Design Guidelines

www.novell.com

ZCM Framework

prepared for

Novell PartnerNet

0.4

Novell

Disclaimer

Novell, Inc. makes no representations or warranties with respect to the contents or use of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.

Trademarks

Novell is a registered trademark of Novell, Inc. in the United States and other countries.

* All third-party trademarks are property of their respective owner.

Novell, Inc.
404 Wyman
Suite 500
Waltham
Massachusetts 02451
USA

Novell UK Ltd
One Arlington Square
Downshire Way
Bracknell
Berkshire
RG12 1WA

Prepared By

Andy Philp, Rolf Lennertz & Oliver Koelsch

ZCM Framework—Design Guidelines

August, 2007

Statement of Work: SOW #

Novell PartnerNet Number: Client #

Consultants: Andy Philp, Rolf Lennertz & Oliver Koelsch

Revision History

Version	Date	Editor	Revisions
0.1	30th August 2007	Oliver Koelsch	First Draft
0.2	11th October	Andy Philp & Oliver Koelsch	Update based on 0.1 reviews
0.3	12th October	Oliver Koelsch	Added “Configuration Settings” & Registration process
0.4	07th November	Oliver Koelsch	Added some screen shots
0.5	05th February	Oliver Koelsch	Added some version infos for System Update

Reviewer Record

Version	Date	Reviewers Name	Reviewers Role (Peer/ Team Leader / Project Manager)
0.1	11th October 2007	Andy Philp & Rolf Lennertz	Peer
0.4	28th January 2008	Norm Rupp	

Final Approval

Version	Date	Reviewers Name	Reviewers Role (Peer/ Team Leader / Project Manager)

Contents

Tables

Figures

1 Executive Summary

The purpose of this document is to give the reader basic design guidelines to setup a ZCM infrastructure in customer environments. As a basis the reader should have read the architecture document which provides the procedures to get all required information to make design decisions.

This document provides the reader with several topics to be discussed with the customer to gain insight into their environment and ensure a robust ZCM design.

At the end of this document the reader will have a clear understanding of the components that are required to be deployed to fulfill the customer's requirements with ZCM.

References:

This document is not intended to be a training document. We assume a good knowledge of ZENworks Configuration Management

Please refer to the on line documentation here www.novell.com/documentation/zcm10

2 Design Guidelines

2.1 Introduction

This chapter will provide a brief description of information we need to collect to design a ZCM infrastructure. It will guide the reader through the design process of a ZCM Zone and will give recommendations to organize devices, policies and bundles within a ZCM infrastructure.

2.2 Basic Information Needed

This information should be gathered during the analysis phase of the project:

- Number of devices per OS / number of users.
- Number of sites / specific needs per site.
- Number of departments / specific needs per department.
- Languages.
- Services to deploy (policies, applications, imaging, inventory, patch service etc).
- Working hours, blocking schedules.
- Connection Speed.
- Basic requirements (load balancing, fault tolerance, traveling/roaming users).
- Special processes like moves, replacements etc.
- User sources including user containers.
- Which applications have to be delivered to devices.
- Inventory data which is needed / actuality of data.
- Asset Data to collect (demographic data).

2.3 Basic Concepts of ZCM

ZCM is based on a top down design within zones:

- A Zone is the top level in ZCM.
- The configuration settings of the zone are inherited to all devices in a zone.
- The configuration settings of folders are inherited to all devices in a folder and sub folders (override zone settings).
- The configuration settings of a device are related to the device only (override folder or zone settings.

Details are covered in the architecture document.

2.4 Defining Naming Conventions

Before starting with creating new objects in ZCM it should be clear how to name objects like folders, groups, and devices.

When you name an object in the ZENworks Control Center (folders, groups, bundles, policies, and so forth), ensure that the name adheres to the following conventions:

- The name must be unique in the folder. It's recommend that the name is unique within a zone.
- Depending on the database being used for the ZENworks database, upper-case and lower-case letters might not create uniqueness for the same name. The embedded database included with ZENworks Configuration Management is case sensitive, so “Folder 1” and “FOLDER 1” are the same name and cannot be used in the same folder. If you use an external database that is case-sensitive, “Folder 1” and “FOLDER 1” are unique. To guarantee the same functionality after changing the database, it's recommended to use only capital letters for object names.
- If you use spaces, you must enclose the name in quotes when entering it on the command line. For example, you must enclose Folder 1 in quotes (“Folder 1”) when entering it in the zman utility.
- The following characters are invalid and cannot be used: / \ * ? : " ' < > | ` % ~
- The device name must be unique in the zone. It's recommended to use unique host names on your devices. If there are devices with the same name, the second device is renamed to “$devicename+$GUID.
- Use folder names that describe their purpose.

Examples:

- Use sites: DUS, FFM, MUC, BRA, PRV.
- Use departments: CONSULTING, SALES, HELPDESK, MGMT.
- Using names based on functionality: DEVELOPER, SUPPORT.
- Using names based on purpose: REMOTE-CONTROL-STANDARD-USER, DLU-STANDARD-USER, DLU-LOCAL-ADMIN.

2.5 Using Folder and Groups

Using ZENworks Control Center, you can manage devices by performing tasks directly on individual device objects. However, this approach is not very efficient unless you have only a few devices to manage. To optimize management of a large number of devices, ZENworks lets you organize devices into folders and groups; you can then perform tasks on a folder or group to manage its devices.

You can create folders and groups at any time. However, the best practice is to create folders and groups before you register devices in your zone. This allows you to use registration keys and rules to automatically add devices to the appropriate folders and groups when they register. Membership to Dynamic Groups will automatically update based on the defined schedule.

To be taken into account when designing folder and groups for a zone:

- Do you need to implement site /sub administrators, which have limited rights to the system or only to part of the zone? For example, a site administrator who is only responsible for a specific location.
- Help Desk users which are only allowed to assign bundle and some remote management task but not allowed to create or modify bundles, polices and so on.
- Do you need site specific settings, like inventory schedules or system variables?
- Do you need department specific configuration, like system variables to set working directories or host Ids?

2.5.1 Folders

Many of the management tasks you perform for devices fall into the two categories:

2.5.1.1 Applying ZENworks Configuration Settings

You can control how often a device refreshes its information from the ZENworks database, which ZENworks Server a device accesses for content, what information a device includes in its log files, how often the device is scanned to create a software and hardware inventory, and much more.

You define configuration settings at the Management Zone, on folders, or on individual devices. All devices inherit the Management Zone configuration settings unless the settings are overridden on the device's folder or on the individual device.

2.5.1.2 *Assigning Content*

You can distribute software (bundles) or apply policies to devices / users.

Depending on the needs you can use device specific or user specific assignments.

All system related bundles or policies should be assigned to devices.

Take the following into account:

- Are there bundles that are needed on each device?
- Are there bundles only needed by a set of devices or users?
- Are there a general demands/requirements to use device based deployment?

2.5.1.3 Recommendations

Folders let you manage both configuration settings and content. For best results, it's recommended to place devices with similar configuration setting requirements in the same folder. If all devices in the folder require the same content, you can also make content assignments on the folder.

- Create folders for each site (i.e. different closed server rules, schedules).
- Create folders for each department in each site (i.e. different blackout schedules, inventory schedules).

