Using Device Group Permissions in Dell OpenManage Essentials

This technical white paper describes how to use the device group permissions feature in OpenManage Essentials

OME Engineering Team

June 2013| Version 1.0

Contents

Figures

Executive Summary

This white paper describes the process of assigning users to the OmeSiteAdministrators role and assigning device group permissions to a user using OpenManage Essentials.

This document explains how to assign device group permissions to a user for targeting system update and remote tasks. OmeSiteAdministrators (a new role introduced in OpenManage Essentials v1.2) can only target device groups assigned to them. Using OpenManage Essentials, an administrator can assign a user to a specific set of device groups for targeting system update and remote tasks, reducing the impact and side effects a user can have in OpenManage Essentials.

Introduction

Several IT professionals can simultaneously use OpenManage Essentials. In many cases, the IT professionals divide responsibilities of devices. The responsibilities can be divided several ways. Devices are categorized and responsibilities divided based on geographical location, device type, operating system, network setup, and other factors. Custom device groups help users divide their devices.

Custom device groups separate and subset devices. Users can create custom device groups in OpenManage Essentials. A custom device group can be created from a query, a combination of other devices groups, a selection of devices, or a combination of device groups and device selections. Creating a subset of devices (a custom device group) makes it easier to accurately target groups of devices throughout OpenManage Essentials.

Creating custom device groups is helpful when dividing responsibilities of devices, but all device groups and devices can be targeted by users. Unwanted behaviors of devices may occur if an overlap in targets or accidental targeting of device groups occurs while creating system update or remote tasks. A misused task or update can cause downtime, additional effort, and even an interruption of service.

To mitigate the risk of incorrectly targeted tasks, reduce the scope of select users and divide the responsibilities of management more easily, the device group permissions portal and functionality was developed for the OpenManage Essentials v1.2 release. The portal configures the newly added OmeSiteAdministrators role and assigns device group permissions to members of the OmeSiteAdministrators role. The device group permissions portal's purpose is to limit what a user can target when creating remote and system update tasks.

The device group permissions portal gives administrators greater control over what users can target. An administrator can create custom groups tailored to the device responsibilities of users and assign users to the created custom device groups. For instance, an administrator can create a custom group based on the IP address range of a data center and assign the custom group to the onsite administrator. Another possible scenario is creating custom device groups based on the operating system of the devices and assigning the device groups to the operating system management specialist.

The benefit of using the device group permissions feature is that administrators have control over what targets are visible to a user. An administrator can reduce the visibility of device groups to users that should not target all device groups and devices. Hiding target devices is especially beneficial when a subset of devices is mission critical and should not be targeted by most users.

This white paper explains the use of the device group permissions portal and how the device group permissions feature in Dell OpenManage Essentials can help mitigate risks of mistargeted tasks and over privileged users. This document includes:

- Assigning users to the OmeSiteAdministrators role.
- The limitations and constraints of an OmeSiteAdministrator.
- Assigning device groups to a user.
- How to use the device group permissions portal.
- Use cases of common scenarios.
- FAQ section about the device group permissions portal and OmeSiteAdministrator restrictions.

OpenManage Essentials Roles

Users of OpenManage Essentials have one or several of the following roles. A role is a set of permissions that determines what a user can and cannot do in OpenManage Essentials. A user can have multiple roles. When a user has multiple roles, the permissions are additive.

The following section is a brief overview of the roles in OpenManage Essentials. For further reading, please visit the OpenManage Essentials roles white paper:
http://en.community.dell.com/techcenter/extras/m/white_papers/20029260.aspx

OmeUsers

Read only privileges. An OmeUser cannot create or edit items in OpenManage Essentials (exception is discovery and inventory). Cannot view or edit device group permissions.

OmePowerUsers

All read write privileges except for preferences (read only). Cannot view or edit device group permissions.

OmeSiteAdministrators

The OmeSiteAdministrators role is a new role introduced in OpenManage Essentials v1.2. The role is similar to the OmeAdministrators role, but has several limitations. To read the limitations, please see the Limitations of OmeSiteAdministrators section below.

The OmeSiteAdministrators role is a virtual user group that does not appear in the active directory. It is managed completely by the OpenManage Essentials console.

Limitations of OmeSiteAdministrators

An OmeSiteAdministrator is a limited user. An OmeSiteAdministrator does not have the same access level of an OmeAdministrator. The device group permissions portal is not visible to an OmeSiteAdministrator. To ensure the security of the role in the OpenManage Essentials console, an OmeSiteAdministrator has the following limitations.

