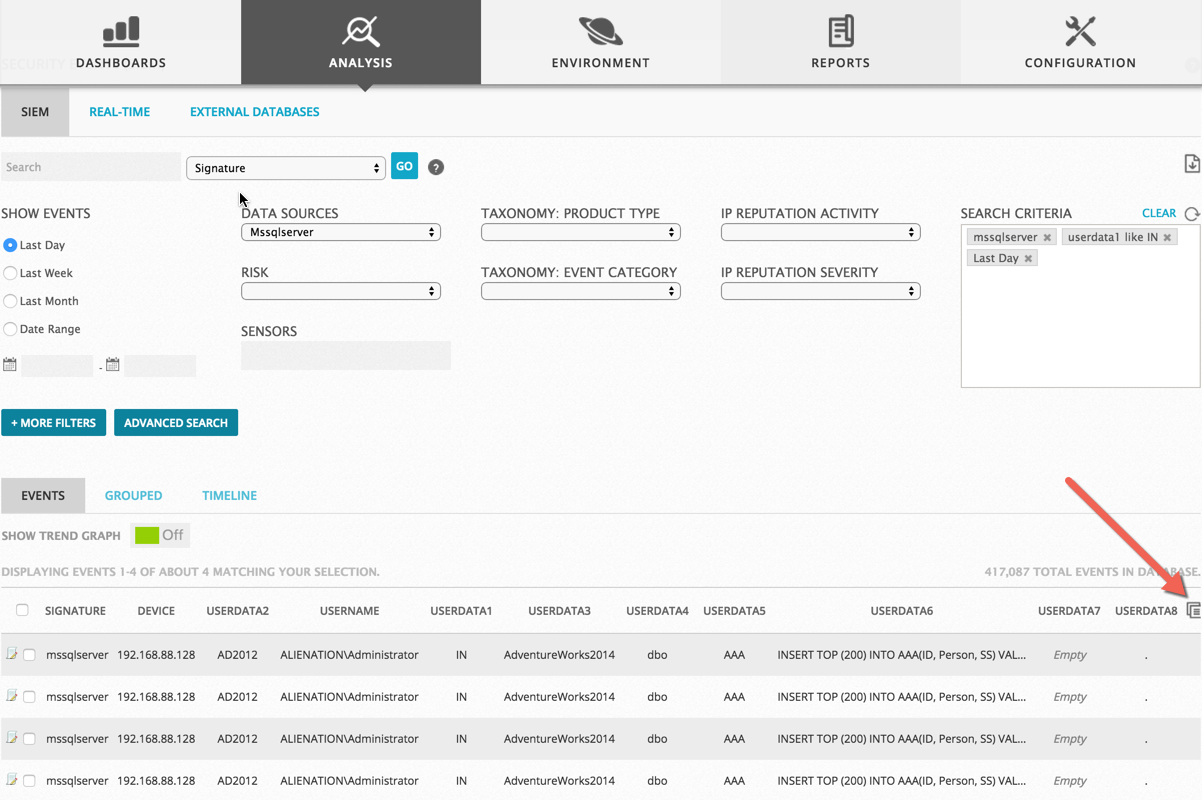
From the plugins dropdown select the plugin, model and version and click apply.



If everything is configured correctly you should start seeing events in your SIEM from the mssqlserver datasource.

# Creating a SQL view

To better view the SQL events you may create a custom view in the SIEM. First select Mssqlserver from the Data Sources drop down menu. Then click the Predefined views icon above the grid, and then click the Create New View.



Add the following columns displayed in the image, and click Create.