Examples:

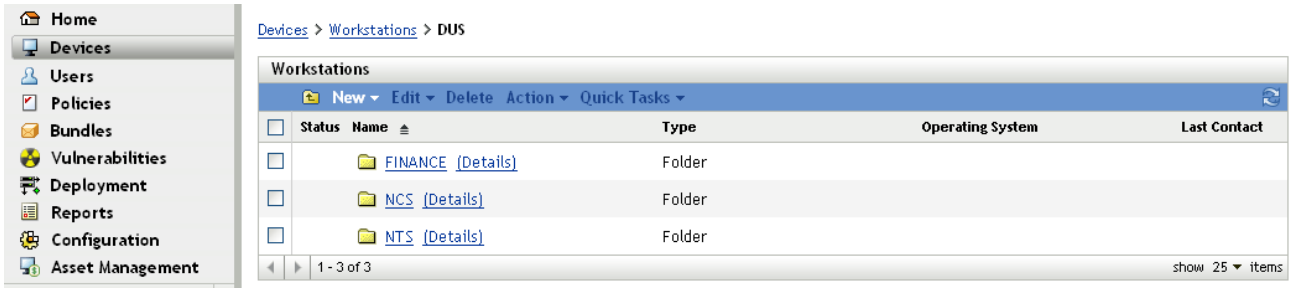

Figure 1: Device Folder - part I

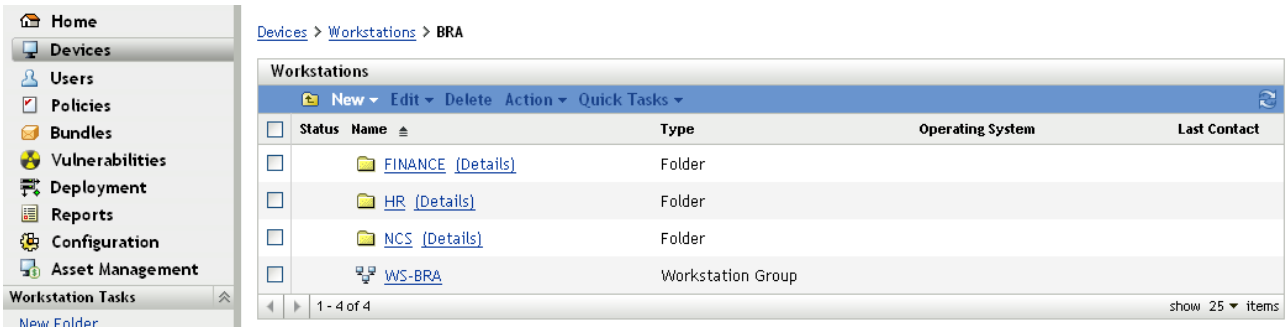

Figure 2: Device Folder - part II

More than likely, all devices in the folder might not have the same content requirements. Therefore, you can organize the devices into groups and assign the appropriate content to each groups (see Groups below). This should be an additional configuration step. It's not recommended having a “group only” setup, because of some limitations for configuration settings.

2.5.2 Groups

In some cases, you might not want to assign the same software or policies to all devices in a folder. Or, you might want to assign the same software or policies to one or more devices in different folders. To do so, you can add the devices to a group (regardless of which folders contain the devices) and then assign the software or policies to the group.

For example, let’s revisit the example of the workstations at two2 different sites (see Folders). Assume that some of the workstations at each site need the same financial software. Because groups can be assigned software, you could create a finance group, add the target workstations to the group, and then assign the appropriate financial software to the group.

The advantage to making an assignment to a group is that all devices contained in that group receive the assignment, yet you only need to make the assignment one time. In addition, a device can belong to any number of unique groups, and the assignments from multiple groups are additive. For example, if you assign a device to group A and group B, it inherits the software assigned to both groups.

ZENworks Configuration Management provides both groups and dynamic groups.

From the perspective of software and policy assignments, groups and dynamic groups function exactly the same. The only difference between the two types of groups is the way that devices are added to the group. With a group, you must manually add devices. With a dynamic group, you define criteria that a device must meet to be a member of the group, and then devices that meet the criteria are automatically added.

ZENworks include several predefined dynamic server groups (Windows 2000 Servers and Windows 2003 Servers) and dynamic workstation groups (Windows XP Workstation, Windows 2000 Workstation, and Windows Vista Workstations). Any devices that have these operating systems are automatically added to the appropriate dynamic group.

2.5.2.1 Limitations of Groups

It's not possible to apply configuration settings to groups.

2.5.2.2 Using Patch Services with Groups

As a limitation in using only folders to organize devices it's not possible to create mandatory baselines for folders and it's not possible to see vulnerabilities based on a folder.

Therefore it's recommended creating groups for patch deployment. So you are able to deploy patches based on pre-defined schedules and order.

2.5.2.3 Recommendations

Groups should be based on the specific needs of the customer as defined in analysis phase of the project. At this moment we can only make some suggestions to organize groups.

- Create groups for each department.
- Create groups for functional device sets (like pilot or test devices).
- Create groups for specific software or requirements (i.e. CAD-devices).
- Create groups based on network address (referred to buildings or levels).
- Create groups on administrative purpose (i.e. rights assignments).
- Create groups for reporting purposes (i.e. workstations in dept. sales, rights assignments).

There is no preferred method of using dynamic groups, but from experience it's more flexible than using normal groups and you do need to add the devices manually.

Examples for Groups:

- DUS-WS: contains all devices in folder DUS.
- FFM-WS: contains all devices in folder FFM.
- CONSULTING-WS: contains all devices in consulting department in all locations (Dynamic Group).
- HELPDESK-WS: contains all HELPDESK devices.
- CAD-WS: contains all device where AUTOCAD is installed (dynamic groups).

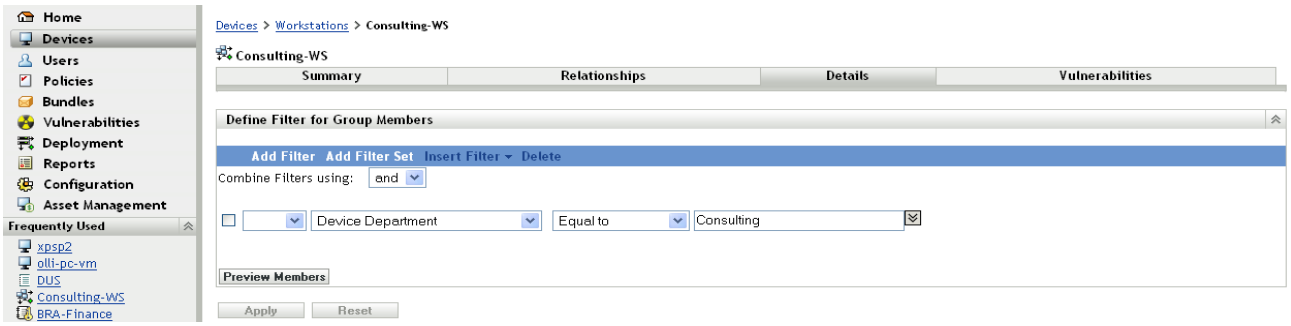

Figure 3: Dynamic Group (based on department)

Novell recommends using a combination of folders and (dynamic) groups as a base level configuration.

- Define global settings on zone level (global variables, refresh schedules etc.).
- Define site settings on folders (site variables, inventory schedules etc.).

- Define department settings on folders (variables, inventory schedules, blackout schedules etc.).
- Keep your folder structure as simple as possible.
- Use dynamic groups for our “soft criteria” like departments or functions.
- Make sure your dynamic groups rules do not affect roaming devices (like IP subnets).

2.6 Registering Devices

When you deploy the ZENworks Adaptive Agent to a device, the device is registered in the Management Zone and becomes a managed device. As part of the registration, you can specify the device’s ZENworks name and the folder and groups to which you want the device added.

