

# TNG Linux

From the Desktop to the Data Center

**Torsten Hallmann**  
Technology Specialist  
Novell (Schweiz) AG

**Andreas Pfenninger**  
Linux Sales  
Novell (Schweiz) AG



**Novell®**

# Agenda

- Introduction
- SUSE Linux Enterprise Server
  - Binary Drivers, High-Availabilty, Virtualization, Application Security, Lifecycle Management
- SUSE Linux Enterprise Desktop
  - Office Automation, File Formate, 3-D GUI
- Questions & Answers



# SUSE Linux Enterprise Server

# *SUSE® Linux Enterprise Server 10*

## Feature Highlights

### • **Virtualization**

- Xen 3 for x86, SMP, PAE and 64-bit
- YaST integrated

### • **Security**

- Application Security
- EAL4+ goal
- Network detection, monitoring

### • **Administration and Management**

- Admin tools
- Novell® Customer Center
- Pattern deployments
- CIM providers

### • **Performance and Scalability**

- Up to 15% improved performance
- 1024 CPUs, 10+TB Memory

### • **Storage & HA**

- OCFS2, EVMS, Heartbeat 2
- iSCSI Target and Initiator
- DRDB for Disaster Recovery
- Multipath – Resiliency

### • **Application Developer Services**

- Single SDK shared with SLED10
- glibc 2.3.90, GCC 4.1.0, GDB 6.4
- Web 2.0 enabled
- Mono® runtime and tools
- Apache Geronimo included

### • **Hardware and New Driver Process**

- x86, x86-64, ia64, ppc, ppc64 and s390x
- New storage, network & graphics drivers
- Hotplug improvements
- Device persistent naming

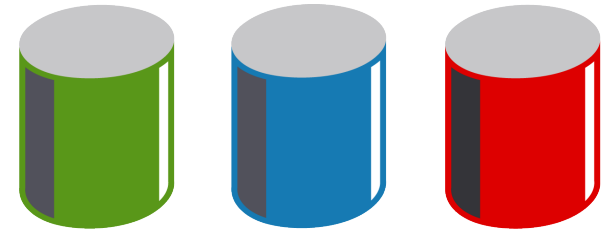
# *SUSE Linux Enterprise 10*

## **Linux Device Driver Process**

- Kernel Module Packages (kmp) for easy installation
- SLE 9 is enabled, SLE 10 fully optimized
- Unique feature only in SLE!
- ATI, NVIDIA, IBM, HP, etc. are active participants
- Every ISV, IHV who has a kernel space application or driver should participate!
- Complete documentation available
  - [http://developer.novell.com/wiki/index.php/Partner\\_Linux\\_Driver\\_Process](http://developer.novell.com/wiki/index.php/Partner_Linux_Driver_Process)

# High Availability Storage Foundation

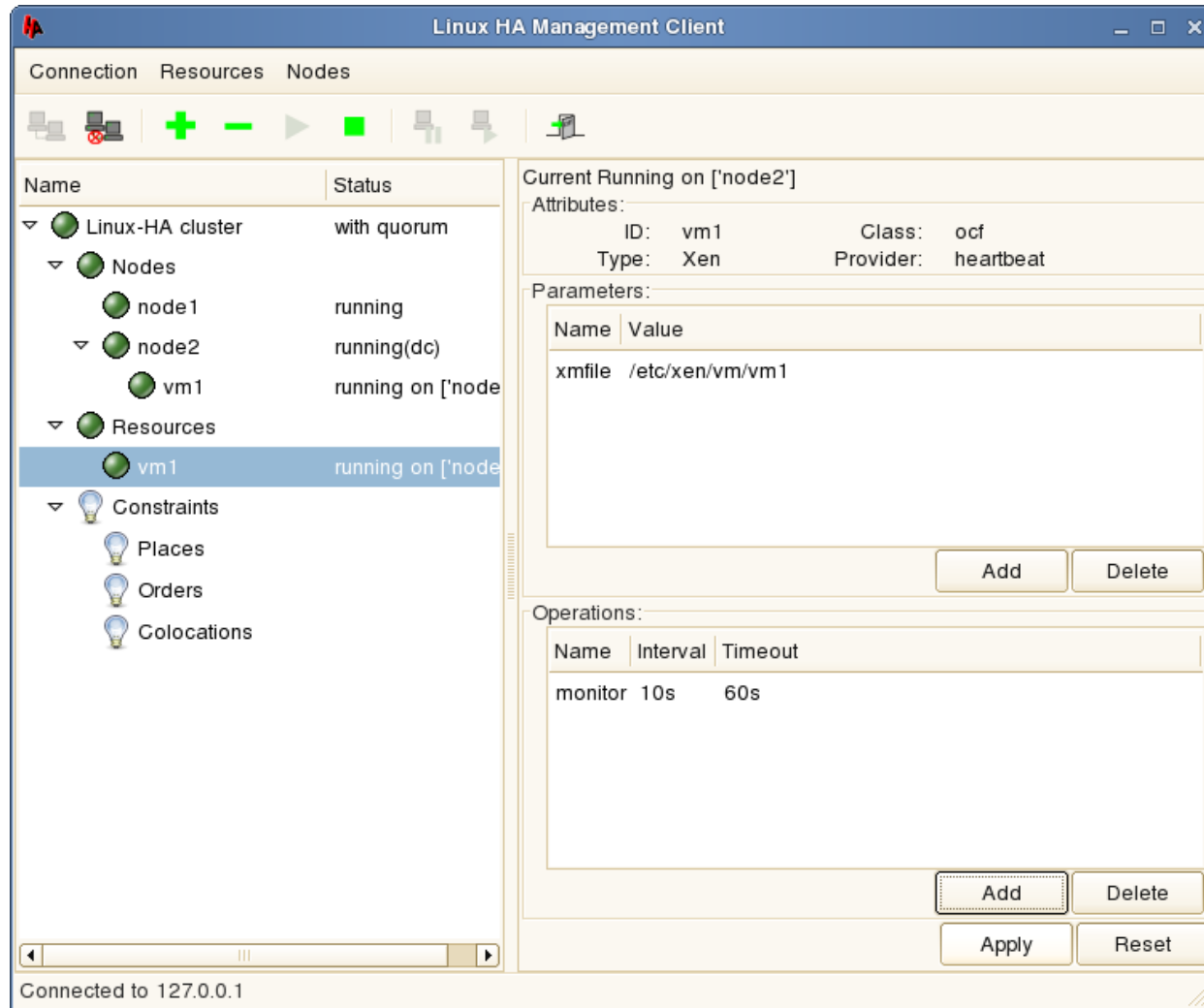
- **Enterprise Volume Management (EVMS2)**
  - Cluster-aware volume manager
  - