Desktop Management With Sun Ray™ Software

May 2006

Table of Contents

Introduction....4
Sun Desktop Manager Architecture....5
Sample Scenario....7
Sun Desktop Manager Installation....9
Sun Desktop Manager Configuration....10
Server Configuration....10
Client Configuration....15
Brief Overview of the Administration User Interface....15
Controlling the Desktop Settings....17
Staging....22
Using Sun Desktop Manager to Improve Desktop Performance....25
Links of Interest....25

Introduction

For several years, Sun Ray clients and Sun Ray Server Software have given organizations the opportunity to implement a desktop service delivered through the network.

Having a desktop service is appealing as it provides the following main advantages:

- **High availability:** The user is not tied to one particular desktop device, and the servers that provide the session for the user can be clustered to provide a service with high availability.

- **Security:** The Sun Ray environment offers a high degree of security by providing encrypted communications and server authentication (supporting the use of smart cards for user authentication), by being able to disable access to the USB ports, and by providing a Controlled Access Mode configuration in which only a restricted set of applications are available. Combined with the Trusted Solaris™ Operating System, this can be used to provide a desktop that supports different security access levels, restricting the possibility of copying information from a higher security level to a lower security level.

- **Reduced total life cycle costs:** Sun Ray clients don't require per-unit management as they are plug and play (no software installation or configuration is required). They lack moving parts, like hard disks, or fans, so the mean time between failures (MTBF) is higher than for many other desktop systems. They do not become obsolete because they don't need additional RAM or CPU power. Sun Ray clients are environmentally friendly as they don't produce noise and the power consumption is very low compared to traditional systems. The administration workload required to manage a Sun Ray environment is greatly reduced -- instead of managing each device, only the servers that provide the sessions should be managed, and one server can provide sessions for hundreds of users.

- **Backup policies for user data:** Backup policies are easy to implement. Only the servers that hold user homes should have the backup agents installed.

With these benefits, Sun Ray technology provides a way to reduce costs and administration workload in the desktop infrastructure. Still, some improvement is possible in reducing the overhead in managing user desktops.

The basic idea behind managing user desktops is to provide a tool that allows administrators to centrally define and configure user desktop settings in an easy way, providing default configuration values or locking down configuration values (which users cannot change) for desktop applications.

Sun Desktop Manager provides this management capability. Here are its main features:

- Ability to define default configuration values or enforced configuration values for the following:
  - GNOME desktop
  - GNOME-based applications that use the GConf configuration management system
  - StarOffice software
  - Mozilla software
  - Applications based on Java technology that use the Preferences API
- Lockdown facilities
  - Panel configuration: Prevents a user from changing the panel configuration
  - Access to terminal: Restricts user access to a command-line terminal
  - Lock screen: Removes the lock screen from the launch menu
  - Logout: Removes the logout from the launch menu
  - Application launching and application list: Prevents a user from launching an application that is not contained in the Allowed Applications list
  - Force quit: Disables ability to force quit an application
  - Disabled Applets: A list of applet IDs ignored by the panel (adding an applet name to the list prevents that applet from loading or showing up in the menu)
- Desktop launchers and menu entries
- Startup applications
- Offline operation

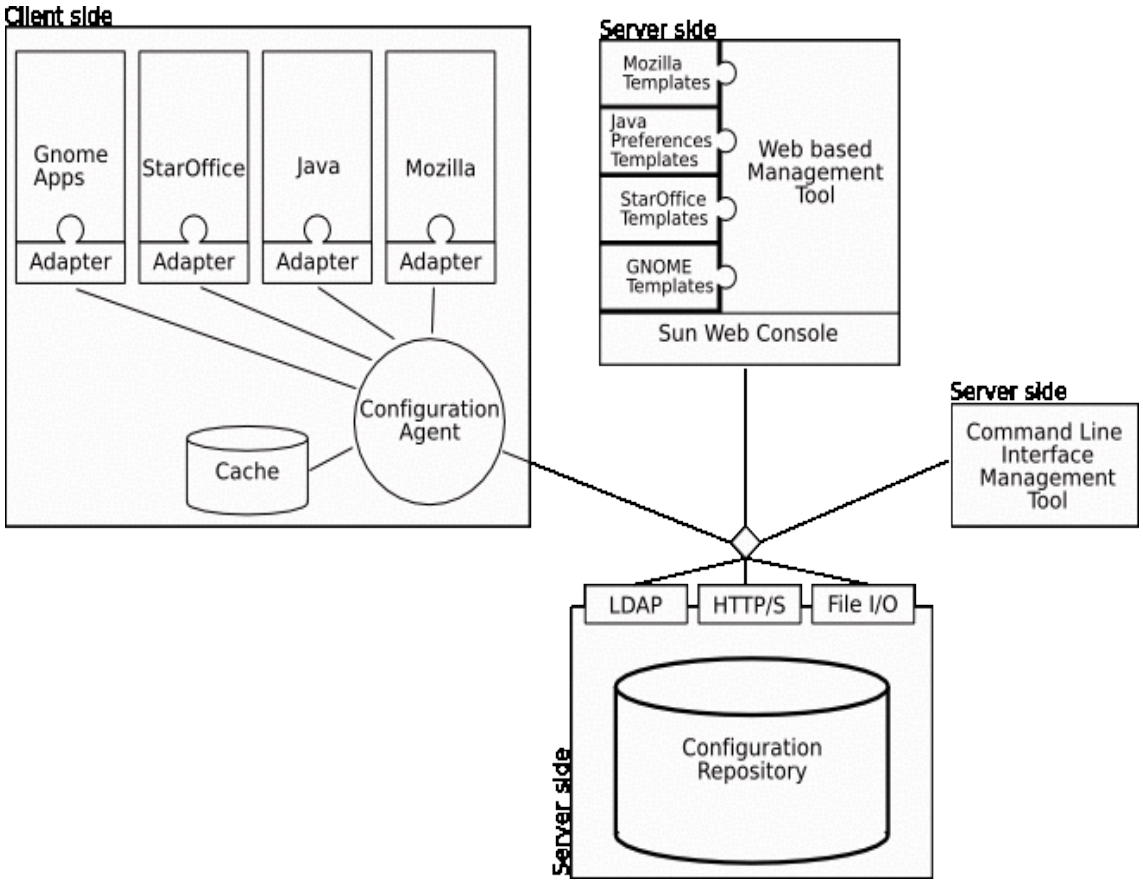
Sun Desktop Manager is a component of the Sun Ray Software 4 product. For more information, see http://www.sun.com/software/sunray/.

Sun Desktop Manager Architecture

Sun Desktop Manager includes three different components:

- Configuration Repositories: These store the configuration policies and organizational structure (including users and hosts).
- Management tools: These create, modify, delete, or assign configuration policies.
- Agent and adapters: The agent fetches the configuration settings from the Configuration Repositories, and the settings are applied using the adapters. The agent and adapters are installed on every client.

See the following diagram for more details.



For more details about the Sun Desktop Manager architecture, please read the *Sun Desktop Manager Administration Guide*.

Sample Scenario

Let's take a quick look at the features provided by Sun Desktop Manager, to see how it can be used to reduce the administration and support workload in a production environment.

Suppose that our requirements are to provide a desktop infrastructure for 500 users with high availability in the desktop service.

The 500 users can be categorized into five different groups: Marketing, Sales, Engineering, Human Resources, and Finance.

A set of applications are specific to each one of these groups, and applications can also be categorized based on the type:

- Solaris native applications: The binaries/libraries must be available on the server that will execute the application.
- Windows native applications: The binaries/libraries are installed on some Windows servers running terminal services.
- Standalone Java applications: This type of application can be deployed on the server that will execute the application.
- Java Web Start applications: These applications reside on a web server, but are downloaded/updated on demand and executed on the server hosting the user session.
- Web-based applications: This type of application has a browser-based interface and is deployed in servers and served using http or https protocols.

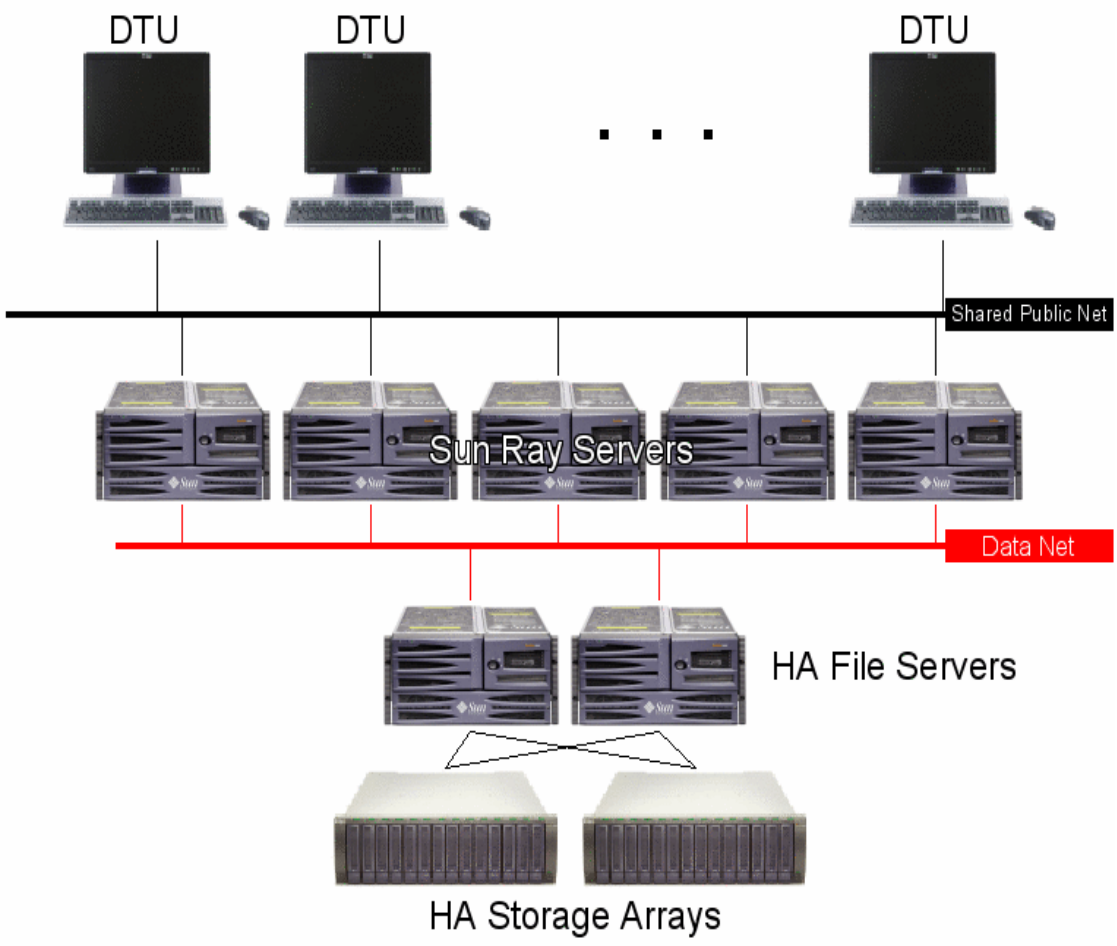
In our scenario, the company wants to provide an easy way to access these types of applications for the different categories of users, depending on the roles the users have.

The company already has an LDAP infrastructure which holds the identities for all users.

Let's see how those requirements can be fulfilled with Sun Ray technology and Sun Desktop Manager.

First of all the Sun Ray infrastructure needs to be deployed, with Sun Ray Software-enabled servers (hereafter referred to as "Sun Ray servers").

The following diagram shows a typical high-level architecture that fulfills the requirements.



The HA File Server will hold the user home directories so that no matter which Sun Ray server users connect to, they will always have their data available. This HA file server also stores the native applications and standalone Java applications. All Sun Ray servers will mount the shared application directory:

```
/usr/shared on filesrv:/usr/shared
remote/read only/nosuid/bg/intr/hard/xattr/dev=45c0020
```

All Sun Ray servers are configured to use the LDAP name service, and all users are managed in a unified LDAP server that stores all company users.

All five Sun Ray servers are configured in a failover group, with all desktop terminal units (DTUs) connected to a shared LAN.

A data network interconnects the Sun Ray servers with the file servers.

The installation and configuration of the Solaris OS, LDAP naming services, Sun Cluster, and Sun Ray Server Software are beyond the scope of this paper.

Sun Desktop Manager Installation

As described in the Architecture section, Sun Desktop Manager requires a client on each system to be managed and a server installation (only one is required, although the server side can be deployed on more than one system).

- Client installation:
    - The sample scenario shows five Sun Ray servers. Sun Desktop Manager's client components should be installed on each of them.
    - Please read the Sun Desktop Manager release notes and apply all required patches before proceeding with the installation.
    - Download the client component files.
    - Unzip and execute the setup script.
- Server installation:
    - The server component can be installed in one or more servers, but only one is required. Let's suppose that we have a dedicated server to install it (this is not a requirement, but is preferable).
    - Please read the Sun Desktop Manager release notes. Apply all required patches and install Sun Web Console 2.2.5 if required.
    - Download the server component files.
    - Unzip and execute the setup script.

Sun Desktop Manager Configuration

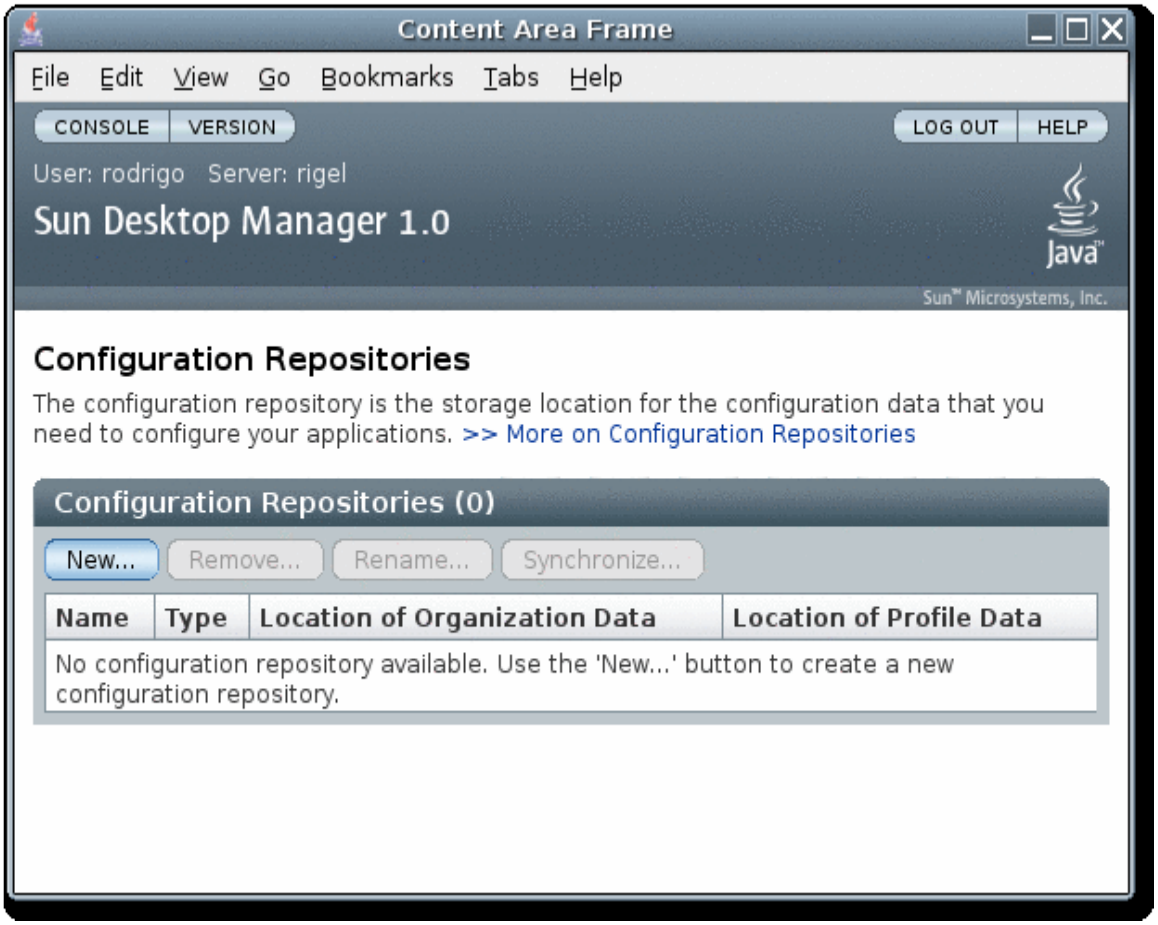
Server Configuration

The first thing to do is to create a Configuration Repository. Configuration Repositories are managed in the Sun Web Console.