- System Update and Remote Task Limitations
    - Can only target device groups assigned to the OmeSiteAdministrator.
    - Cannot edit remote tasks.
    - Cannot activate or deactivate remote tasks' schedules.
    - Cannot clone remote or system update tasks.
    - Cannot target device queries.
    - Can only run and delete remote and system update tasks created by the site administrator.
- Custom Device Group Limitations
    - Cannot edit custom groups.
    - Can only create custom groups under All Devices.

OmeAdministrators

All read write privileges, no restrictions.

Device Group Permissions Portal

The device group permissions portal configures the OmeSiteAdministrators role and assigns device group permissions to members of the OmeSiteAdministrators role. The portal is only visible and editable for OmeAdministrators. The following sections are instructions on the use of the device group permissions portal.

Editing Members of OmeSiteAdministrators

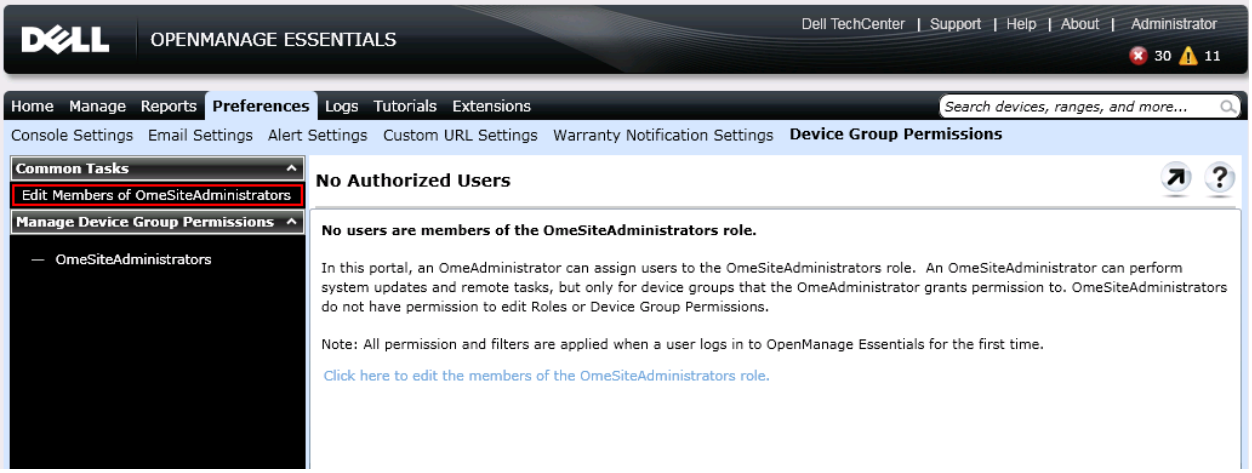
The members of the OmeSiteAdministrators role have limited system update and remote tasks targets based on assigned device groups. This limits what device groups a user can target when creating and executing system update and remote tasks. The following sections provide instructions on how to edit the members of the OmeSiteAdministrators role.

Add New User

An administrator can add users that have never logged into OpenManage Essentials by using the device group permissions portal. To add a new user that has not logged into the OpenManage Essentials console, use the following steps.

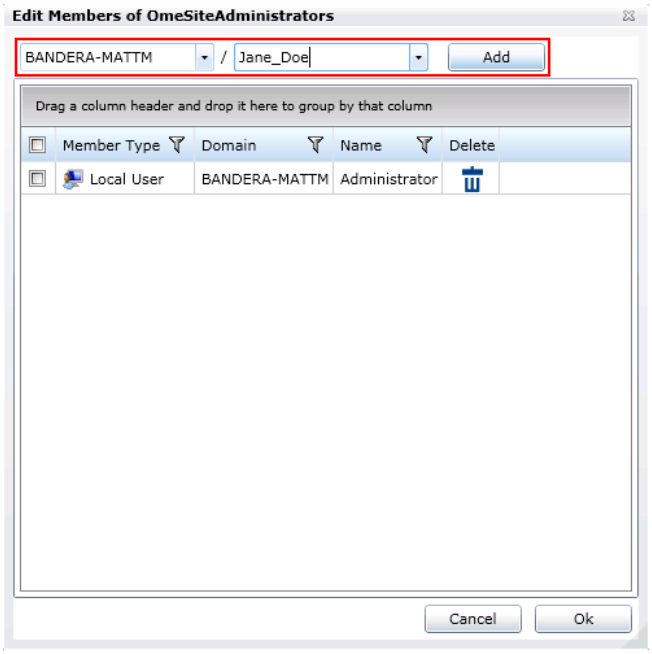
1. Navigate to the device group permissions portal (under 'Preferences').
2. Click 'Edit Members of OmeSiteAdministrators'.

