



Crafting Zenoss Core users for events and zProperties

February 2009

Jane Curry

Skills 1st Ltd

www.skills-1st.co.uk

DRAFT

Jane Curry
Skills 1st Ltd
2 Cedar Chase
Taplow
Maidenhead
SL6 0EU
01628 782565

jane.curry@skills-1st.co.uk

Synopsis

Zenoss comes effectively with three types of user built-in – Manager, ZenManager and ZenUser. Manager can do anything; ZenManager seems to be able to do many Zenoss things; ZenUser is fairly restricted.

The requirement is for operational users who largely needs access to events.

- They should be able to Acknowledge and/or Close events from some devices (but not others).
- They should be able to see the history table of the events database for these same devices and be able to Undelete events, if necessary
- They must also be able to add comments to the Log tab of an event's detailed view.
- In addition, they must **not** be able to see Zenoss screens that show SNMP community names or Windows Usernames / passwords (zProperties screens).

By default, the ZenUser role does not get access to a generic Event Console but they can see zProperties for all devices; however it is possible to modify the Zenoss menus to show a user's specific Event Views and modify access permissions to hide the zProperties page of a device.

The Zenoss Professional chargeable offering includes the Role-Based Access Control zenpack; this paper demonstrates how to achieve limited control simply using Zenoss Core. Note that there is some documentation of the Role-Based Access Control in the 2.3 version of the Zenoss Administration Guide (Chapter 6).

This paper was written based on stack-built Zenoss Core 2.3.2 on Open SuSE 10.3.

Table of Contents

1 Viewing Events.....	4
2 Acknowledging / Closing / Undeleting events.....	9
3 Adding to the Log details of an event.....	11
4 Modifying Zenoss menus to show a user's Event Views.....	15
5 What about controlling zProperties?.....	16
6 Conclusions.....	18
Acknowledgements.....	18

1 Viewing Events

There are three ways of viewing events through the Zenoss web interface:

- A full Event Console from the left-hand menu
- The Events tab from the main page of a specific device
- An Event View configured for a specific user

By default, only a user with the Manager role has an unrestricted Event Console. A user with the ZenManager role sees the Event Console in the left-hand menu but does not have unrestricted authority to Acknowledge or Close events; neither are they able to add to the Log tab of an event's detailed data. A user with the ZenUser role has no left-hand Event Console menu.

Device Id	IP	Class	Prod State	Event Summary
adsl2.skills-1st.co.uk	10.0.0.254	/Discovered	Production	0/0 0/0
bino.skills-1st.co.uk	10.0.0.121	/bino_vms	Production	0/0 0/0
deodar-mgt.skills-1st.co.uk	10.0.0.96	/Ping	Production	0/0 0/0
deodar.skills-1st.co.uk	10.0.0.95	/VMs	Production	0/0 0/0
group-1-a1.class.example.org	172.31.1.3	/Server/Linux	Production	0/1 0/0
group-1-b1.class.example.org	172.31.1.19	/Server/Windows	Production	0/1 0/2
group-100-b1.class.example.org	172.31.100.19	/Ping	Production	0/0 0/0
group-100-b2.class.example.org	172.31.100.20	/Ping	Production	0/0 0/0
group-100-c1.class.example.org	172.31.100.34	/Ping	Production	0/0 0/0
group-100-c2.class.example.org	172.31.100.35	/Ping	Production	0/0 0/0
group-100-c3.class.example.org	172.31.100.36	/Ping	Production	0/0 0/0
group-100-r1.class.example.org	10.191.100.4	/VMs	Production	0/0 0/1
group-100-r2.class.example.org	172.31.100.17	/VMs	Production	0/0 1/1
group-100-r3.class.example.org	172.31.100.2	/VMs	Production	0/0 1/1
group-100-s1.class.example.org	172.31.100.37	/Discovered	Production	0/0 1/1
group-100-s2.class.example.org	172.31.100.21	/Discovered	Production	0/0 1/1
hp7410.skills-1st.co.uk	10.0.0.97	/Printer	Pre-Production	0/0 0/1
server.class.example.org	10.191.101.1	/VMs	Production	0/0 0/0
tile.skills-1st.co.uk	10.0.0.98	/Ping	Production	0/0 0/0
zen232.class.example.org	172.16.223.232	/VMs	Production	0/0 0/0
zenoss.skills-1st.co.uk	10.0.0.131	/Discovered	Production	0/0 0/0

Figure 1: Default left-hand menu for user with ZenUser role - note no Event Console

A user with the ZenUser role can access the Events tab of any discovered device (as can the other two roles); however they cannot Acknowledge or Close events.