By default, when a device’s host name is used as its ZENworks name, it is added to the /Servers or /Workstations folder, and it is not given membership in any groups. You can manually move devices to other folders and add them to groups, but this can be a burdensome task if you have a large number of devices or if you are consistently adding new devices. The best way to manage a large number of devices is to have them automatically added to the correct folders and groups during registration.

To add devices to folders and groups during registration, you can use registration keys, registration rules, or both. Both registration keys and registration rules let you assign folder and group memberships to a device. However, there are differences between keys and rules that you should be aware of before choosing whether you want to use one or both methods for registration.

2.6.1 Registration Keys

A registration key is an alphanumeric string that you manually define or randomly generate. During deployment of the ZENworks Adaptive Agent on a device, the registration key must be provided. When the device connects to a ZCM Server for the first time, the device is added to the folder and groups defined within the key.

You can create one or more registration keys to ensure that devices are placed in the desired folders and groups. For example, you might want to ensure that all of the Sales department’s workstations are added to the /Workstations/Sales folder but are divided into three different groups (SalesTeam1, SalesTeam2, SalesTeam3) depending on their team assignments. You could create three different registration keys and configure each one to add the Sales workstations to the /Workstations/Sales folder and the appropriate team group. As long as each workstation uses the correct registration key, it is added to the appropriate folder and group.

2.6.2 Registration Rules

If you don’t want to enter a registration key during deployment, or if you want devices to be automatically added to different folders and groups based on predefined criteria (for example, operating system type, CPU, or IP address), you can use registration rules.

ZCM includes a default registration rule for servers and another one for workstations. If a device registers without a key, the default registration rules are applied to determine the folder and group assignments. The two default rules cause all servers to be added to the /Servers folder and all workstations to the /Workstations folder.

The two default rules are designed to ensure that no server or workstation registration fails. Therefore, you cannot delete or modify these two default rules. You can, however, define additional rules that enable you to filter devices as they register and add them to different folders and groups. If you’ve established folders for devices with similar configuration settings and groups for devices with similar

assignments, newly registered devices automatically receive the appropriate configuration settings and assignments.

2.6.3 Recommendations

Based on your final folder and groups design it's recommended to create registration keys for each folder you have created/defined.

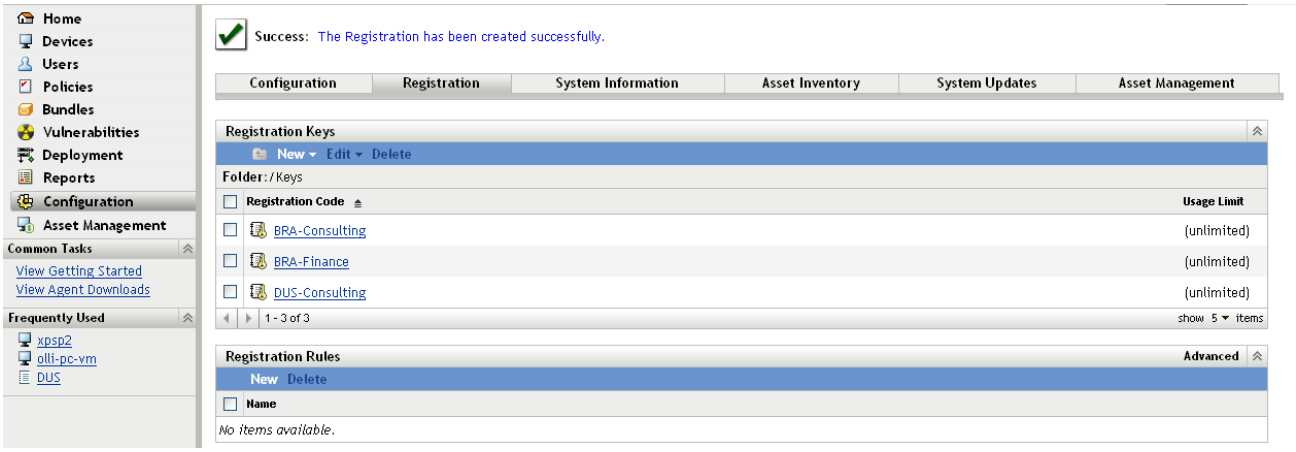

Figure 4: Registration Keys

Examples:

- DUS-Consulting: Registers to Folder CONSULTING below DUS.
- BRA- Finance: Registers to folder FINANCE below BRA.

In combination with dynamic groups which are based on department it's possible to manage device registration very easily. Using these keys in your deployment packages you can auto-register all devices in your Zone.

Novell recommends using a special folder for all new devices (i.e. “NEW DEVICES”). This folder is used to auto-register your new devices temporarily to make sure all new device are manageable after agent installation without affecting other devices. Afterwards the zac tool has to be run to re-register the device with your predefined keys to place the device in the correct folder.

2.7 Organization and Management of Bundles

There is no technical requirement to organize bundles in different folders, but from the administrative side it's recommended to use a minimal folder structure to divide applications and images. With folders it's very easy to create special administrative accounts which only have limited rights to a given folder.

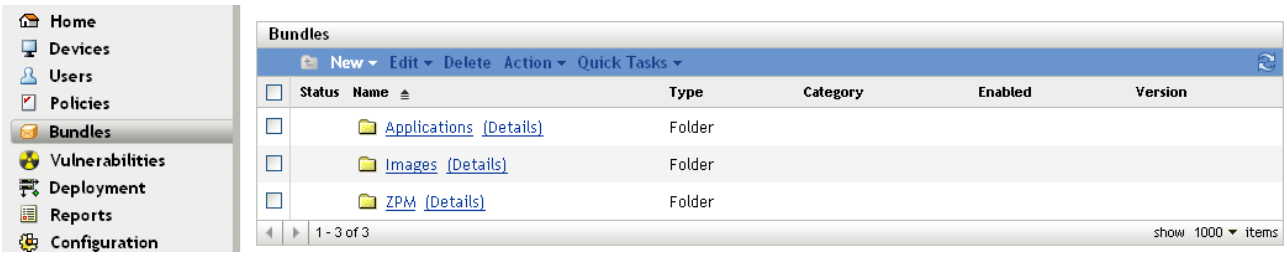

Figure 5: Bundle Folder

2.7.1 Recommendations for Organizing Bundles

- Create a folder for application bundles.
- Create a folder for imaging bundles.

The ZPM-folder is an auto-generated folder which contains all patch-service related bundles. This cannot be changed, but it's possible to create bundles in this folder manually.

The folder structure below these base-folders depends on customer needs but it's recommended to use additional folders to sort image-bundles and application-bundles. The following are some examples:

- Create folder for Software vendors.
  - Microsoft (Office, IE7, MediaPlayer).
  - Adobe (Reader, Photoshop).
  - SAP (Basis, HR).
  - Novell.
- Create folder for special applications.
  - CAD.
  - Database applications.
  - Software development.
- Create folder for tools.
  - Windows tools (WinZip, WinRAR, UltraEdit).
- Create folder for base images.
- Create folder for Add-on images.

These folders can be used to limit the access to special applications folders only.

Figure 6: Bundle Folders

2.7.1.1 Bundle Groups

In addition to a folder it's a good idea to create bundle groups for some sets of applications which makes assignments easier. Each group contains a set of bundles which belong together. These groups can be organized on special functions or tasks.

The following are some examples.

- APPS-Base: contains all applications which are needed by all users.
- Finance-Applications: contains bundles which are need to work with finance applications.
- Help Desk-Tools: contains bundles which are Help Desk related.