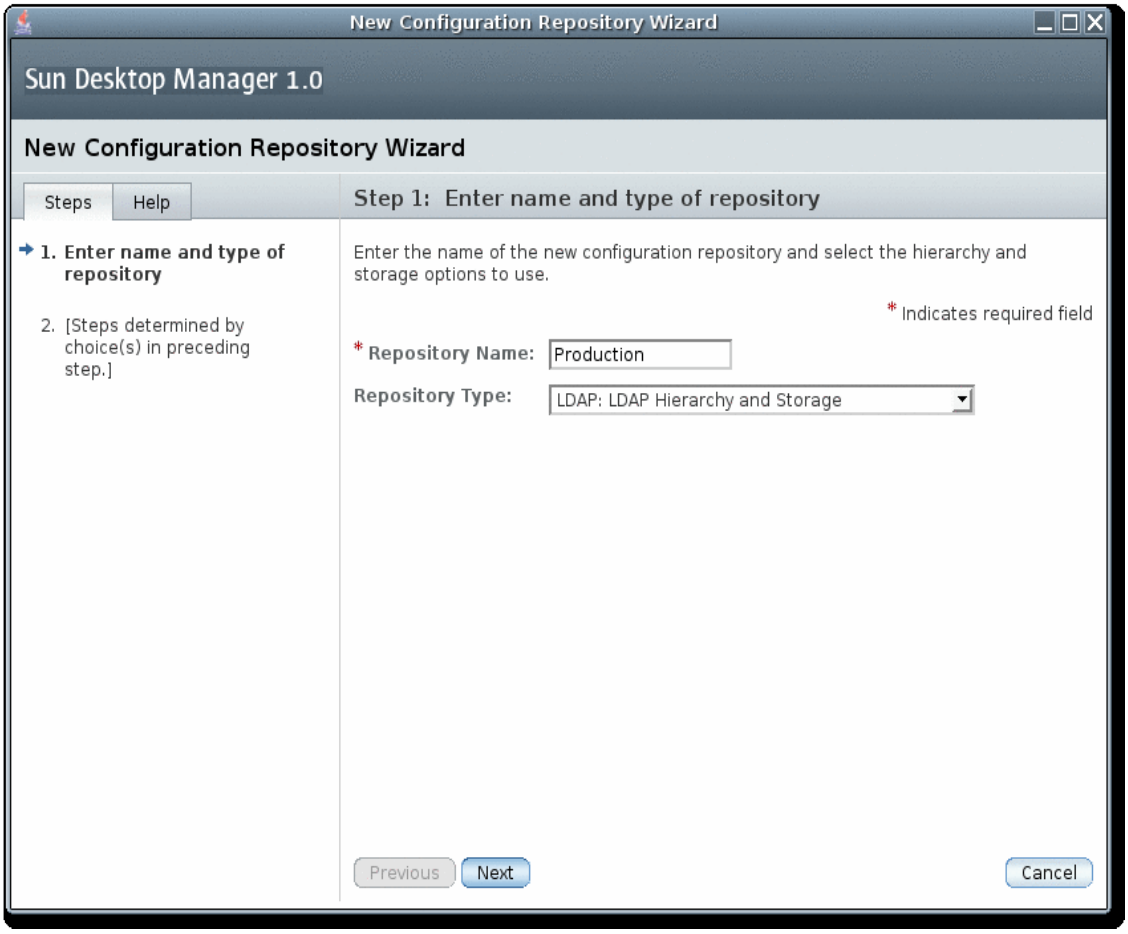
Point your browser to the server where you installed the server side of Sun Desktop Manager, for example `https://<server name>:6789`.

Log in to the console (any UNIX® user will work). If you have the LDAP naming service configured, any LDAP user will work, too.

In Desktop Applications, click on Sun Desktop Manager and you will see the Configuration Repositories window.



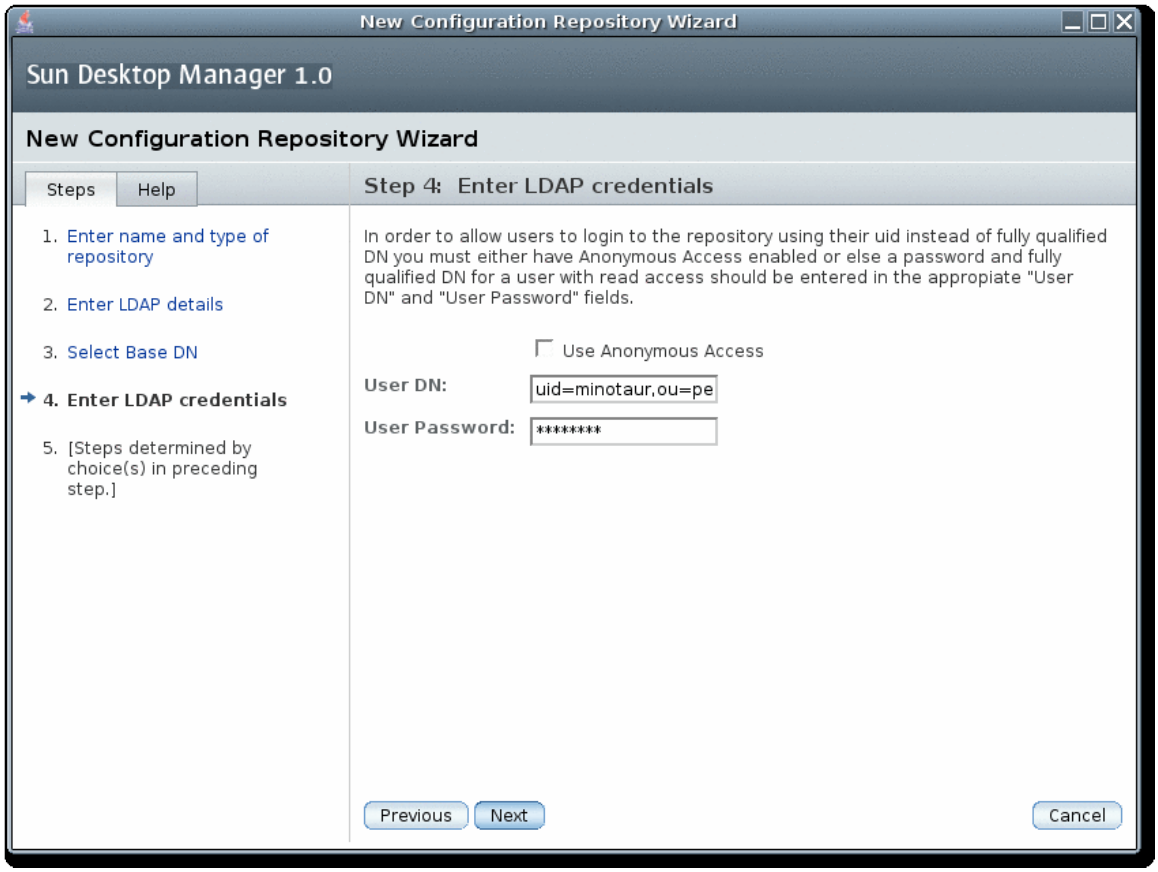
As there is no Configuration Repository, one should be created. Click on New.



Create a new Configuration Repository called Production that is based on LDAP.

Follow the wizard -- In Step 2, type in the server name and port. In Step 3, select the base DN that contains the organization and domain.

To allow the Desktop Manager components to map a UNIX user identifier to an LDAP entry, searches in the LDAP directory need to be performed. By default these searches will be done using anonymous access. However, if anonymous access is disabled on your LDAP server, you need to provide in Step 4 the full DN and password of an LDAP entry that has read/search/compare rights on the directory.