Figure 1. Edit Members of OmeSiteAdministrators



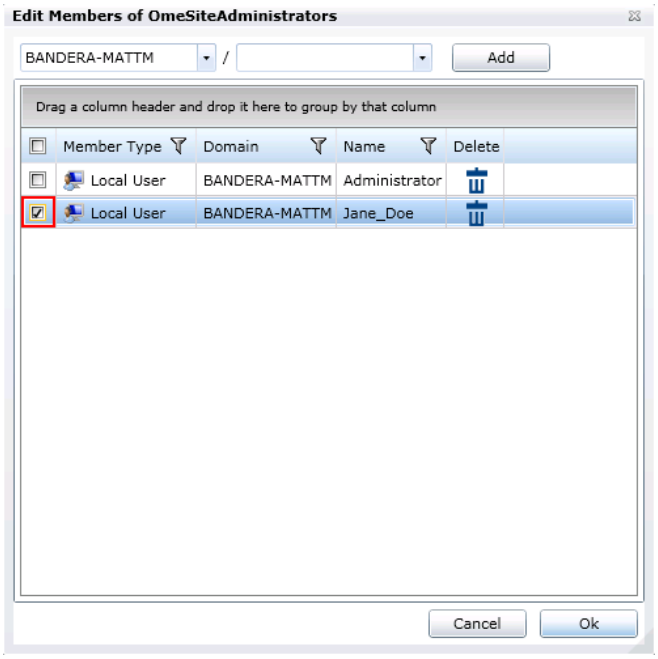
3. Click 'Domain' and type the domain of the user. (See Figure 2. Edit members wizard below)
4. Click 'Username' and type the username of the user. (See Figure 2. Edit members wizard below)
5. Click 'Add'. (See Figure 2. Edit members wizard below)

Figure 2. Edit members wizard



6. Select the added user in the users' grid.

Figure 3. Select user in edit members wizard



7. Click 'Ok'.

Add/Remove Existing User

An administrator can add and remove users from the OmeSiteAdministrators role by using the device group permissions portal. To add or remove a user that has logged into the OpenManage Essentials console before, use the following steps.

1. Navigate to the device group permissions portal (under 'Preferences').
2. Click 'Edit Members of OmeSiteAdministrators'. See Figure 1. Edit Members of OmeSiteAdministrators.
3. Check a user to add him or her to the role. Uncheck to remove him or her from the role. See Figure 3. Select user in edit members wizard.
4. Click 'Ok'.

Add an OmeAdministrator

An OmeAdministrator can become an OmeSiteAdministrator. However, to apply the limitations to the new OmeSiteAdministrator, he or she must be removed from any Window's group that is a member of the OmeAdministrators user group. To add an OmeAdministrator to the OmeSiteAdministrators role, use the following steps.

1. Navigate to the device group permissions portal (under 'Preferences').
2. Click 'Edit Members of OmeSiteAdministrators'. See Figure 1. Edit Members of OmeSiteAdministrators.
3. Check the user in the users' grid. See Figure 3. Select user in edit members wizard.