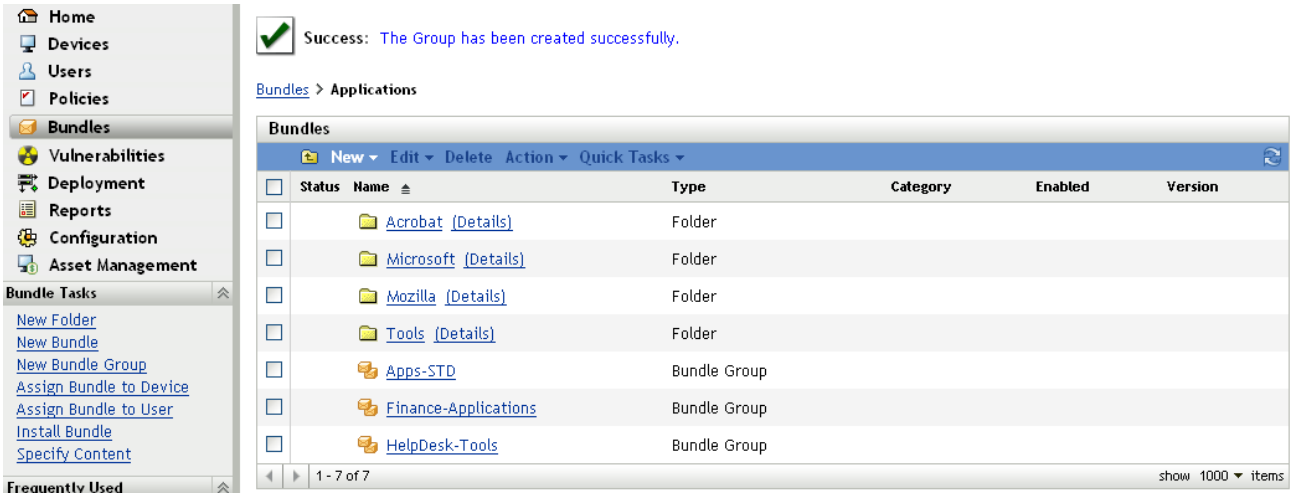

Figure 7: Bundle Groups

Current Limitations of using bundle groups:

If you are trying to order the installation of bundles, you can change the order of each bundle. However there is no logic behind the scenes that actually runs the bundles in that order. At the moment, bundles are ordered alphabetically for the first few and then the order is random.

Novell recommends using bundle groups for icon delivery only.

2.7.2 Assigning Bundles

As stated earlier in this document a major feature of ZCM is inheritance of assignments. With this feature it's very easy to assign a bundle or bundle groups to lots of devices in seconds. You do not need to assign bundles to each device.

Based on your folder and group design it's recommended to use folder or group assignments instead of direct assignments. Use these indirect assignments wherever possible, because of speed and administration effort.

Examples:

- If you have a set of bundles which are required for all devices in a site, use the site folder to assign these bundles or bundle groups.
- If you have special bundles which are used in one or more departments, assign these bundles only to these department folders.
- If you have bundles which are used by several devices in different folders, setup groups for assignments.
- Only use direct assignments if a single device or quite small number of devices needs special assignments.

2.8 Organization and Management of Policies

In general it's not a good idea to have thousands of different policies in place, to fulfill all requirements, therefore, a folder might be not useful in this case. Normally in desktop management areas there are some sets of policies for normal users, administrative users and special user groups like software developers.

But from the administration side it might be an option to organize policies in more than one folder, to restrict access and administration to specific groups or users.

Putting all things together it would be a good idea to organize different set of policies in different folders. In addition it's recommended using policy groups to put different policies together in a single package. (Remember Policy Package in older ZENworks Versions) and then associate these Policy Groups to devices or Users.

To make sure every device will receive the required and needed (effective) settings, it's recommended to define the order of applying policies. There are 4 options you can use:

- Apply device policies first, user policies last (user assigned policy wins).
- Apply user policies first, device policies last (device assigned policy wins).
- Only device policies.
- Only user policies.

All policies are applied in the order folder, group, device or user.

The following picture shows the effective policies on a device.

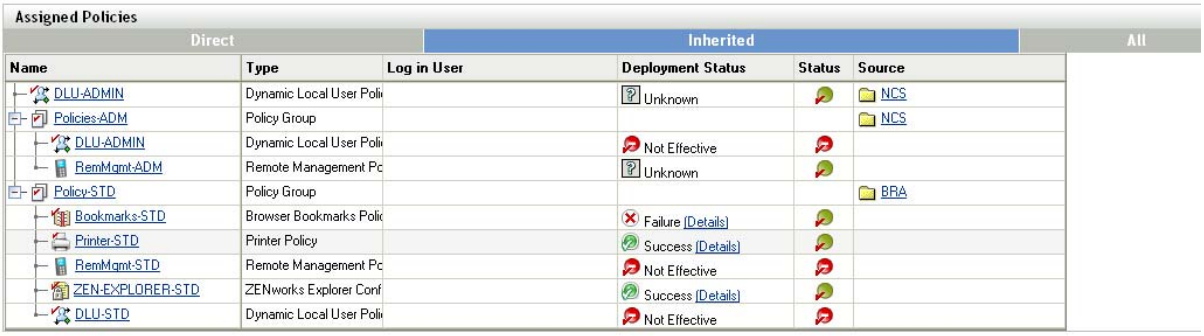

Figure 8: Policy Assignments

In the above example there is a policy group assigned to a folder BRA. This group contains all policy settings (Policy-STD) which are required for all users in BRA. Additionally there is policy group assigned to the NCS folder (below BRA). At the end there is a direct policy assignment to the NCS folder which modifies the DLU-Settings only.

2.8.1 Recommendations

- Define user and device categories based on analysis phase, like Standard-user, Admin -user, mgmt-user, Help desk-device.
- Define required policies and sets which can be used for bundle groups.
- Define order of applying policies (can be done for each assignment), but it's very hard to change later.
- Assign policy groups to folders as needed.
- Use folder or group assignments wherever possible.

2.9 Connecting to User Sources

In addition to assigning content (bundles and policies) to devices, you can assign it to users. Unlike device-assigned content, user-assigned content is available on a device only when the user is logged in to the device.

To be able to assign content to users, you must create a read-only connection to an LDAP directory that contains the users. This exposes the users in ZENworks Control Center and enables you to make the assignments. Your LDAP directory is not affected; ZENworks requires read access only to the LDAP directory and stores all assignment information in the ZENworks database.

You can connect to Novell® eDirectory™ and Microsoft* Active Directory* as user sources.

After you connect to an LDAP directory, you define the containers within the directory that you want exposed. You could reference the top level containers of the user source as the source and or especially the containers which contain users. This limits access within the directory to only those containers that include users.

Both have some advantages and disadvantages which are mostly related to administration. There is no difference in assigning bundles or policies.

Selecting top level containers enables all users in sub-containers and additions to these structure (adding new containers) are maintained automatically and can be used for assignments without changes within ZCM. The big disadvantage is that there is no way to detect deleted containers in the user source. If you assign a bundle to a container which will be deleted later, you cannot see this change in ZCM.

In addition it's not possible to add sub-containers if the parent container is already in list. If you want to change this, you have to delete the parent container, but you will loose all assignments.

Therefore it's recommended using only containers where users reside.
This means adding multiple sublevel folders from an eDirectory or ADS directory rather than only one.