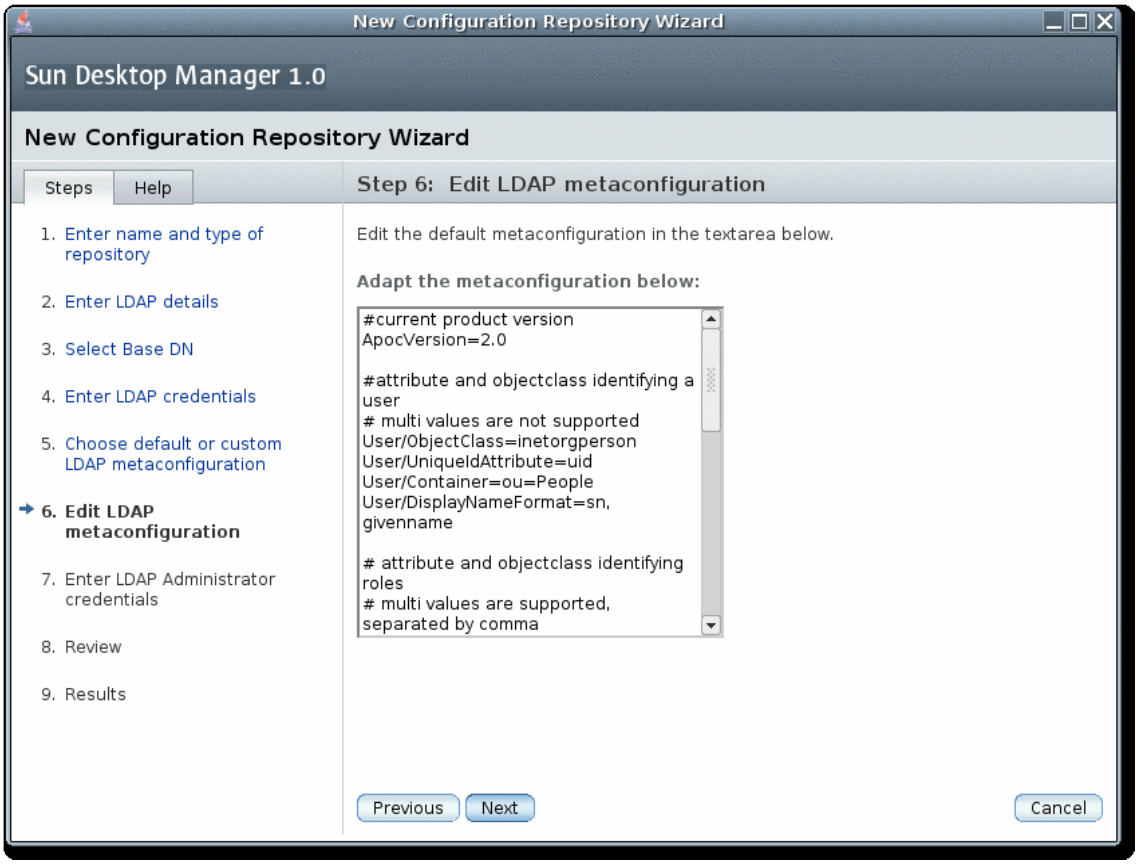


Sun Desktop Manager stores data in the LDAP server. To adapt Sun Desktop Manager to the structure of the LDAP server, a mapping between Sun Desktop Manager data and LDAP objects should be defined. As the LDAP directory has never stored any Configuration Repository data before, mapping information (called meta configuration) should be created and stored in the LDAP directory. In Step 5 select Yes and proceed.

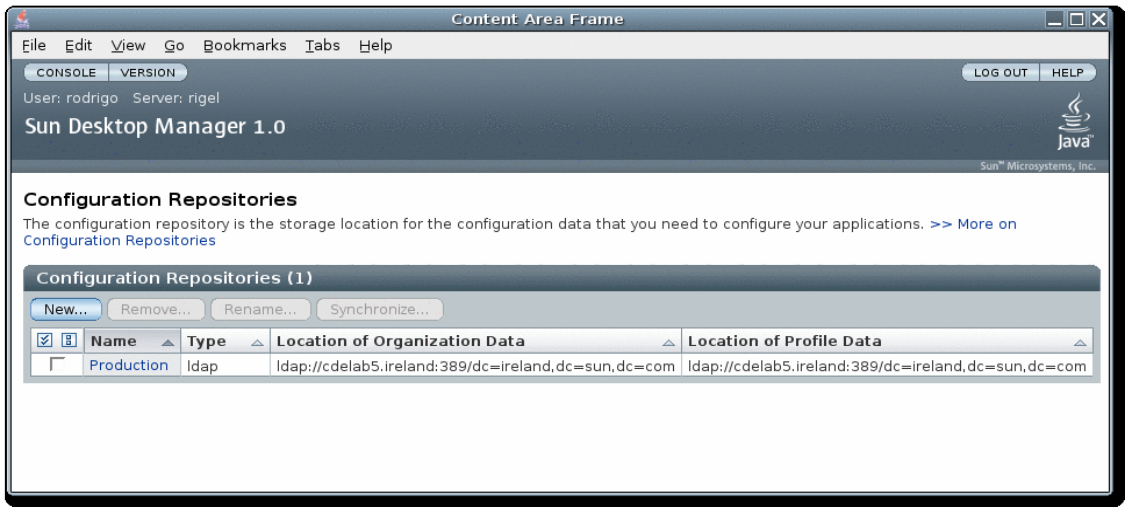
In Step 6 you will be given the opportunity to modify the mapping to LDAP objects. It is very important that you adapt this information to match your LDAP contents, otherwise the tool will not be able to show the hierarchy of users/hosts, organizations, and domains properly.

If this is the first time you have used a particular LDAP server to hold a Configuration Repository, the schema should be extended before the meta configuration can be installed. This step can be done automatically by the wizard if the LDAP server is a Sun Java System Directory Server. In that case, in Step 7 credentials with administrative rights will be required.

In Step 8 you will have a chance to review the settings. Click on Finish after reviewing the settings. (See the following figure for Steps 5 through 8.)



A Configuration Repository is now available (see the following screen capture).



Client Configuration

After the installation, the client should also be configured to define the Configuration Repository that will be used to fetch the profiles as well as other things such as poll intervals and log verbosity.

To start the client configuration wizard, run `apoc-config` as root on each Sun Ray server.

In the first page of the wizard, be sure to check the Active checkbox. Be sure that the Host identifier matches the elements that are stored in the Configuration Repository (host names or IP addresses). In the sample scenario the Configuration Repository is stored in LDAP, so be sure to select the appropriate Context Type (LDAP in this case).

In the second page, type the LDAP server information so that the agent can query the Configuration Manager.

The default settings in the next screen should be acceptable. On the fourth page it may be interesting to lower the General Detection Interval if you plan to do a quick evaluation, but do not do it in a production environment. This value defines the poll interval the Agent will use to query the Configuration Repository for changes.

Follow the wizard and finish the configuration.