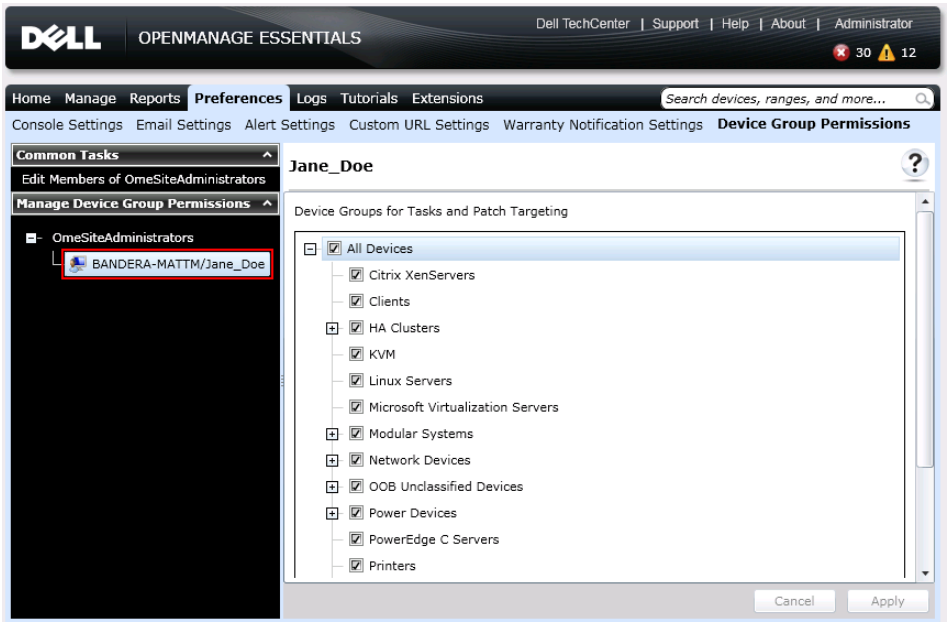
4. Click 'Ok'.
5. Click 'Ok' to the warning message that appears. This message informs you that an OmeAdministrator has been selected, and that you must remove them from the OmeAdministrators user group for the limitations to apply.
6. Navigate to the Local Users and Groups on the OpenManage Essentials' server (Server Manager → Configuration → Local Users and Groups).
7. Navigate to the OmeAdministrators user group.
8. Remove the user from any user groups that are a member of the OmeAdministrators user group.

Assigning Device Groups to an OmeSiteAdministrator

The device groups that are assigned to an OmeSiteAdministrator determine what the user can target when creating a system update or remote task. Device groups can only be assigned to a user that is a member of the OmeSiteAdministrators role. To add a user to the OmeSiteAdministrator role, please read the Add/Remove Existing User section. To assign device groups to an OmeSiteAdministrator, use the following steps.

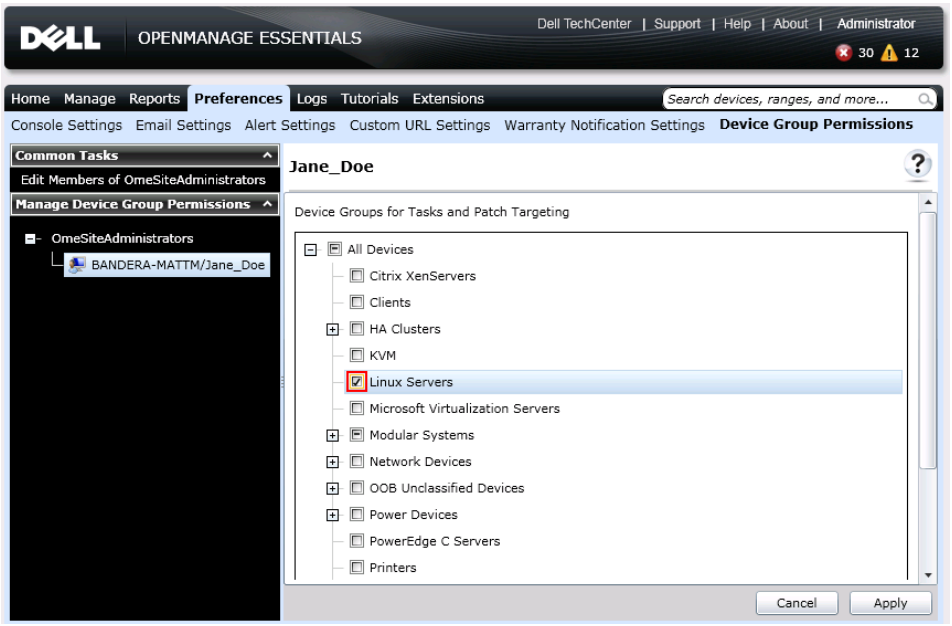
1. Navigate to the device group permissions portal (under 'Preferences').
2. Select the user in the left hand users' tree.

Figure 4. Select user in OmeSiteAdministrators tree



3. Check device groups that the user can target.
4. Uncheck device groups that the user should not target.

Figure 5. (Un)select device group permissions



5. Click ‘Apply’.

Use Cases

The following sections are examples of uses of the device group permissions portal.

Assigning Users to Location Based Device Groups

Objective: Assign all devices from a given data center location to an OmeSiteAdministrator.