For examples see below:

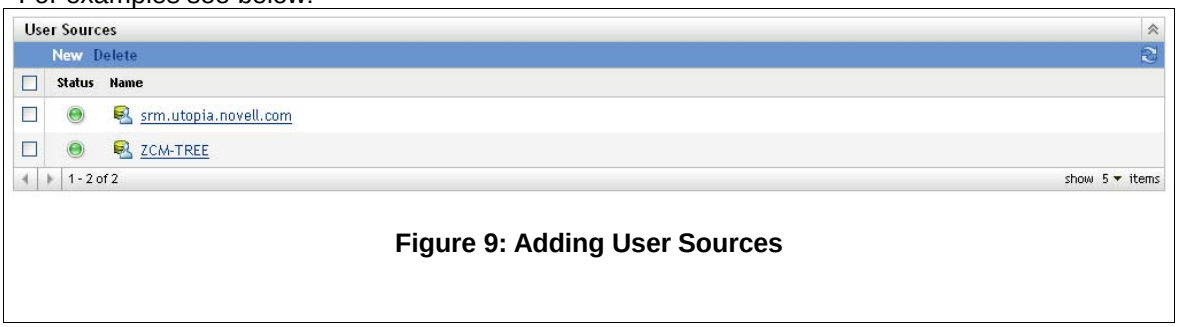

Figure 9: Adding User Sources

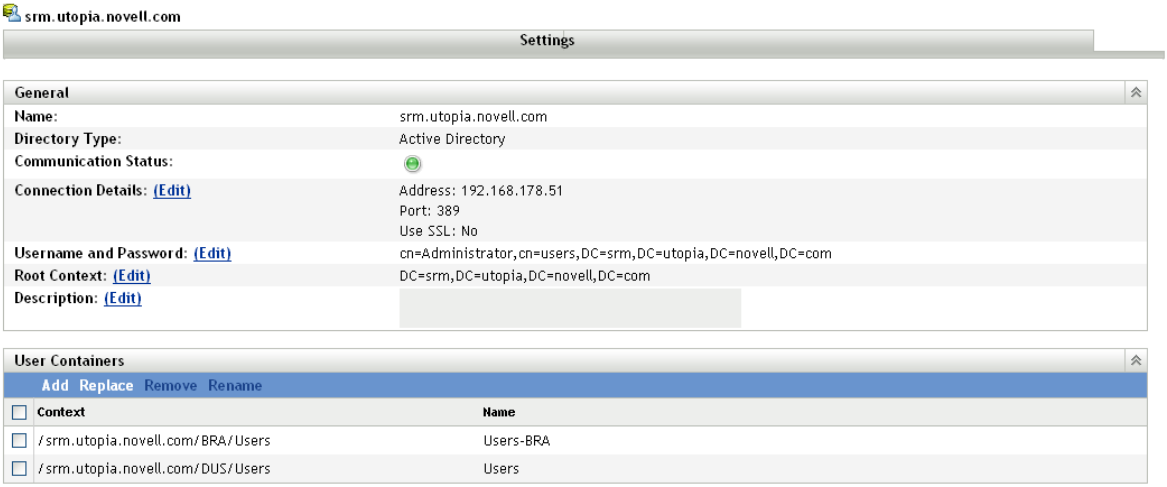

Figure 10: Adding User Container in AD

2.10 Configuration Settings

This section provides all information which is needed to configure your zone with some basic settings. Novell cannot cover all settings at this time, but will give some recommendations to get your servers up and running as quickly as possible.

The Management Zone Settings panel lets you manage the global configuration settings for your Management Zone. These global configuration settings are inherited by other objects (devices, users,

and folders) within your Management Zone and remain in effect unless they are overridden on those objects.

You should configure the global settings to accommodate the largest possible number of objects, and then use the override option on any objects you want to configure differently. For example, you should use the Device Refresh Schedule setting to define the schedule that you want the majority of devices to use, and then override the schedule on individual devices or device folders if those devices require a different schedule.

Based on the data you have collected during the analysis phase of a project, Novell recommends a minimum configuration which is described in the next chapters.

2.10.1 Content Blackout Schedule

Define a zone based setting only if you are sure to use this seating for all devices. In normal environments it's not recommended to use common blackout schedule for all devices.

A content blackout schedule is needed only for special devices, like device in the finance department or production PC's, which are used for controlling production processes.

2.10.2 ZENworks Explorer Configuration

This settings defines the uninstall feature. If your customer does not need to uninstall, disable this feature in your zone. Otherwise define this feature as required.

2.10.3 System Variables

System variables are used to define paths, names and other things in your system. In addition to the predefined variables. Novell recommends the use of variables in bundles.

Common variables are “SOURCE_PATH” or “TARGET_PATH”

- Define Variables for your zone.
- Define Variables for your folders if you need different or additional settings.
- Define Variables in your bundles only if above settings do not fit your needs.

2.10.4 Content Replication Schedule

The content replication schedule defines how often a content server (CDP or primary server) checks the database for updates (new content or deleted content).

Novell recommends changing the default value (5 Minutes) to at least 30 minutes to prevent the system from heavy load.

2.10.5 Local Device Logging

- Log Messages with the severity “Error”.
- Rolling log files based on a date. Create a new log file every day.

2.10.6 Device Refresh Schedule

Use the default schedule as a starting point. Discuss the schedules with your customer.

Short refresh times for a huge number of devices can cause extensive server load.

Use random refresh rates to prevent server overload.

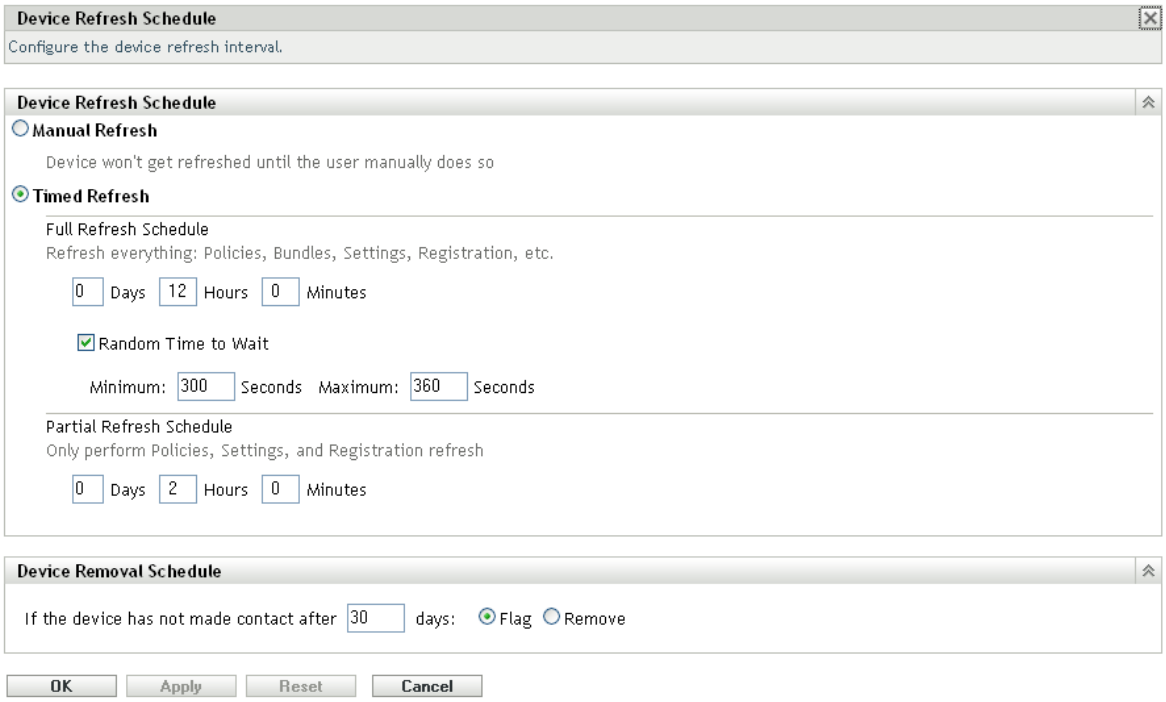

Figure 11: Device Refresh Schedules

2.10.7 Device Removal Schedule

Discuss this setting with your customer. Use the default setting as starting point.