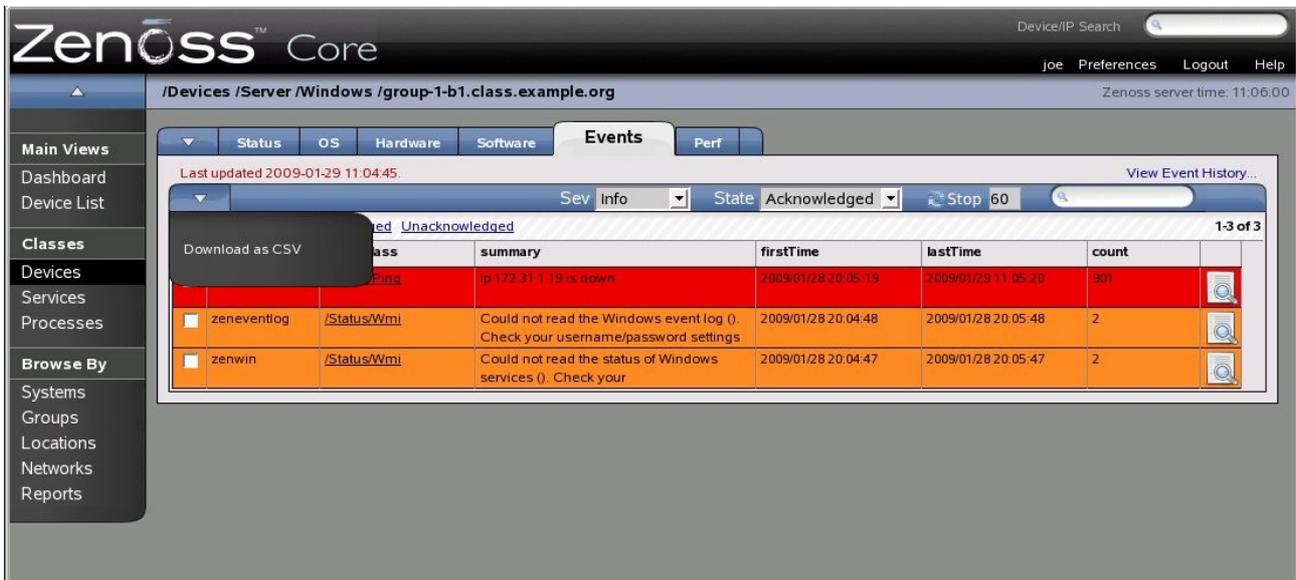


Figure 2: Events for a specific device for a user with ZenUser role

Note that although the Events tab can be accessed for any device, the table drop-down menu is very restricted – no Acknowledge or Move to History options.

In addition, such a user is unable to add to the Log tab of an event's detailed data.



Figure 3: Log tab of the detailed data of an event for a user with default ZenUser / ZenManager role

One way to provide an Event Console for a user with ZenUser role is to create an Event View for them – this would need to be done by a user with Manager role. Start from the left-hand Settings menu and select the Users tab. A user definition includes the role (or roles) of that user.

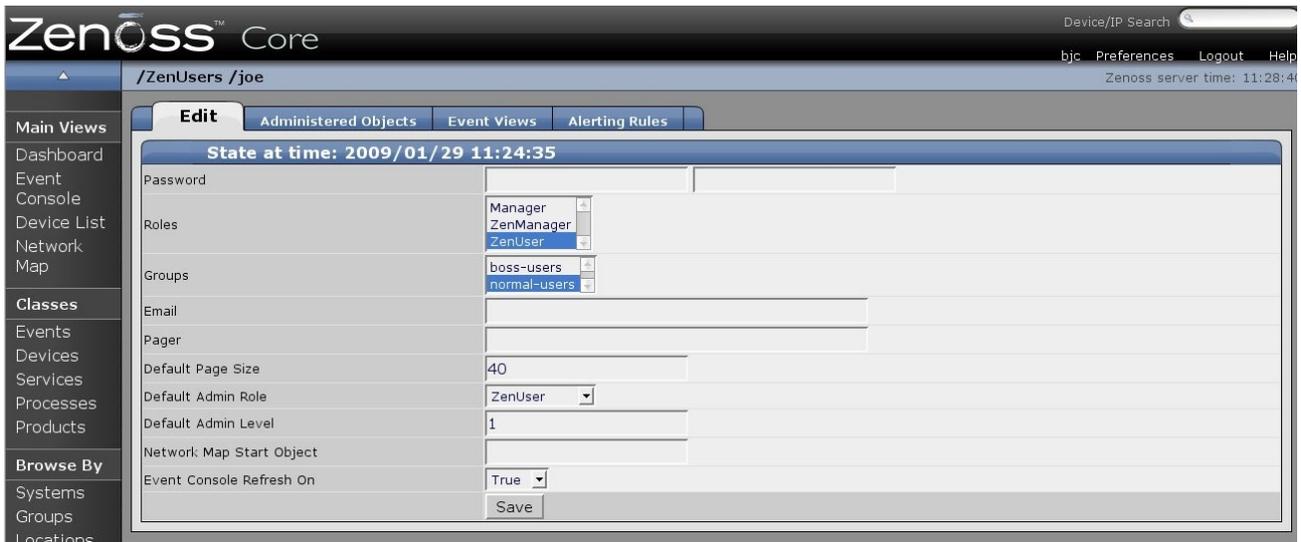


Figure 4: Editing base properties for a user

The Admin *Level* is defined in the Zenoss Administration Guide as

“currently merely ways to categorize and group users. In the future there may be more attributes that would be assignable per group/role. For now it is just a way to categorize and classify users.”

The defined levels are Administrator, Engineer, Analyst and Tester. This Admin Level is nothing to do with user groups.

Any user can have one or more Event Views created for them, using the Event Views tab.



Figure 5: Configuring an Event View

Note that the default type of Event View draws data from the status table of the events database – if a user needs to see cleared events in the history table then a second Event View must be created to achieve that.

The filter drop-down can be used to specify a comprehensive list of attributes, including device, device class, event class, location, severity, etc. If multiple filters are specified then they are logically ANDed. If no filters are specified, all events are included.

Fields displayed in the Event Console can be controlled; although the *Add Fields* link always appears greyed-out, extra fields **can** be added by clicking on this link.

Note that the user themselves will have authority to configure any of their event views but they will not have authority to create new Event Views.

Although a user with the ZenUser role does not see the left-hand *Settings* menu, they can access their own Event Views from the *Preferences* tab at the top right of the Zenoss console (next to the user name). It is also possible to customise the Zenoss left-hand menu to show a user's specific Event Views (see Chapter 4).

Unless limited by a filter, an Event View will show all events for all devices although the user will not be able to interact with those events.