For this example:

1. UserA will be assigned to the Austin data center.
    a. Austin data center is on IP range 123.45.6-7.*
2. UserB will be assigned to the Boston data center.
    a. Boston data center is on IP range 65.43.20-21.*

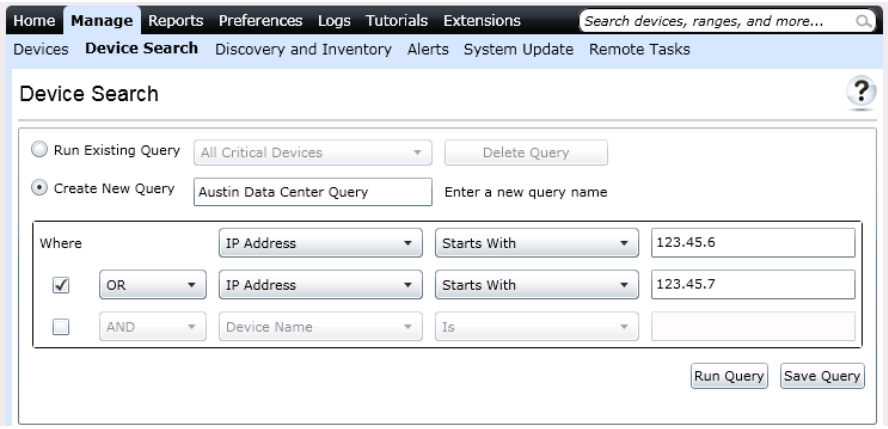
Procedure:

1. Create queries based on location.
    a. Create the ‘Austin Data Center Query’.
        i. Navigate to the device search portal (Manage → Device Search).
        ii. Name the query ‘Austin Data Center Query’.
        iii. In the ‘Where’ section, select ‘IP Address’ ‘Starts With’ and type ‘123.45.6.’.
        iv. Click the left hand checkbox to add an additional where clause.
        v. Select the ‘OR’ clause.

vi. Repeat step iii using '123.45.7.' as the IP address.

vii. Click 'Save Query'.

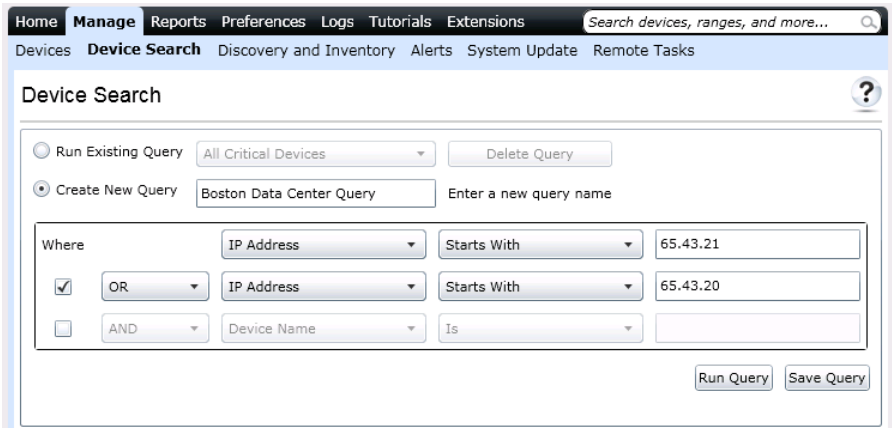
Figure 6. Create Austin Data Center Query



b. Create the 'Boston Data Center Query'.

i. Repeat step a using the IP addresses '65.43.21.' and '65.43.20.'.

Figure 7. Create Boston Data Center Query



2. Create device groups from location queries.

a. Create Austin Data Center device group.

i. Navigate to the Devices portal (Manage → Devices).

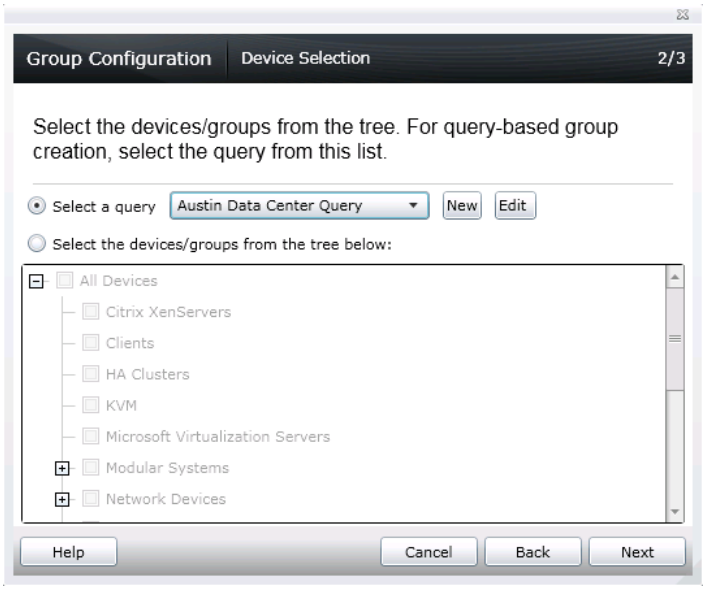
ii. Right click the 'All Devices' device group.