Take the following into account:

- How to maintain actual reporting data? Do you need very accurate data?
- How long are the devices off-line (average time)? Possible cases are vacation, illness,etc.
- Do you need statistics on removed devices?

2.10.8 Dynamic Groups Refresh Schedule

Novell recommends the usage of dynamic groups. Therefore the membership of these groups has to be recalculated on a regular basis to get the expected results.

For your initial configuration Novell recommends a daily refresh schedule. (All days of the Week).

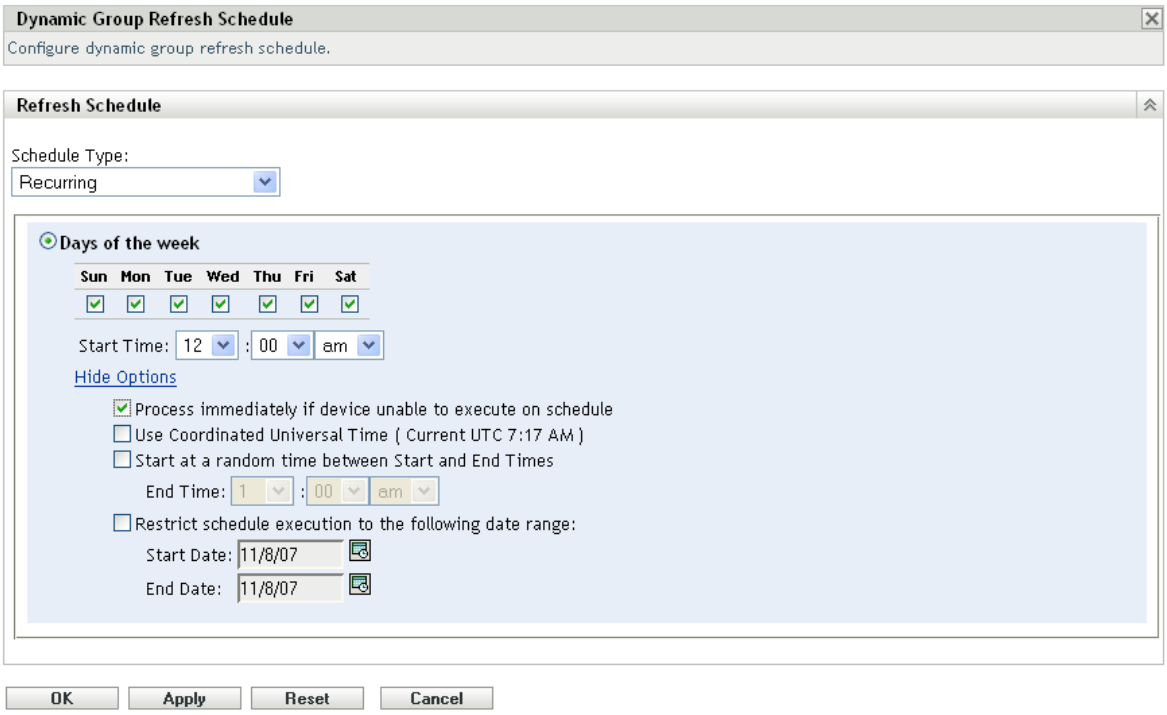

Figure 12: Dynamic Group Refresh Schedule

2.10.9 Registration

Enable dynamic device rename which is disabled by default.

This feature will provide a very flexible way to handle some desktop management processes like renaming or re installation. During our ZCM framework based installation process the device name changes to a randomly generated name, but with this feature in place and a working imaging partition all references are maintained automatically by the ZCM-agent registration process.

This will prevent having duplicated device entries (with GUID added) in the database.

2.10.10 Closest Server Rules

Setup “Closest Server Rules” to fulfill your requirements.

If you have servers on different subnets define a rule for each subnet.

If you have your devices in different (sub)-domains setup a rule for each domain.

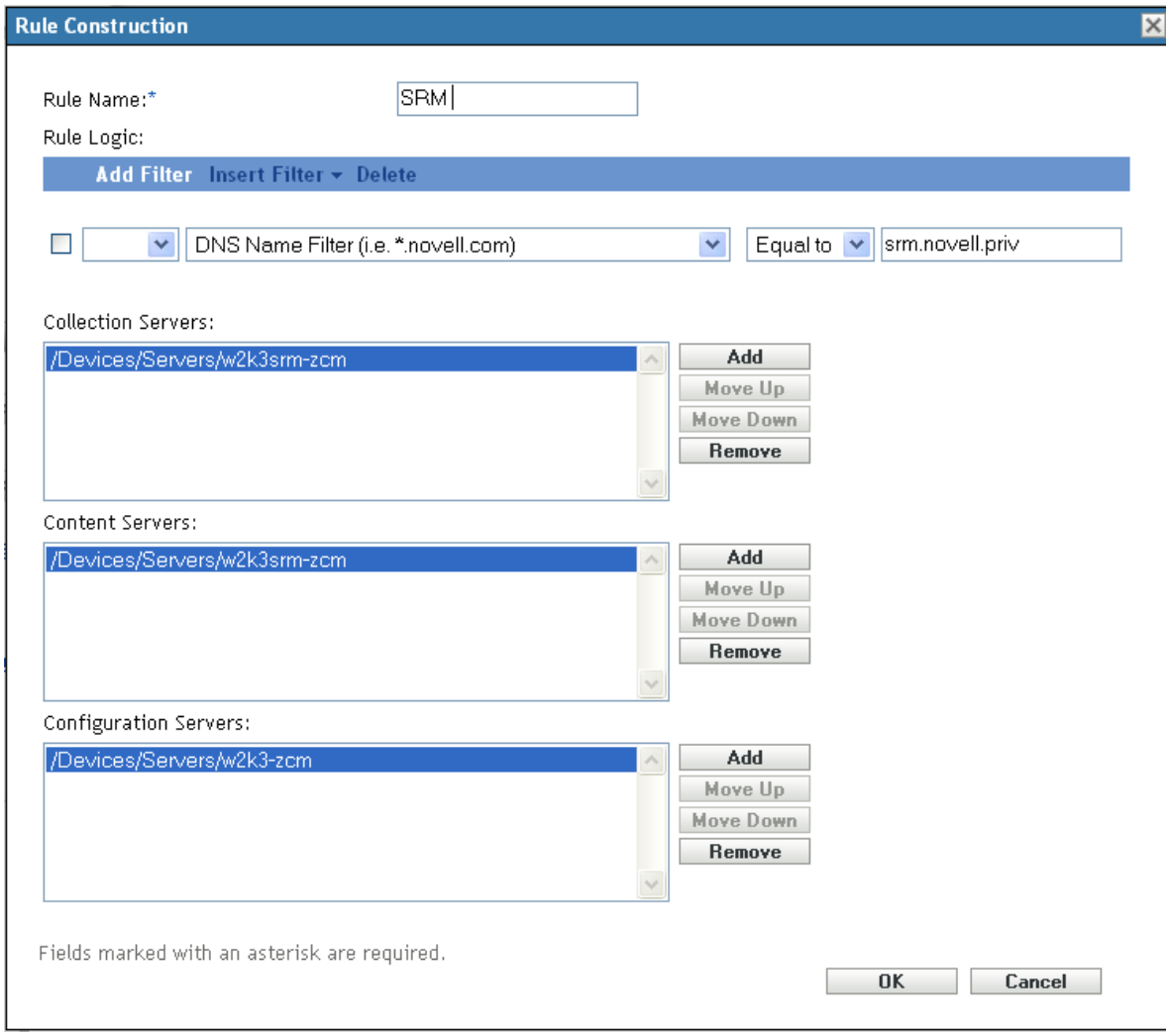

Figure 13: Closest Server Rules

2.10.11 Inventory Schedules

Setting the inventory schedules depends on the requirements in your database should be. Under normal circumstances it should be enough to collect inventory data on a weekly or monthly basis. It's not recommended scanning thousands of devices every day.