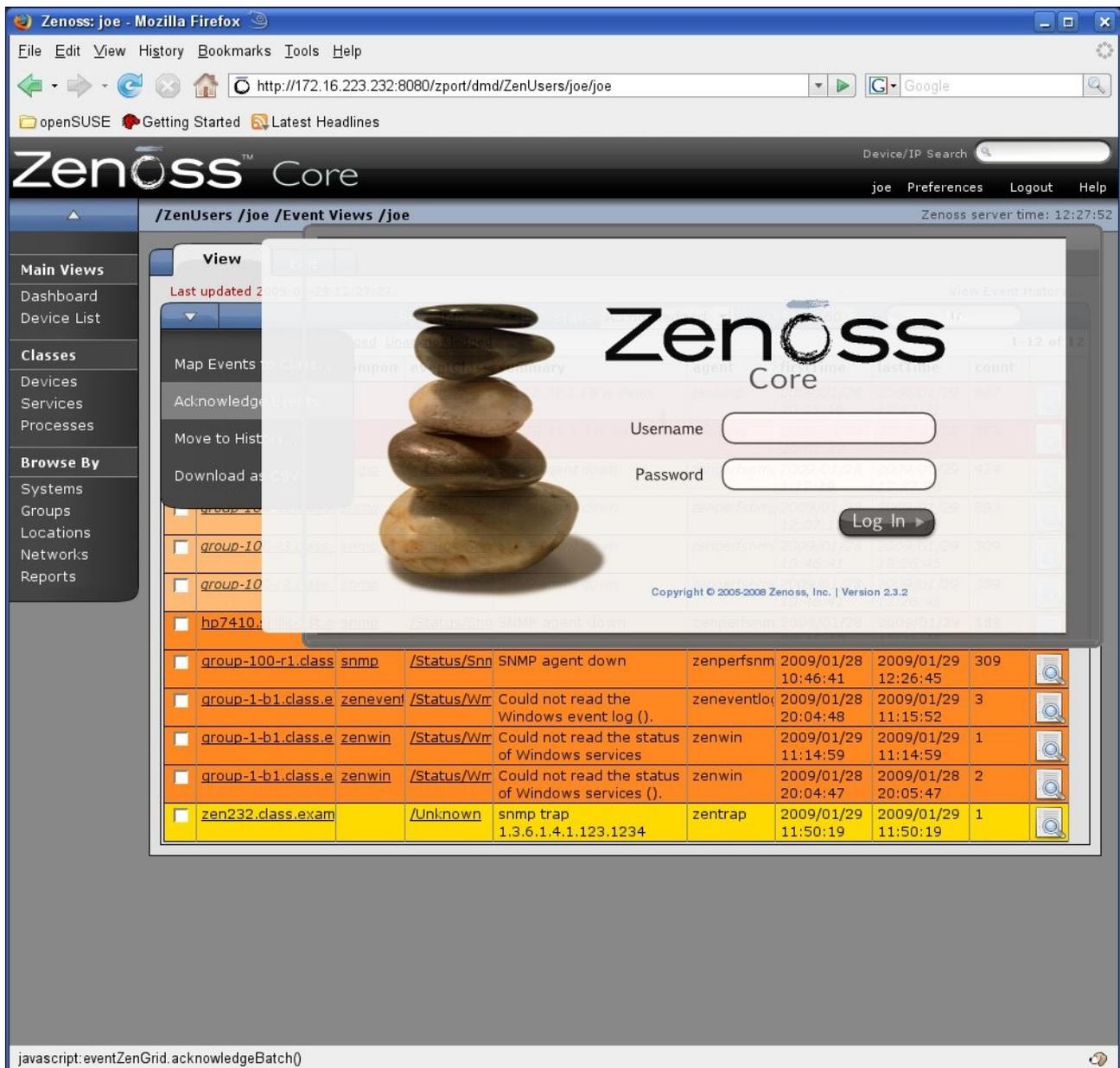


Figure 6: Attempting to Acknowledge event in an Event View for user with ZenUser role

Although the Event View table menu drop-down will show options to Acknowledge and Move to History, a user with the ZenUser role does **not** have authority to interact with these events and will receive a flashing Zenoss login screen for a few seconds.

Note that if user groups are created and a user is placed in a user group, then an Event View is **not** inherited from a user group – Event Views must be created for individual users..

Also note that user groups are nothing whatever to do with device groups (the Groups option in the left-hand menu) .

So, if a user does not have full Manager privilege and needs to see all events in a single Event Console, they need to have at least one individual Event View setup for them. If they only need to access events for specific devices, through the event tab of a

device page, no Event View is necessary (and may provide a back-door for users to see events that they would otherwise be unauthorised to see).

2 Acknowledging / Closing / Undeleting events

Thus far, a user with the ZenUser role is unable to Acknowledge events, Move them to History, or add comments to the Log tab of an event's detailed data.

If the requirement is only to be able to Acknowledge or Clear events from specific devices **and** there is no requirement to annotate the Log, this can be achieved using the *Administered Objects* tab for a user (which requires full Manager privilege to modify).



Figure 7: Setting up Administered Objects for a user

Specific devices, device classes, systems, (device) groups and locations can be chosen – having selected the type, a second window appears with a drop-down to select the particular instance of that type.

To be able to modify an event from a device then either the specific device or the relevant device class needs selecting **and** the role needs changing from ZenUser to Manager. Note that selecting systems, locations or groups that include a device does **not** have the desired effect.

Note that granting the Manager role on a device gives much more power than simply modifying events; one consequence is that it provides access to the *Edit* tab of a device so almost any reconfiguration is possible. It also ensures that a user has access to the zProperties of a device, including edit capability.



Figure 8: Administered objects for user joe with different roles

In Figure 8 above, user joe is given the Manager role just for the specific device zen232.class.example.org . The result is that in the Events tab of the device zen232.class.example.org, the table drop-down menu shows Acknowledge and Move to History options and these options are effective (no flashing Zenoss login screen). Similar, the *View Event History* link is active and, from the History view, events from that specific device can be Undeleted.