iii. Select 'New Group'.

iv. Name the group 'Austin Data Center' and click 'Next'.

v. Select the 'Austin Data Center Query' in the 'Select a query' drop down menu and click 'Next'.

Figure 8. Select the Austin Data Center Query



vi. Review and click 'Finish'.

b. Create Boston Data Center device group.

i. Repeat step a using the device group name 'Boston Data Center' for step a.iv and the 'Boston Data Center Query' for step a.v.

3. Assign the custom groups in step 1 to the users.

a. Navigate to the device group permissions portal (Preferences → Device Group Permissions).

b. Click 'Edit Members of OmeSiteAdministrators' (see Figure 1. Edit Members of OmeSiteAdministrators).

c. Add/Select 'UserA' and 'UserB' and click 'Ok' (see Figure 2. Edit members wizard).

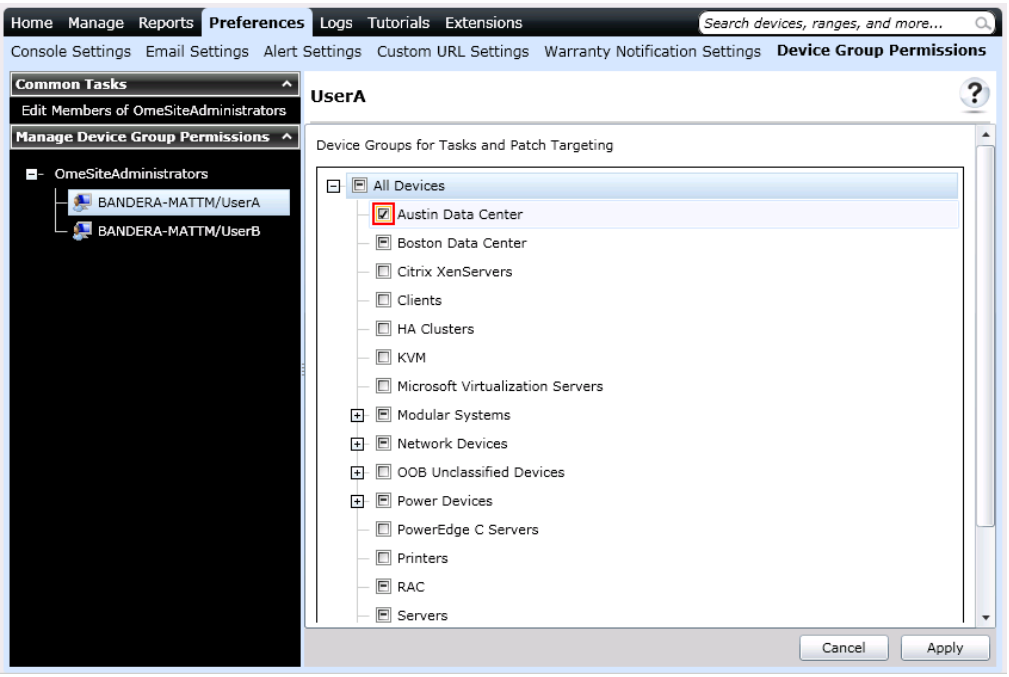
d. Select 'UserA' in the left hand OmeSiteAdministrators' tree.

i. Uncheck 'All Devices'

ii. Check 'Austin Data Center'

iii. Click 'Apply'.