For a weekly scan select a certain day (do not scan on Monday or Friday) and a period of time during normal working hours that best fits your environment. In addition select the “process immediately” option to make sure that all active devices are scanned during the scan interval.

Select a start time and use the “random” option.

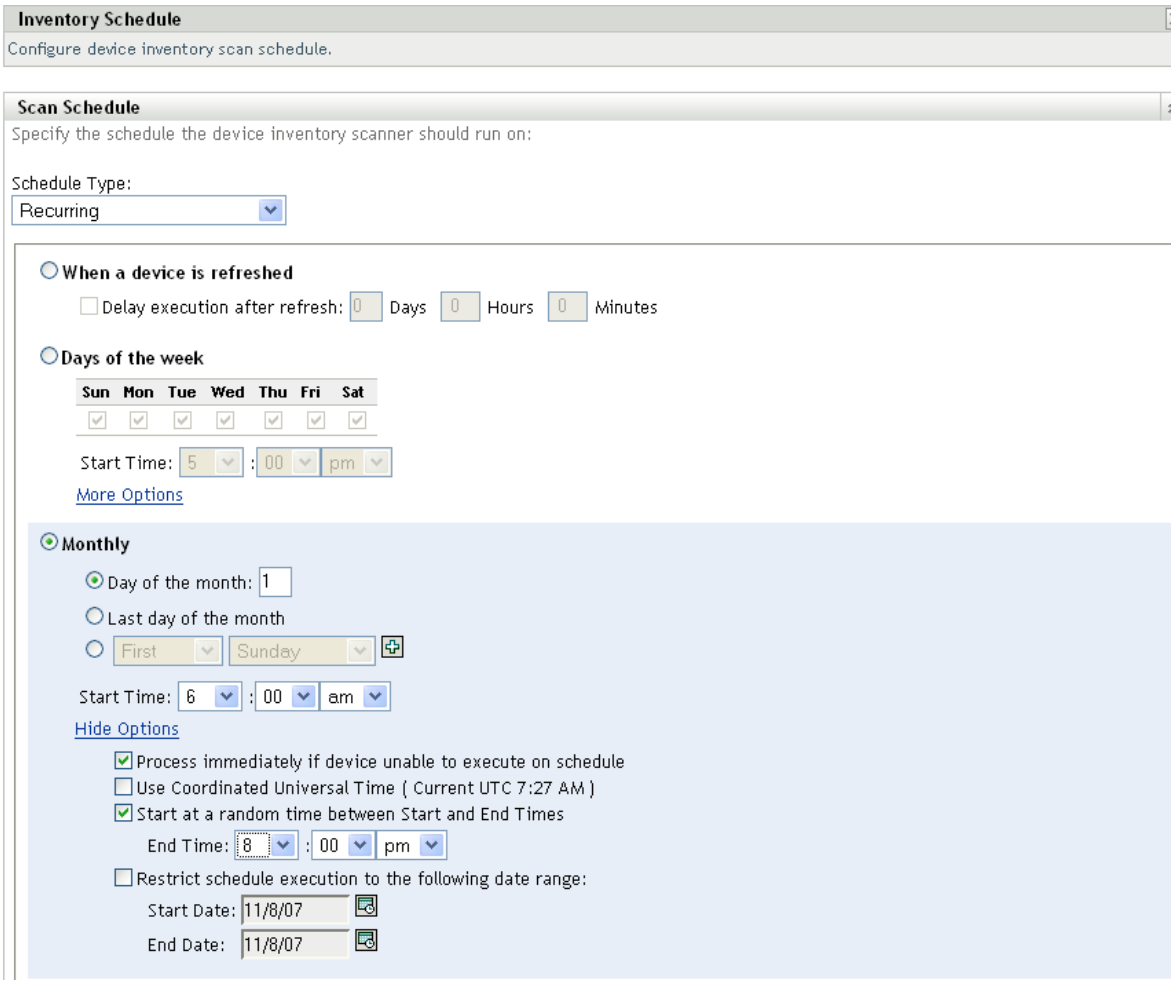

Figure 14: Inventory Schedules

2.10.12 Collection Data Form and its Schedules

The collection data form is used to collect demographic information of a device or user. The information can be collected on several schedules or events.

Select a schedule which best fits your requirements. Collecting this information on a monthly basis should be a good choice. You have to make sure a new collection is run after a change (like move, user change).

Use the auto fill-function if possible to avoid user input.

Define as much data as possible (site, department, cost center) which is auto configured with system variables or registry settings. These things can be delivered through the install process or bundles.

2.10.13 Remote Management

Use default settings as a starting point.

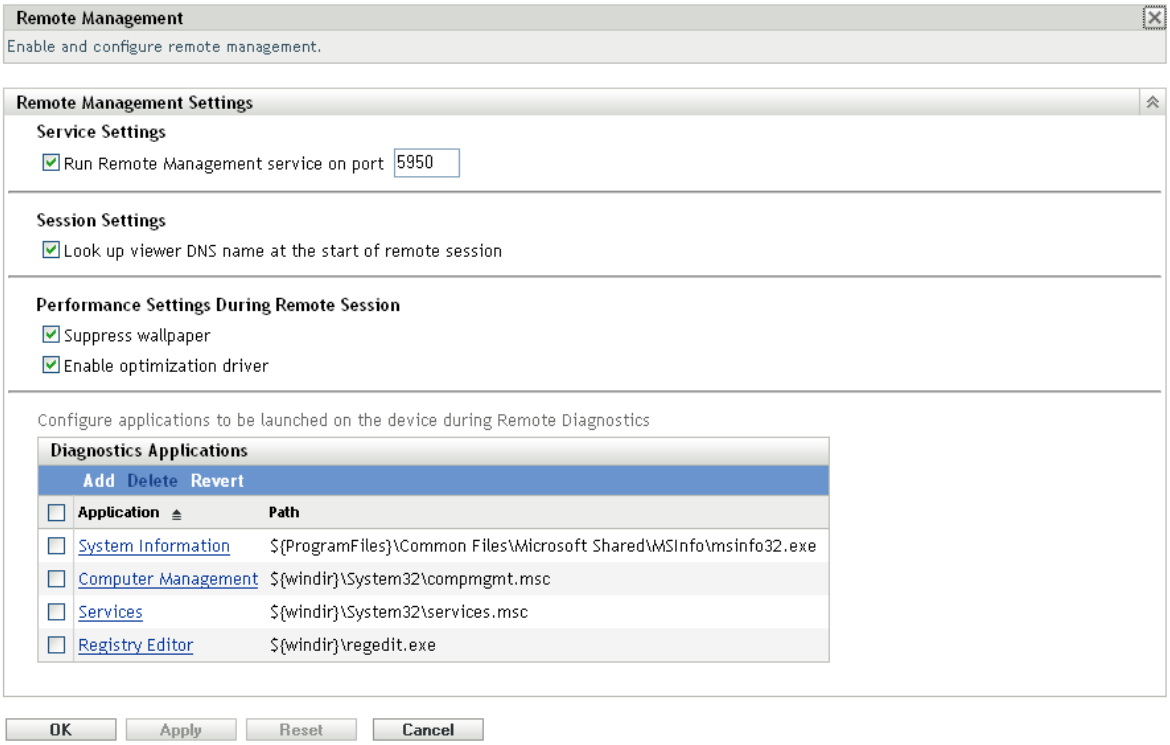

Figure 15: Remote Management Settings

2.11 Setting Up Administrative Accounts

In ZCM you can define additional user accounts which are able to manage the ZCM infrastructure. These accounts can be both new accounts and accounts that are defined in your user sources.