Check if the agent is running with this:

```
svcs apocd/udp
```

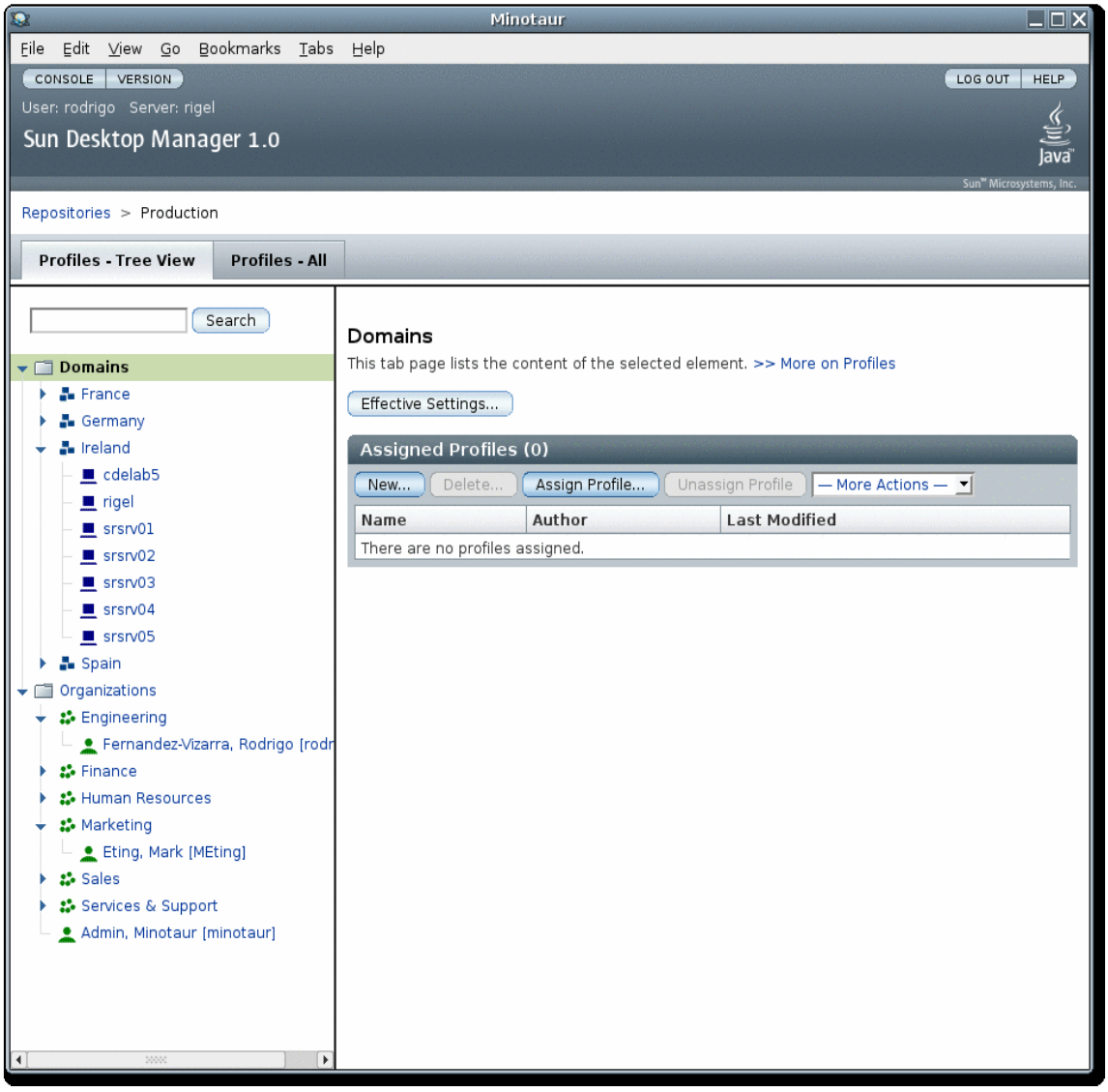
If the agent is not running, start it with this:

```
svcadm enable apocd/udp
```

Brief Overview of the Administration User Interface

To access the management tool, log into the Sun Web Console, and start Sun Desktop Manager by clicking on the link labeled Sun Desktop Manager. Select the Configuration Repository with which you want to work (Production).

The Profiles – Tree View provides a view of how configuration profiles are assigned to the different elements (users, hosts, domains and organizations).



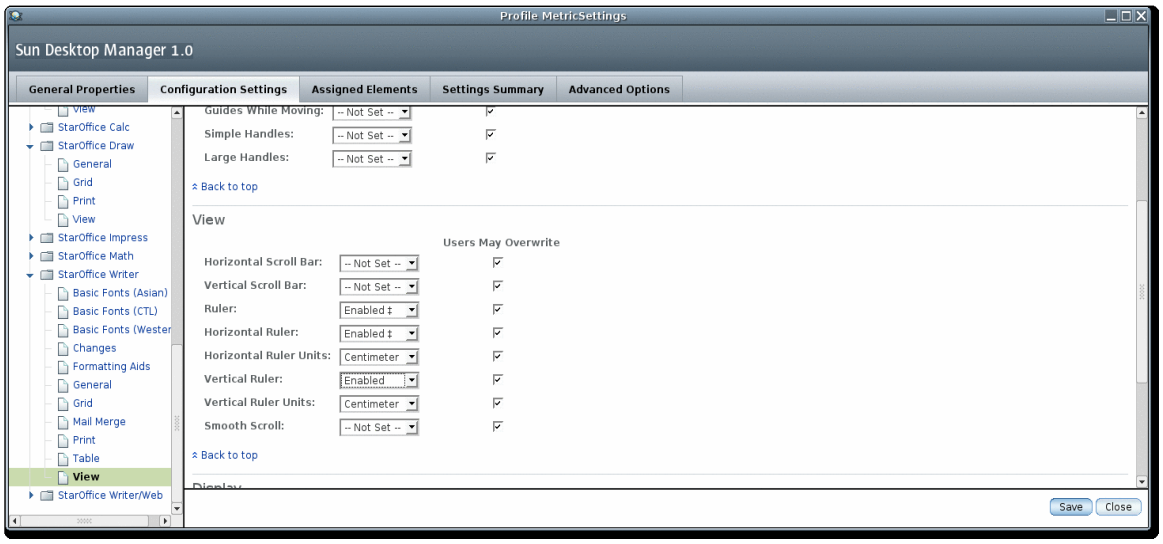
On the left side of the page there is the Navigation Tree, divided in two parts, Domains and Organizations. With this view it is possible to browse the tree to see the profiles assigned to different elements. The Navigation Tree could contain large amounts of data. To make administrators' lives easier, a *Search* facility is provided so they can quickly locate any element in the repository.

On the right side of the page there is a view of the assigned profiles (directly assigned or inherited from any parent element) of a selected element in the Navigation Tree. It is possible to assign, unassign, rename, copy, move, import, and export profiles in this window.

The Effective Settings button will show a list of all settings that apply to that element. All settings defined in any parent element will be merged with the profiles directly assigned to the actual one. The results will be shown in a different page. This provides a quick way to see what configuration settings will be applied to specific users, hosts, groups or domains.

The Profiles – All tab provides a list of all available profiles divided in Domain and Organization categories.

When a new profile is created or modified, a new window pops up. This window is the Profile Editor.



Under the Configuration Settings tab, a Navigation Tree is available. This tree shows a categorization of the configuration settings available. The settings for a particular category are displayed on the right side of the page.

Controlling the Desktop Settings

Let's focus now on defining some profiles to fulfill the requirements described in the Scenario section.

In most situations, access to the Internet is provided via proxies (for different protocols). A profile that configures the proxies for the desktop applications eliminates the need for users to do it themselves, and thus reduces the possibility of mistakes that can increase the number of calls to the support center.

Suppose that in the sample scenario, the Sun Ray servers are located under the Ireland domain, and that there is a proxy server in that domain called `webproxy.ireland`. This proxy handles http/https and ftp protocols.

As we want these settings to be the default for all systems in the Ireland domain, the profile will be created and assigned to the Ireland domain element. In the Navigation Tree browse to the Ireland Domain, and then click on New.

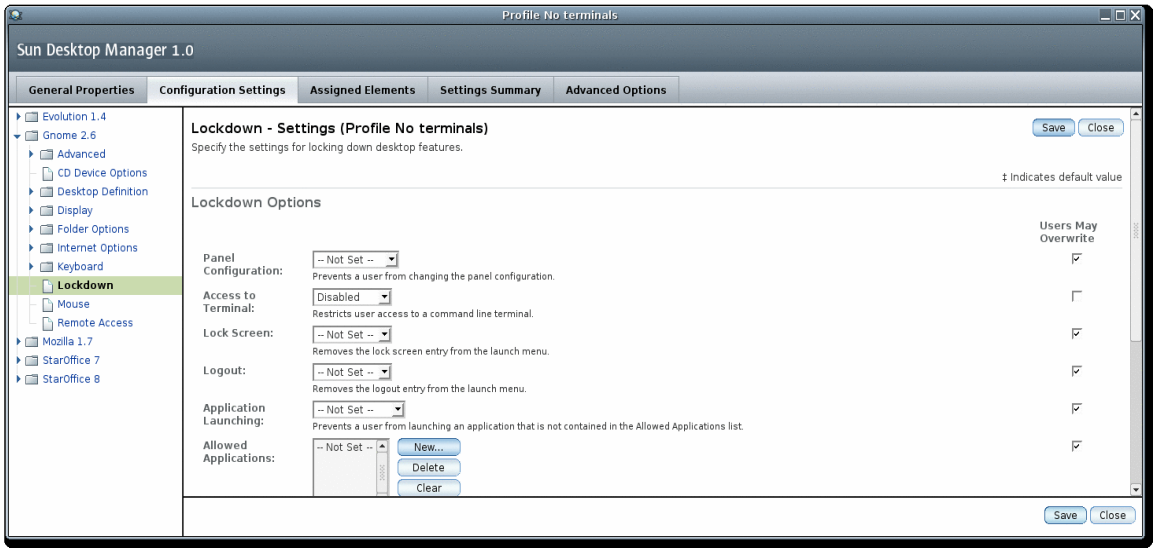
After giving a meaningful name to the profile and clicking on Save, go to the Configuration Settings Tab. In the Navigation Tree that is available on the left side of the page, browse to the Proxy Settings under GNOME 2.6/Internet Settings and fill in the form with the proxy configuration.