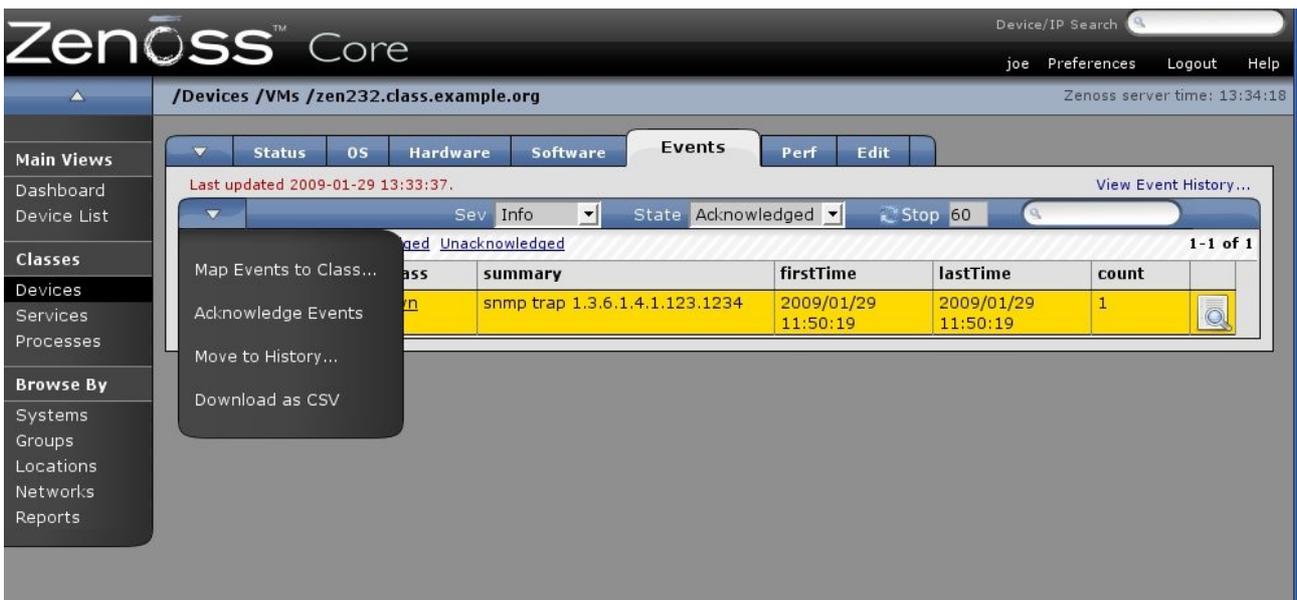


Figure 9: Drop-down menu options for device event with Manager role

In contrast, any other device for which joe only has the ZenUser role, the drop-down menu would only show the *Download as CSV* option as shown in Figure 2.

Note that if joe has an Event View configured for him, although the Acknowledge and Move to History menus **are** available there, they will **not** be effective – even for zen232.class.example.org. He will receive the flashing Zenoss login screen as shown in Figure 6.

Note that if a user **group** is created, then Administered Objects and their roles can be associated with a user group and any user members of that group **will** inherit these characteristics.

It is also possible to make the Administered Object association between device and user from the main page of a device. Select the table drop-down *More* menu followed by *Administration*. Add users and roles to the *Administrators* section.

Thus far, we have a method for Acknowledging / Closing / Undeleting events from specific devices provided we can accept that this privilege extends further than the events subsystem. Changing roles on Administered Objects does **not** affect the ability to add to the Log tab of an event's detailed page.

3 Adding to the Log details of an event

When an event is Acknowledged, Closed or Undeleted, the Log tab of the detailed event is automatically updated.



Date	User	Text
2009/01/29 13:33:33.000	joe	Undeleted by user
2009/01/29 13:33:16.000	joe	Deleted by user
2009/01/29 13:26:31.000	bjc	Undeleted by user
2009/01/29 13:25:44.000	bjc	Deleted by user
2009/01/29 12:56:35.000	joe	Undeleted by user
2009/01/29 12:56:16.000	joe	Deleted by user

Figure 10: Records in the Log tab of an event

Any user that does not have full Manager privilege is unable to add to this log though all users can see it. Changing the privilege on a device to Manager does not affect log update capability.

To allow users to update the Log tab, permissions can be changed for a role. Use a web browser to connect to the Zenoss server, port 8080 (by default), and access `zport/manage_access`. You will need to logon as a user with full Manager rights (user admin, password zenoss is the default). This is a Zope interface (Zope is the applications framework that Zenoss is built in) and provides a way to adjust the privileges of the configured roles (and, indeed, create new roles).