One admin user is created as part of ZCM Installation. This account is called Administrator.

All admin accounts receive view rights. These rights are not removable.

During the analysis phase of the project, all requirements regarding administration should be collected. In most environments some accounts are needed to maintain bundles, some accounts are responsible for policy and so on. In addition most customers need users to collect and define reports on specific devices or user.

As a minimum, it's required to add each administrator by name. Using accounts based on the user source should be preferred.

In addition, it's recommended to setup a special super admin which is not connected to a user source. This account should be used in case of emergency, .i.e. forgotten passwords for admins.

If you need to provide accounts / passwords in automatic deployments using ZAC, Novell recommends creating special users for creating devices. Assign these users rights to modify devices as shown in the following figure:

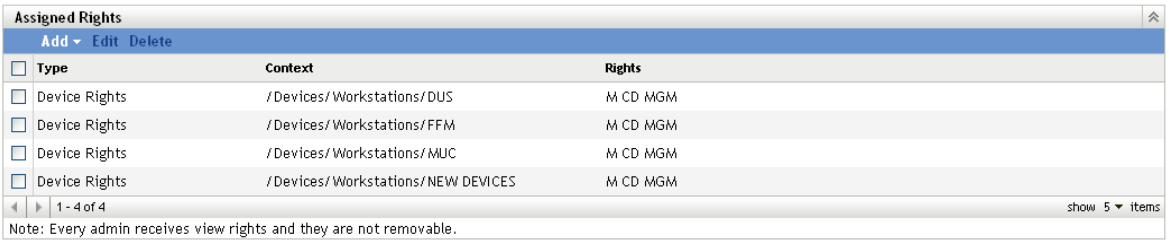

Figure 16: Device Rights for Register/Unregister Devices

2.12 Agent Deployment

Novell ZENworks Configuration Management provides a variety of methods you can use to install the ZENworks Adaptive Agent to devices:

- Use ZENworks Control Center to deploy the agent from the ZENworks Server to the device.
- At the device, use a Web browser to download the agent from the ZENworks Server and install it.
- Include the agent in an image and apply the image to the device.
- Use a login script, Windows group policy, or ZENworks 7 Application object, to install the agent.

As you normally implement ZCM in larger environments it's recommended deploying the ZCM agent automatically to your devices, therefore it should not be an option to manually install the agent.

It's recommended using one of the following deployment methods:

- Use deployment task from ZCC, after discovering or importing devices.
- Use your existing software distribution tool to deploy the agent.
- Include the ZCM agent in a new image.

For all methods you must have registration keys in place as described earlier in this document.

2.12.1 Custom Deployment Packages (with alias names)

During the ZCM installation default agent deployment packages are created. These packages are tied to the primary server and contain the URI from this server to register devices. There are no registration keys configured and the registration process will use default rules to register devices.

If you have more than one primary server which is the case in most environments you should consider setting up an alias name (i.e. ZCM-SERVER.<yourdomain>.com) in your DNS which points to all of your primaries (DNS Round Robin). Then you can use this alias name to configure a custom deployment package on one of your primary servers.

This configuration makes agent deployment very flexible and you can use single name in all of your packages.

2.12.1.1 Disabling Certificates Verification

To avoid a certificate verification dialog coming up during install or registration it might be useful to disable this.

For disabling, the following registry key should be set before agent deployment:

[HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Zenworks]

"require-verified-certs"="false"

2.12.2 Agent Deployment with ZCC

If you want to use this deployment method:

- Discover your devices or import them (based on segments, buildings or sites).
- Create discovery tasks based on your folder structure (one for each folder). You have to know which device belongs to which site.
- Use your registration rules within these tasks.

This can only be done, if you know all passwords of your devices, which is usually not the case.

2.12.3 Agent Deployment with Existing Tools

The easiest way to deploy the agent is to use an existing distribution tool.

- Create a standalone or network deployment package (Custom Deployment) which registers the device to a folder named “New Devices” (-> Custom Deployment Package).
- Run “ZAC unr” to delete default registration.
- Run “ZAC register -k MYKEY <URL of the server> -u UserName -p PASSWORD” to register the device to the preferred folder. In this case you can use a DNS-Alias as the server URL.
- You have to provide an administrative account of your zone to register the device.
- Use this package within your existing tool (login script, Group Policy, NAL, SMS)

2.12.4 Agent Installation with a New Image

For new installations it's recommended to include the ZCM agent in a new image.

- Create a standalone deployment package which registers the device to a folder named “New Devices”.
- Use this deployment package during setup process to install the agent.
- All newly installed devices will register to “New Devices” folder.
- Run “ZAC unr” to delete default registration.
- Run “ZAC reg -k MYKEY <URL of the server> -u <USERNAME> -p PASSWORD” to register the device to the preferred folder. In this case you can use a DNS-Alias as the server URL.
- You have to provide an administrative account of your zone to register the device.

Within the above scenario it's possible to deploy the agent without creating more than one deployment package for your enterprise.

Novell recommends using a special user to register new devices. This user only has the rights to register devices (See Administrative Accounts).

2.13 Using System Update

ZCM provides a new feature called “System Update” which is used to download and install Support Packs, Patches and Product Recognition Updates (PRU).

For this function to work properly all primary servers in your zone must have an Internet connection to detect and download new Updates.

In the current version of ZCM (10.0.1) Updates are randomly assigned to a server. It's not possible today to configure a special update server that is responsible to download the required updates. After applying SystemUpdate1 (10.0.2) it´s recommended to nominate a given primary server to download system updates.

For internal distribution to primary servers and devices in your IT environment it is highly recommended to use staging groups for the updates.

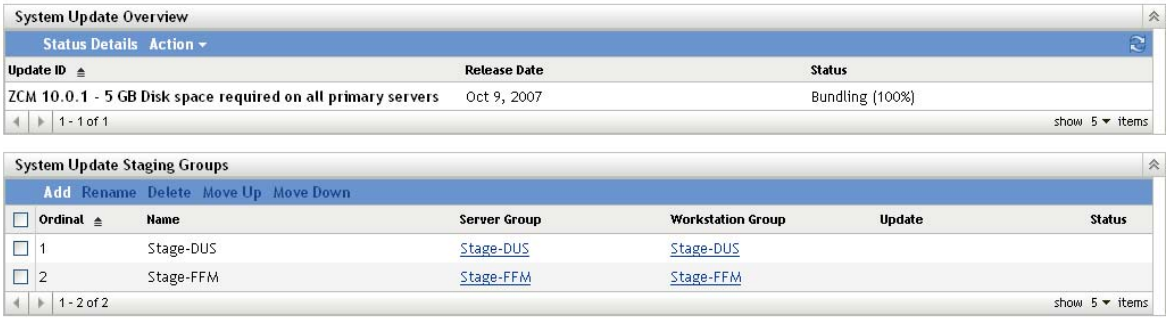

Figure 17: System Updates

Novell®