Figure 9. Select the Austin Data Center device group



e. Select 'UserB' in the left hand OmeSiteAdministrators' tree.

   i. Uncheck 'All Devices'

   ii. Check 'Boston Data Center'

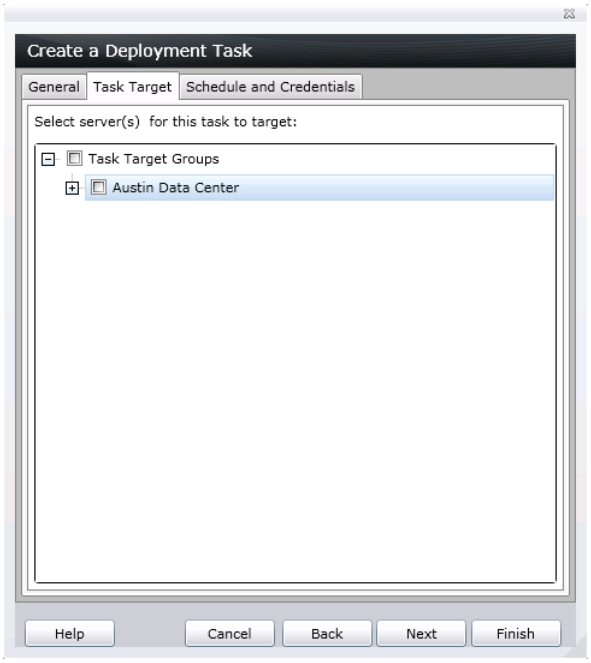
   iii. Click 'Apply.

Note: After completing the above procedure, the user must re-log into OpenManage Essentials to apply the changes.

Result:

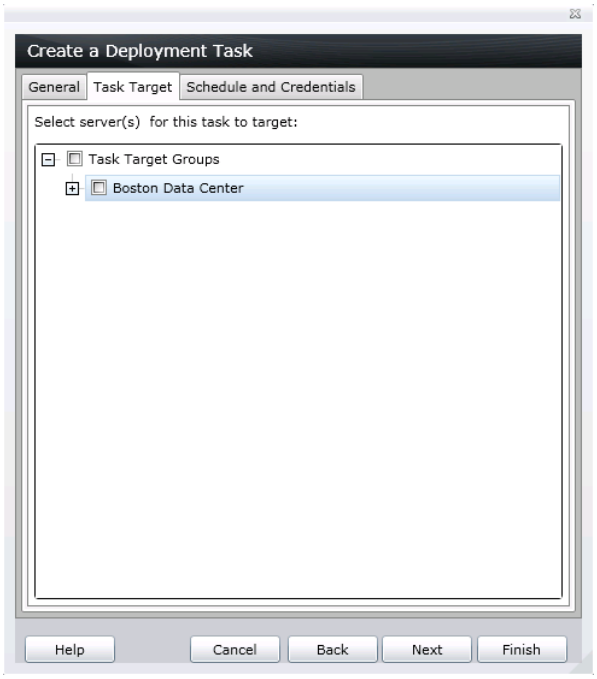
The following targets are available to 'UserA' when he or she creates a deploy server administrator task:

Figure 10. UserA deployment task targets



The following targets are available to 'UserB' when he or she creates a deploy server administrator task:

Figure 11. UserB deployment task targets



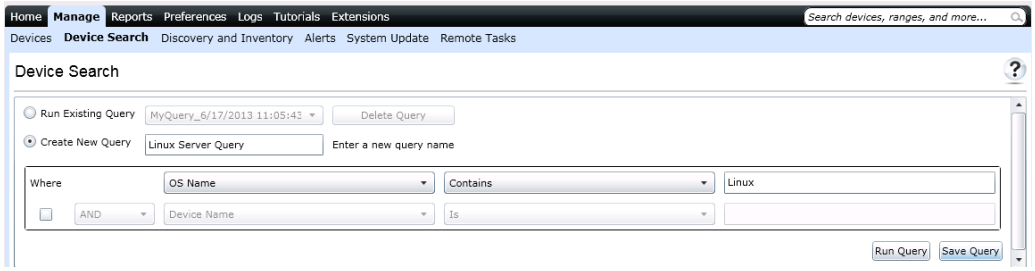
Assigning Users to Operating System Based Device Groups

Objective: Assign all Linux based machines to an OmeSiteAdministrator.

Procedure:

1. Create a device group query to target all devices with the Linux operating system.
    a. Navigate to the 'Device Search' portal (Manage → Device Search).
    b. For simplicity, use 'OS Name' for the first parameter, 'Contains' for the second and type 'Linux' for the third.