This profile will create a default proxy configuration for all users that have a session on any of the Sun Ray servers (`srsrv01-srsrv05`). This configuration is not enforced, as the users may override the configuration by themselves. If you want to avoid this, de-select Users May Override and the configuration will be enforced (users will not be able to change it). This may be useful again to reduce the risk of users changing configurations and generating support calls as a result.

Another common requirement is that users shouldn't be able to execute some applications, the most common one being the terminal.

Using the lockdown features of Sun Desktop Manager, it is possible to create lockdown profiles. In this case we don't want Sales staff to open a terminal since all the applications they need for their tasks are delivered through web-based interfaces.

Let's create a profile that restricts access to terminals. This time go to the Profiles-All tab in the main page, and in All Organization Profiles create a new profile by clicking on New.



The Lockdown configuration form is located under the GNOME 2.6 category. Set the Access to Terminals to Disabled, untick Users May Override and Save.

Now we have a profile that disallows access to terminals, but it is not assigned to any element. In the Assigned Elements Tab it is possible to assign the profile to different elements. We will assign it to all groups except the Services & Support and the Engineering ones (since these users may need to perform command-line operations).

With those two simple profiles, you have an idea of how Sun Desktop Manager can provide useful settings that reduce the administration workload needed to provide a usable desktop environment. Every time a new user is created in the LDAP server, all applicable profiles will be taken into account automatically.

Now you are familiar with how to create profiles that provide desktop configuration settings. The next step is to provision user desktops with application launchers. The goal is to make applications easily available to users depending on their role in the company.

Native and Standalone Java Applications

These will be installed on the file server, and the directories containing them will be exported to each Sun Ray server. In this way, the application is deployed in only one place, but is available to all users on the Sun Ray server. After that, we create a profile that contains a desktop launcher (an icon on the desktop that starts the application) and another profile that contains a menu entry. Of course

one profile can contain one or more desktop launchers and/or menu entries, so if a user role requires a lot of applications, all of them can be defined in one profile.

Web-Based Applications and Java Web Start Applications

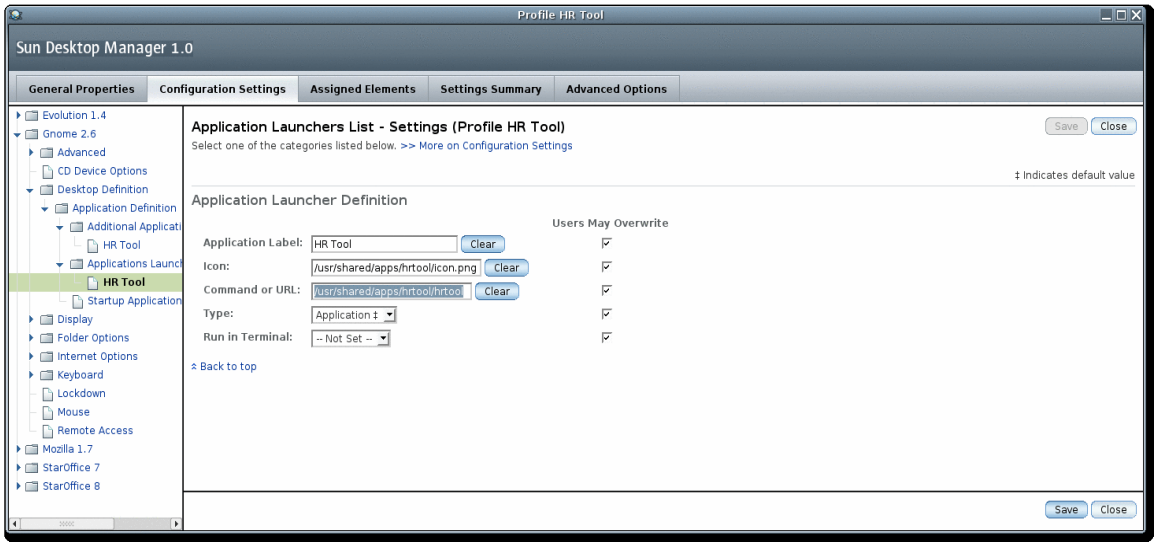
These applications are defined using a URL. To create a launcher or menu, follow the same procedure as in the native and standalone Java applications, but select Link Type.

Windows Applications

Again, the same procedure should be followed. The type should be Application, and the Command should use the `uttscwrap` command (installed in `/opt/SUNWuttscwrap` by default).

Let's create a launcher and menu entries for an HR Tool that is installed on the file server.

As for any other setting, you have to create a profile (or modify an existing one).

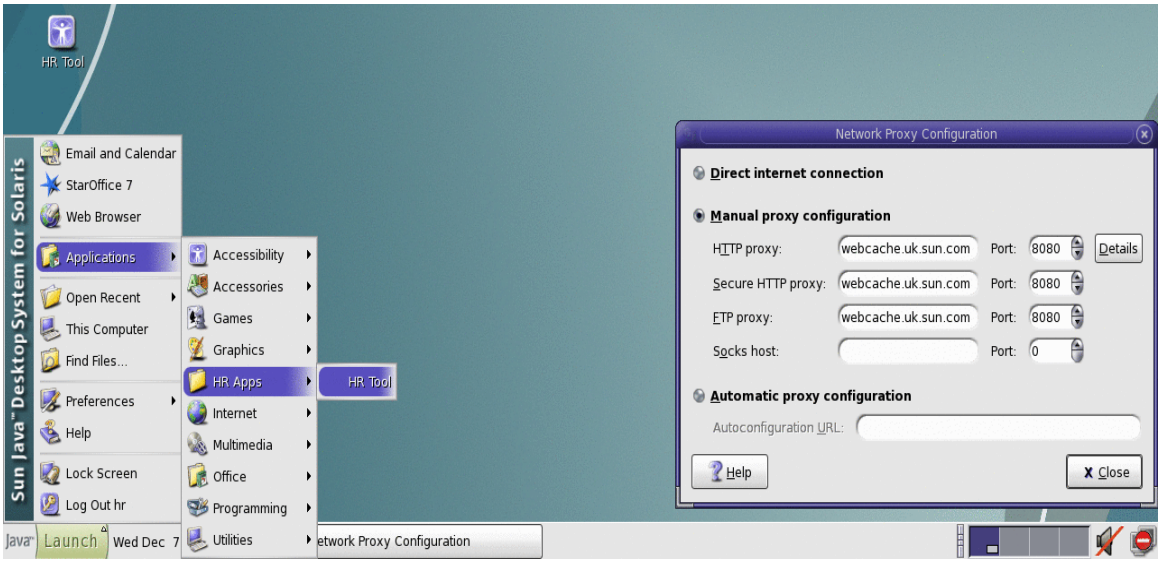


If you are not willing to wait until the agent refreshes the cache (60 minutes by default) you can force the agent to query the Configuration Repository for changes by running the following command as root:

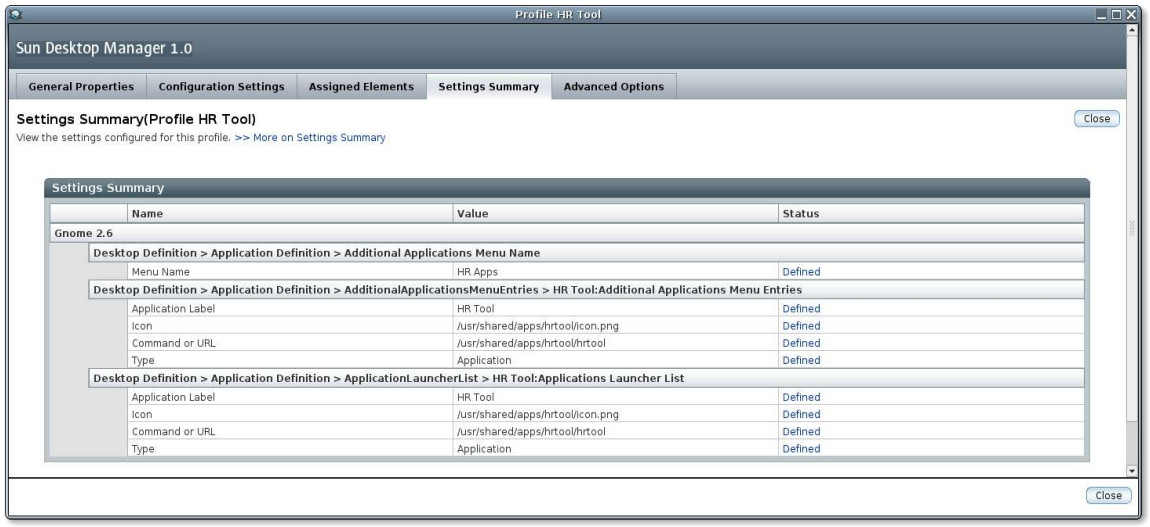
```
/usr/lib/apoc/apocd change-detect
```

You will see how the new settings are applied in real time to user desktops.

The following screen capture shows how the configuration settings for a user in Human Resources are applied.



The list of settings applied to the user is shown here in the Profile Settings Summary.

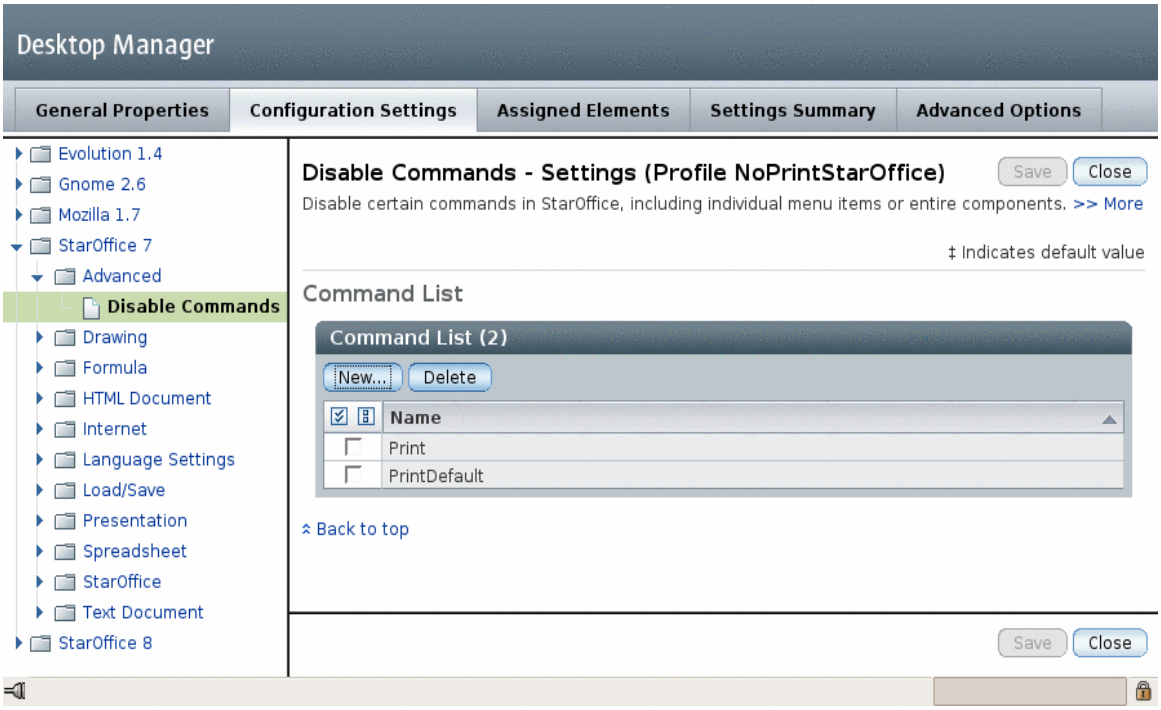


Another interesting use case for Sun Desktop Manager is to restrict StarOffice functionality to some users.

Suppose that the organization doesn't want to allow some users to print StarOffice documents. Using Sun Desktop Manager it is possible to disable functionality that it is ordinarily available to users. To restrict access to the *print*

functionality in StarOffice software go and create or modify a profile. In the profile editor go to StarOffice 7/Advanced/Disable Commands and click in the button labeled as New in the Command List. When the pop-up window appears, type *Print*. Add also the *PrintDefault* command to the list to disable the print icon in the tool bar.

Print and *PrintDefault* are the commands that you want to disable from StarOffice software.



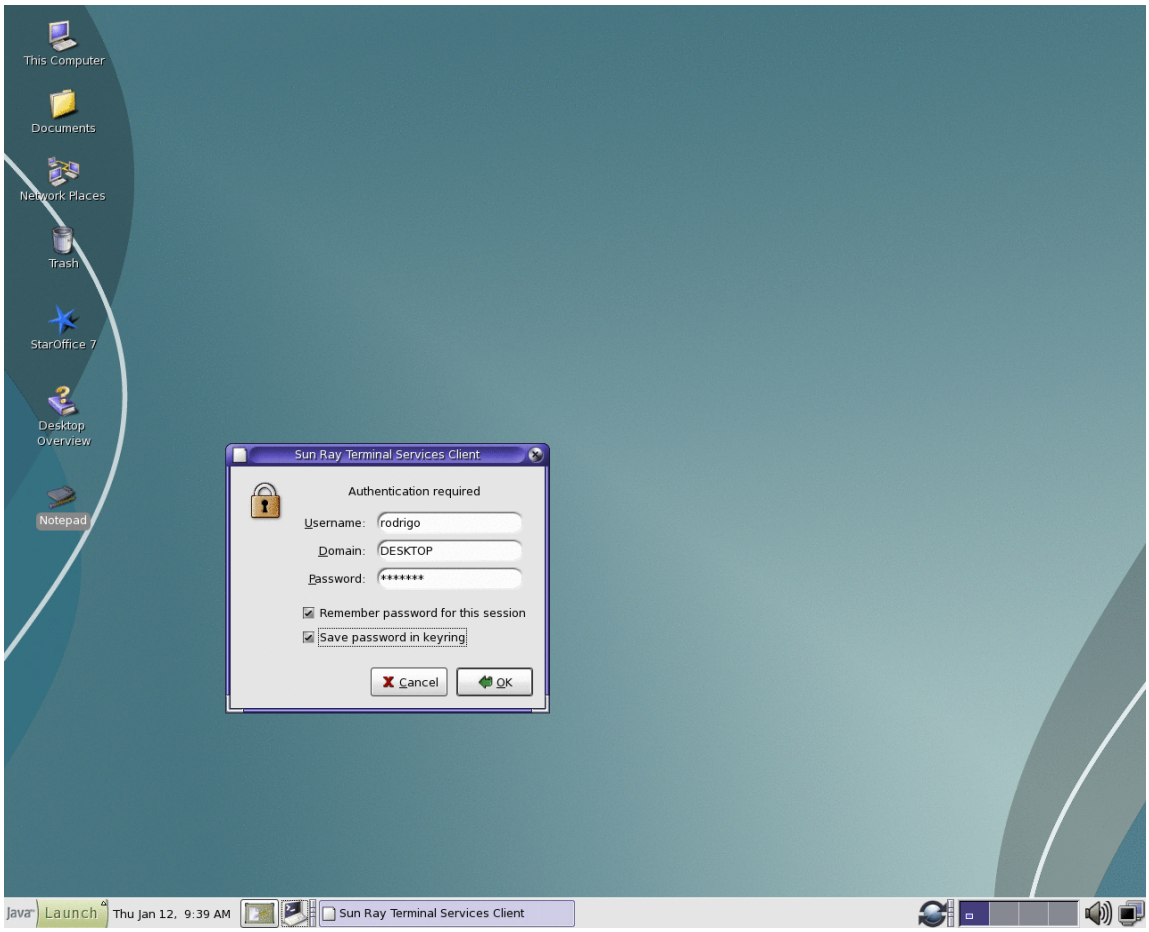
For a list of available commands, consult the StarOffice Administration Guides:

- For StarOffice 7.0 software, the section "List of StarOffice Slot Id Command Names" offers a list of commands that can be disabled.
- For StarOffice 8.0 software, go to the section "Appendix A Index of UNO Command Names for StarOffice 8".