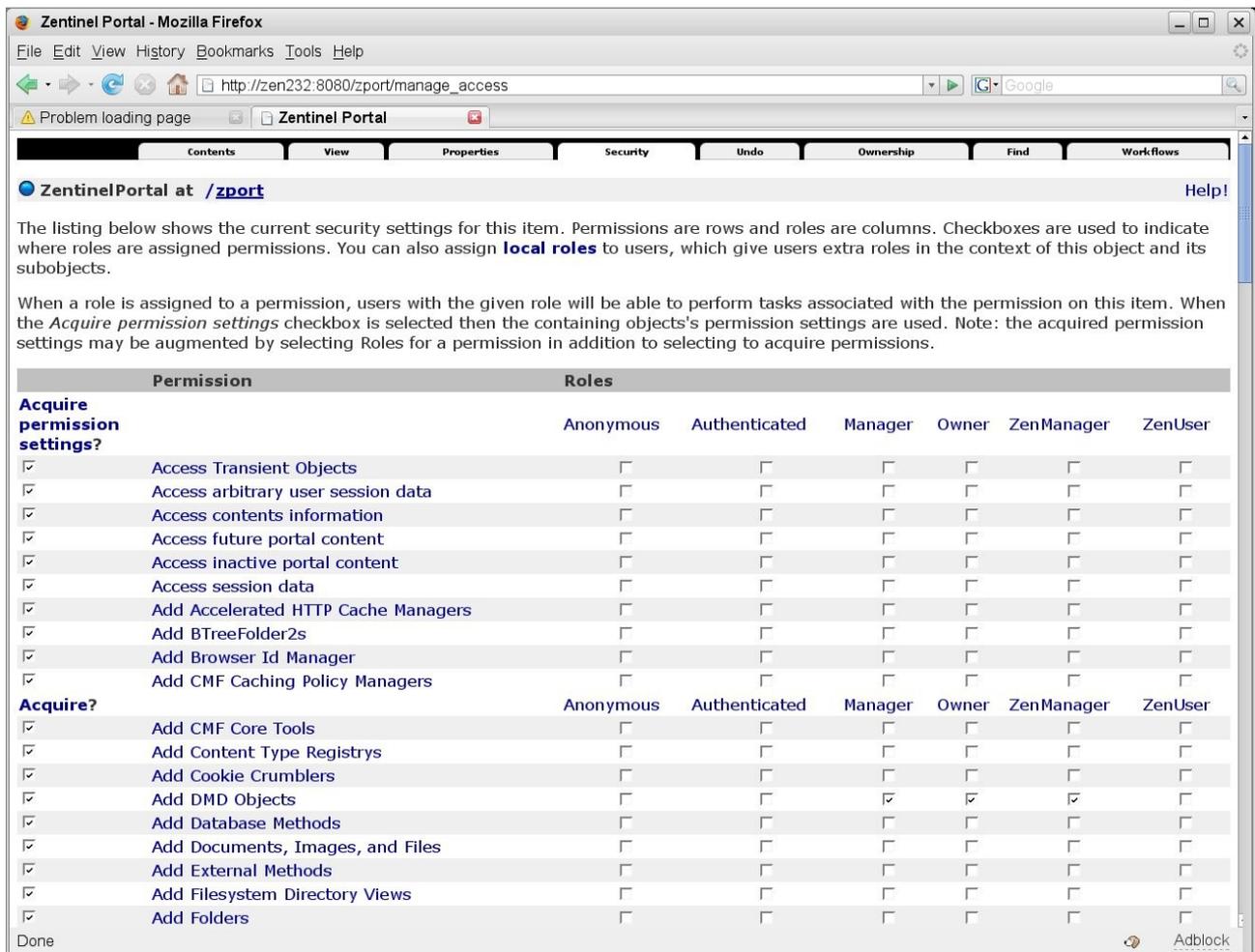


Figure 11: Accessing the Zope security options

To provide edit access to the Log tab, the *Manage Events* permission must be granted. Don't forget to click the *Save Changes* button at the bottom of the screen. Changes take effect immediately – even to logged on users.

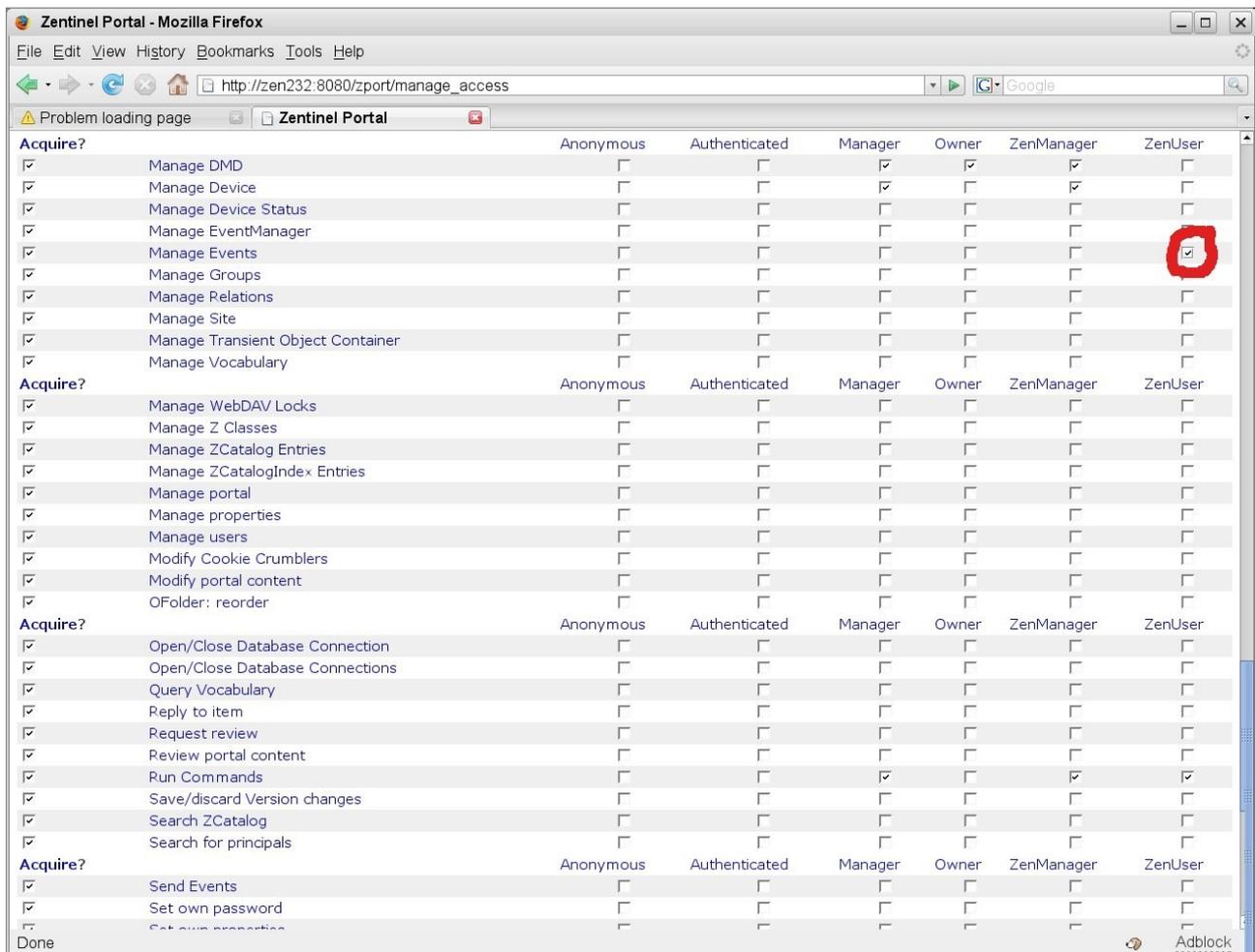


Figure 12: Adding the Manage Events permission to the ZenUser role

This permission changes effects, both for Event View Consoles and for Event tabs for devices. Assuming that user joe is still setup with the ZenUser role but has been given the Administered Object zen232.class.example.org with the Manager role, the effect on Event View Consoles is:

- joe still doesn't have an Event Console in the left-hand menu
- joe's Event View for the status table of the events database now gives him the ability to Acknowledge and / or Clear any events from any devices (instead of getting the flashing Zenoss login screen)
- joe's Event View for the history table of the events database does **not** give him permission to undelete events – he still gets the flashing Zenoss login screen
- joe can see and edit the Log tab of any event from any device, whether the event is in the status table or the history table

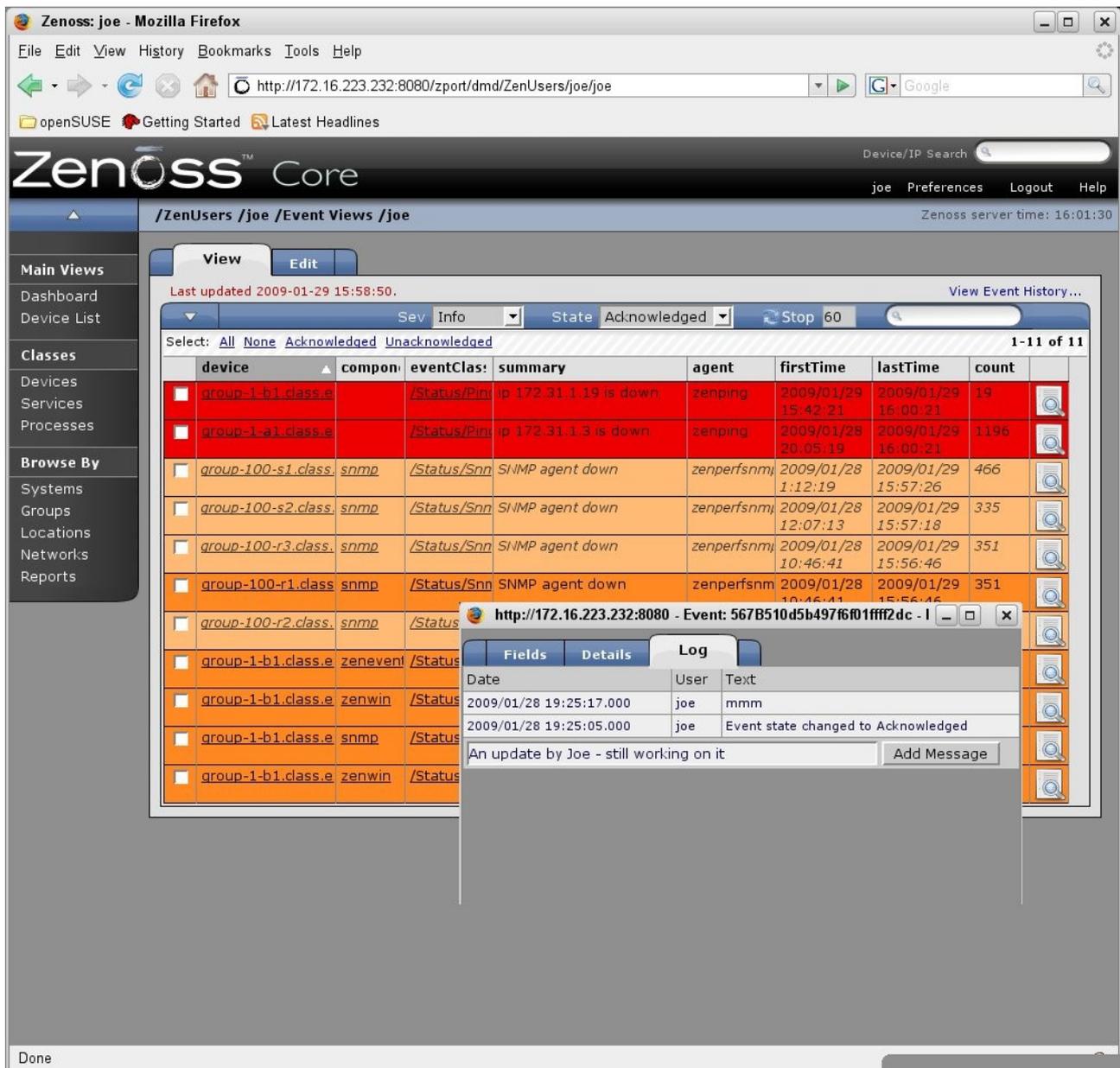


Figure 13: Updating the Log tab for an event in a user's Event View

For events viewed through the Events tab of a device page:

- For devices with the ZenUser role, there is still no Acknowledge or Move to History options in the Event Console drop-down menu, and no Undelete option on the history view menus.
- The Log tab can be seen and edited for any events, regardless of the role for the device, in both status and history tables.
- For devices with the Manager role, Acknowledge, Move to History and Undelete menus are available and active, as they were before changing the Manage Events permission

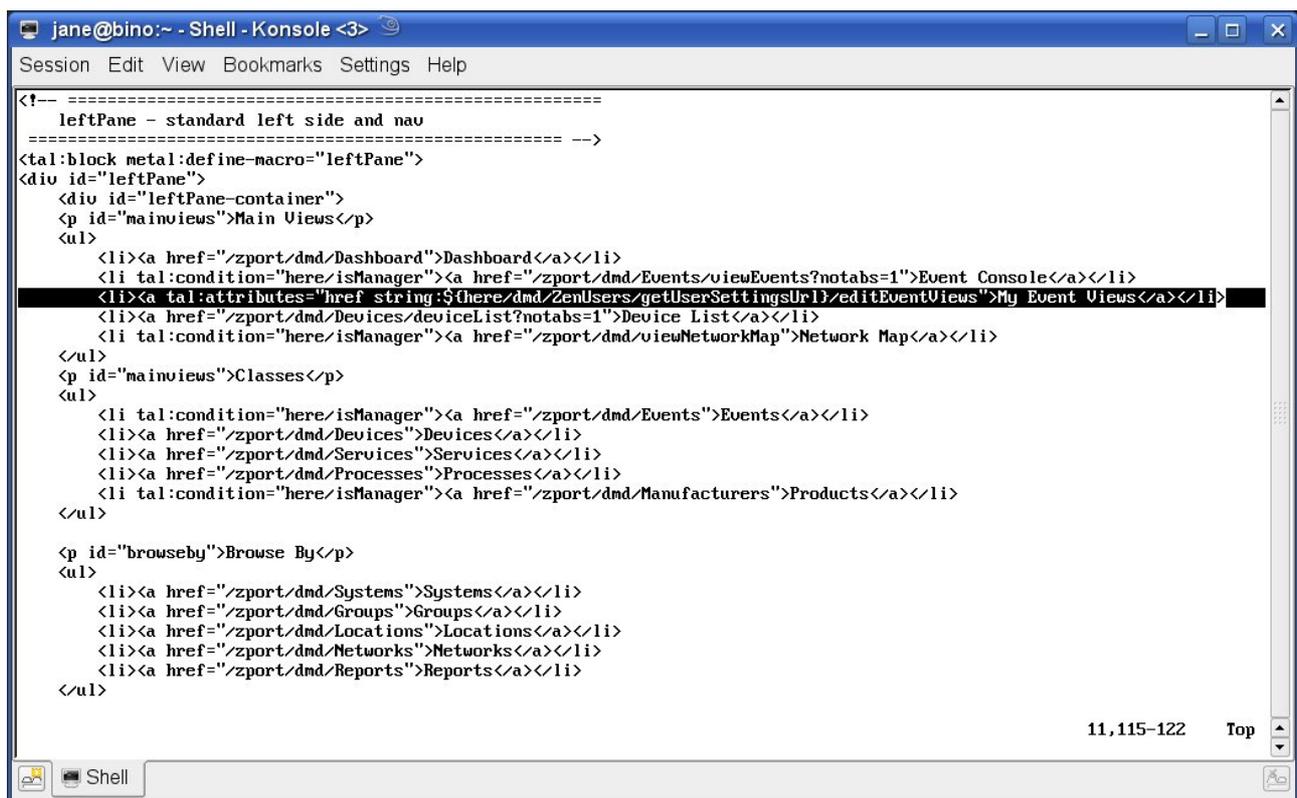
So, if you need to be able to modify the Log tab for an event to provide problem management updates, you have to set the Manage Event permission on a role that

those users have. If those users have customised Event Views for the status table of the events database, they now have the ability to Acknowledge and Close events from **any** device though they have **no** ability to Undelete any events from a customised history Event View.

If these users do not have customised Event Views, but do have the Manager role assigned for some devices through Administered Objects, then for those devices only, they can Acknowledge and Close events in the status table of the events database, they can Undelete events from the history table and they can append to the Log tab of events from **all** devices. There seems to be no way to restrict Log updates to specific devices.

4 Modifying Zenoss menus to show a user's Event Views

It is possible to modify the menus presented by Zenoss. The left-hand menu is defined by the file `$ZENHOME/Products/ZenModel/skins/zenmodel/leftPane.pt`. This file can be modified – but make sure you take a backup first!



```

<!-- =====
leftPane - standard left side and nav
===== -->
<tal:block metal:define-macro="leftPane">
<div id="leftPane">
  <div id="leftPane-container">
    <p id="mainviews">Main Views</p>
    <ul>
      <li><a href="/zport/dmd/Dashboard">Dashboard</a></li>
      <li tal:condition="here/isManager"><a href="/zport/dmd/Events/viewEvents?notabs=1">Event Console</a></li>
      <li><a tal:attributes="href string:${here/dmd/ZenUsers/getUserSettingsUrl}/editEventViews">My Event Views</a></li>
      <li><a href="/zport/dmd/Devices/devicelist?notabs=1">Device List</a></li>
      <li tal:condition="here/isManager"><a href="/zport/dmd/viewNetworkMap">Network Map</a></li>
    </ul>
    <p id="mainviews">Classes</p>
    <ul>
      <li tal:condition="here/isManager"><a href="/zport/dmd/Events">Events</a></li>
      <li><a href="/zport/dmd/Devices">Devices</a></li>
      <li><a href="/zport/dmd/Services">Services</a></li>
      <li><a href="/zport/dmd/Processes">Processes</a></li>
      <li tal:condition="here/isManager"><a href="/zport/dmd/Manufacturers">Products</a></li>
    </ul>
    <p id="browseby">Browse By</p>
    <ul>
      <li><a href="/zport/dmd/Systems">Systems</a></li>
      <li><a href="/zport/dmd/Groups">Groups</a></li>
      <li><a href="/zport/dmd/Locations">Locations</a></li>
      <li><a href="/zport/dmd/Networks">Networks</a></li>
      <li><a href="/zport/dmd/Reports">Reports</a></li>
    </ul>
  </div>
</div>

```

Figure 14: `$ZENHOME/Products/ZenModel/skins/zenmodel/leftPane.pt` modified for Event Views

The figure above highlights the single line to be inserted.

```
<li><a tal:attributes="href string:${here/dmd/ZenUsers/getUserSettingsUrl}/editEventViews">My event views</a></li>
```

Note that there is no *isManager* criteria following *here* in the new line, so this menu option will show for all user roles. Edits will take effect whenever a user logs on – there is no need to recycle any Zenoss daemons.

Note that this change will **not** be preserved during a Zenoss update.

The page contents are in Zope Page Template (ZPT) format; more details from <http://www.zope.com> . It is also possible to access the menu skins from http://yourzenossserver:8080/zport/portal_skins/zenmodel/manage .