Figure 12. Create Linux OS query



    c. Name the query and click 'Save Query'.
2. Create a custom device group from the saved query.
    a. Navigate to Manage → Devices.
    b. Right click the 'All Devices' group and select 'New Group'.
    c. Name the group and click 'Next'.
    d. Select the device group query saved in step 1 and click 'Next'.
    e. Click 'Finish'.
3. Assign the custom device group created in step 2 to the user using the device group permissions portal (see Assigning Device Groups to an OmeSiteAdministrator for instructions on assigning device group permissions).

Note: After completing the above procedure, the user must re-log into OpenManage Essentials to apply the changes.

Promoting an OmeSiteAdministrator to an OmeAdministrator

Objective: Remove the restrictions of the OmeSiteAdministrator role and add a user to the OmeAdministrators role.

Procedure:

1. Remove the user from the OmeSiteAdministrators role.
    a. Navigate to the Device Group Permissions portal (under 'Preferences').
    b. Click 'Edit Members of OmeSiteAdministrators'.
    c. Uncheck the promoted user.

   d. Click 'Ok'.

2. Add the user to the OmeAdministrators user group.

   a. Navigate to the Local Users and Groups on the OpenManage Essentials server (Server Manager → Configuration → Local Users and Groups)

   b. Add the promoted user to the OmeAdministrators user group, or add the promoted user to a member user group of OmeAdministrators.

Note: After completing the above procedure, the promoted user must re-log into OpenManage Essentials to apply the changes.

Summary

The Device Group Permissions portal gives administrators the tools to restrict and limit the scope and impact of a user. Creating and assigning custom device groups allows administrators to tailor the devices available to a user based on the user's responsibilities and expertise. An administrator can limit the target device groups of a user and mitigate the risk of a user unintentionally targeting and executing against devices and device groups.

An OmeSiteAdministrator is a limited user. This type of user has several restrictions and limitations to ensure the security of assigned device groups. An OmeSiteAdministrator can only target device groups assigned to them for system update and remote tasks.

An administrator can assign device group permissions to users that have and have not previously logged into the OpenManage Essentials console. An administrator can demote an administrator or promote an OmeSiteAdministrator.

Using the device group permissions portal adds a layer of granularity to the security of the OpenManage Essentials console. The device group permissions security reduces the risk of task execution side effects and helps administrators better manage users of OpenManage Essentials.

FAQ

Device Group Permissions Portal

1. Can I add a user group to the OmeSiteAdministrators role?
   a. No, in OpenManage Essentials v1.2 we do not support adding a user group to the OmeSiteAdministrators role.
2. Can I add an administrator to the OmeSiteAdministrators role?
   a. Yes, you can add an OmeAdministrator to the OmeSiteAdministrators role. However, you MUST remove the administrator from the OmeAdministrators user group.
3. Can I add a user that has not logged into OpenManage Essentials to the OmeSiteAdministrators role?
   a. Yes, you can use the edit members wizard to add a user that has not logged into OpenManage Essentials to the OmeSiteAdministrators role.
4. What happens if a user is a power user and a site administrator?
   a. Roles and permissions are additive. The user will no longer have all of (but retain some of) the restrictions of a site administrator. The user will be able to perform edit actions

that the site administrator was not able to perform. Target security cannot be guaranteed for this type of user (they can edit groups assigned to them).

5. Can I promote an OmeSiteAdministrator to an OmeAdministrator?
    a. Yes, the user will have all rights and will be able to target all devices. It is suggested, but not required, to remove the user from the OmeSiteAdministrators role first.

Remote and System Update Tasks

1. What happens to a remote task's targets if a site administrator's device group permissions change?
    a. The remote task's targets are not affected by changes to device group permissions. Remote tasks that were created in the past may have targets that the site administrator no longer has.
2. What should a site administrator do if he or she needs to edit a task?
    a. If a site administrator is the owner of the task, he or she should delete the existing task and create a new task.
3. Can a site administrator re-run a task?
    a. If a site administrator is the creator of a task, he or she can re-run the task.
4. Can a site administrator re-run a task after renaming a site administrator?
    a. No, a site administrator must re-create tasks after being renamed.

Custom Groups

1. Can a site administrator delete devices in any group?
    a. Just like a power user or administrator, the site administrator can delete devices in any group.
2. Can a site administrator edit his or her created device groups?
    a. No, a site administrator cannot edit groups or queries.
3. Can a site administrator delete queries and custom groups?
    a. Yes, a site administrator can delete queries and custom groups.
4. Can a site administrator add devices to a custom device group?
    a. No, a site administrator cannot edit a group.