Windows applications are of special interest, as some tools are not available in a UNIX environment. For this type of application, the Sun Ray Connector for Windows OS can be used to execute a Windows application from a remote server and have it displayed on a Sun Ray client's terminal. As described before, the procedure to deploy launchers for this kind of applications is the same as any other launcher: Create a profile that contains a launcher with the appropriate command line to start the remote session.

The Sun Ray Connector for Windows OS provides one extension for the Sun Ray desktop that can make the Windows integration experience smoother by providing a password caching mechanism. Users will not be required to type in the password every time they start a new Windows application. The password caching can be persistent or session only. To enable the password caching, use `uttscwrap`.

The following screen capture displays a user belonging to the Engineering group, for which we created a launcher to Notepad.



Staging

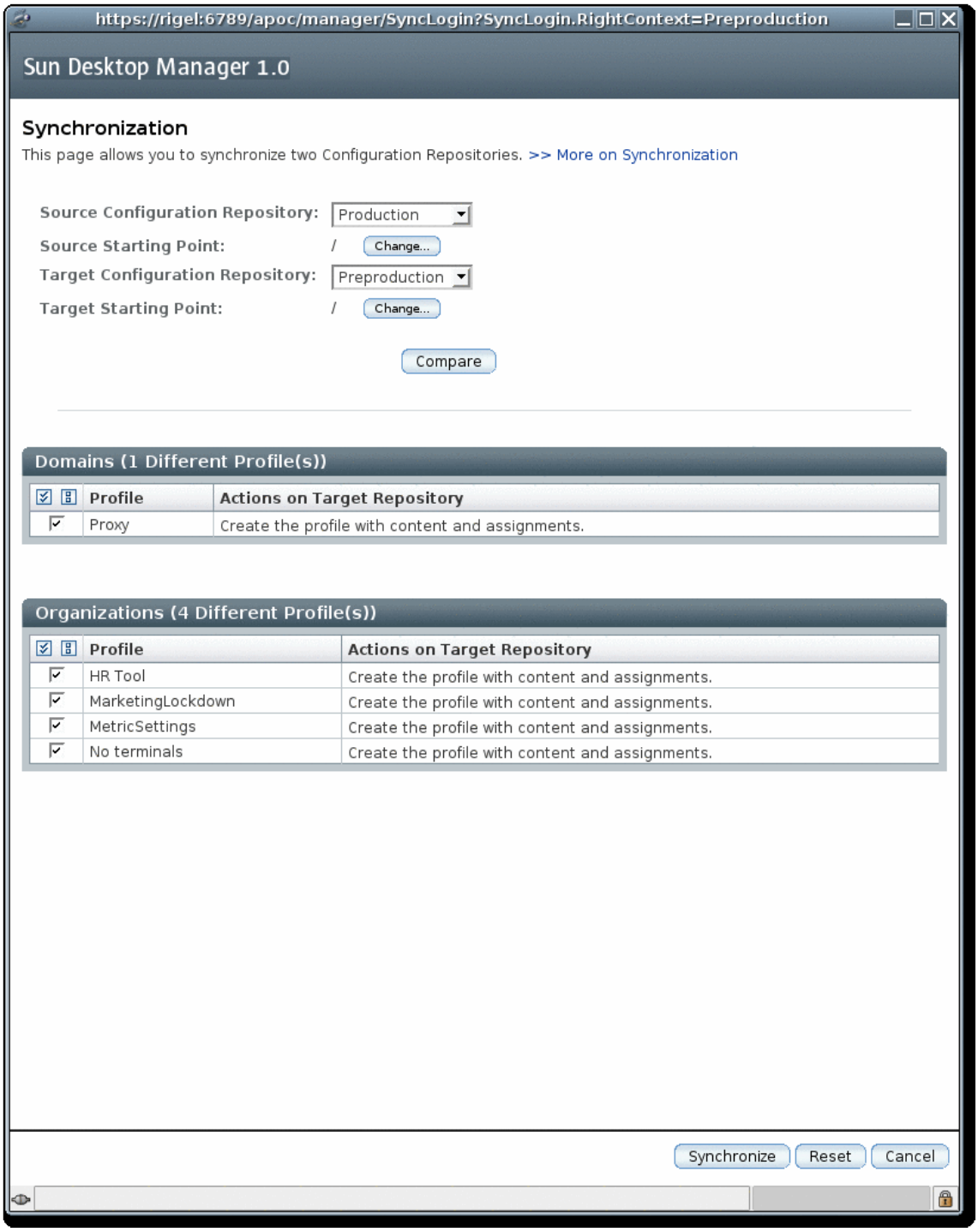
Now that you have the knowledge to manage user desktops in a Sun Ray environment, it is time to go to production. However, you may want to have a preproduction environment where you can test new profiles without going directly to production with them.

What you should do is create a new Configuration Repository to hold the preproduction profiles, configure a Sun Desktop Manager agent on a separate machine to query the new Configuration Repository, and test all profiles. Once you are satisfied with the setup, you can synchronize the preproduction profiles with the production profiles.

Create a new configuration repository with the same structure as the production one, and call it preproduction. If you already have profiles that you want to keep in the production environment it would be a good idea to synchronize both repositories first and then work on the preproduction one.

To do so, first create the preproduction repository, following earlier instructions. Then in the Configuration Repositories page, select production and click on Synchronize. In the Synchronization page, select preproduction as the target Configuration Repository and click on Compare. Select the profiles that you want to synchronize (all of them) and click on Synchronize.

After the last step, both Configuration Repositories contain the same profiles. If you need to modify or add any new profile, you should do it in the preproduction environment, and after testing you can synchronize the preproduction and production Configuration Repositories again (see the following screen capture).


https://rigel:6789/apoc/manager/SyncLogin?SyncLogin.RightContext=Preproduction
Sun Desktop Manager 1.0
Synchronization
This page allows you to synchronize two Configuration Repositories. >> More on Synchronization
Source Configuration Repository: Production
Source Starting Point: / Change...
Target Configuration Repository: Preproduction
Target Starting Point: / Change...
Compare
Domains (1 Different Profile(s))
Profile
Actions on Target Repository
Proxy
Create the profile with content and assignments.
Organizations (4 Different Profile(s))
Profile
Actions on Target Repository
HR Tool
Create the profile with content and assignments.
MarketingLockdown
Create the profile with content and assignments.
MetricSettings
Create the profile with content and assignments.
No terminals
Create the profile with content and assignments.
Synchronize
Reset
Cancel

Using Sun Desktop Manager to Improve Desktop Performance

Some desktop settings can improve performance in a Sun Ray environment. The good news is that almost all of them can be enforced by the administrator using Sun Desktop Manager.

Configuration settings that can improve the performance of a Sun Java Desktop System session over Sun Ray clients are described in the article "Sun Java Desktop System 2.0 Optimization for Sun Ray Server Software 3.0" at http://www.sun.com/bigadmin/content/submitted/jds_optimize.html.

A zip file containing a sample profile with the configuration settings can also be downloaded from the article. Import the profile into the manager as follows:

1. Log into the administration console.
2. Select the Configuration Repository; remember that it is a good idea to use the preproduction one first.
3. In the sample scenario case we are interested in importing it and assigning it to the Sun Ray servers. In the Profiles - Tree View select one of the Sun Ray servers and in the More Actions pull-down menu, select Import, select the zip file with the profile, and click Import.
4. Select the other Sun Ray servers and assign the profile by clicking on Assign Profile and selecting the profile that contains the optimization settings. Note that you only have to import the profile once.

Links of Interest

Sun Ray Software 4: http://www.sun.com/software/sunray/documentation.jsp

Sun Desktop Manager Installation Guide, Administration Guide, and Developer Guide: http://docs.sun.com/app/docs/coll/1230.4

Sun Ray Server Software 4 Collection: http://docs.sun.com/app/docs/coll/1230.4

StarOffice 7 Administration Guide: http://docs.sun.com/app/docs/doc/817-1820

StarOffice 8 Administration Guide: http://docs.sun.com/app/docs/doc/817-7496

Sun Java Desktop System 2.0 Optimization for Sun Ray Server Software 3.0: http://www.sun.com/bigadmin/content/submitted/jds_optimize.html