5 What about controlling zProperties?

The initial requirement was to be able to Acknowledge, Close and Undelete events from particular devices, add to the Log tab of those events, **and** protect access to the zProperties pages of devices so that SNMP community names and Windows users and passwords could not be seen.

The good news is that there are Zope permissions explicitly for *zProperties View* and *zProperties Edit*. The bad news is that, if you need to give Manager access to a device to be able to modify events, then that will also grant both View and Edit permissions on the zProperties! You do not want to remove these permissions entirely from the Manager role.

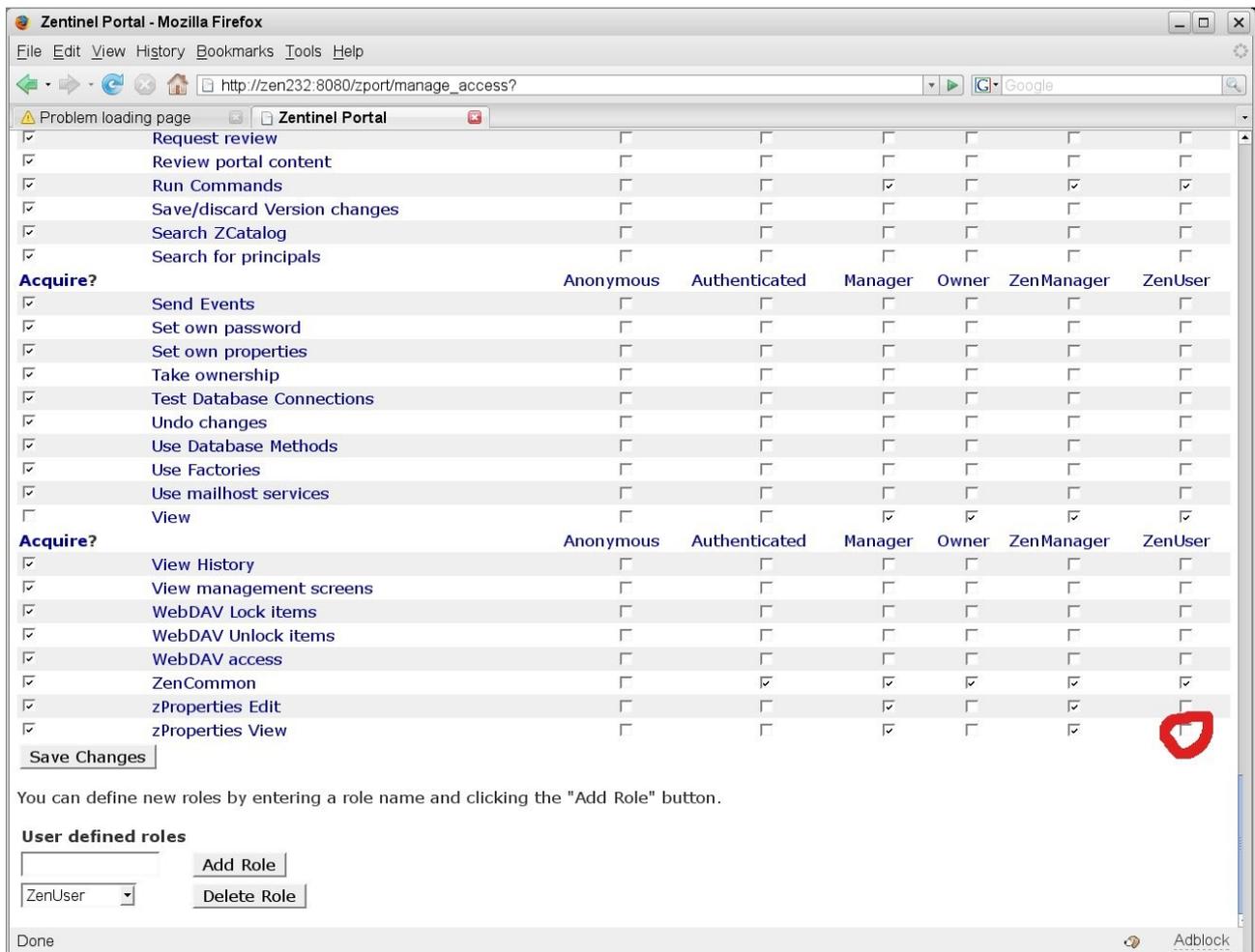


Figure 15: Zope permissions for zProperties

By default, the ZenUser role does not have the zProperties Edit permission but does have the zProperties View permission. If there is a strict requirement to protect SNMP communities and Windows logons, then both these roles can be removed. Thus, the *More* option on the table drop-down menu from a device page, will no longer have zProperties as an option.

In that case, Acknowledge / Close of events can only be achieved by granting the Manage Event permission through the Zope interface, and then creating individual Event Views for users to view events in the status table of the events database. Events from **any** device shown can be Acknowledged or Closed and the Log tab of any event can be updated. The only way to restrict which devices are shown in the Event View, would be the Event View filter mechanism; however a user with the ZenUser role can modify the filters in their own Event View. It will not be possible for such a user to Undelete events, even if they have an Event View configured to show the history events.

If the policy is that users who need Acknowledge / Close privilege on events from specific devices are also allowed to see and modify the zProperties for those devices (say the Unix sysadmin group of people need full access to all the devices in

the /Server/Linux device class), then the better solution would be to avoid individual Event Views and grant the Manager role on devices or device classes using Administered Objects, along with adding the Manage Events property to allow Log updates. Thus, these users can only interact with events through the Events tab of a device page and they can only modify events for devices where they have full authority – they can Acknowledge, Close, Undelete and modify the Log tab.

6 Conclusions

There are doubtless many more permutations of roles and access permissions, especially with further investigation of the Zope *zport/manage_access* web page. The Role-Based Access Control zenpack, available with the Zenoss Professional and Enterprise offerings, should certainly be explored first if you have access to them. That said, it is possible to craft some role-based restrictions for users simply using Zenoss Core.

Acknowledgements

Many thanks to Florian Deckert for the method for modifying the Zenoss menus.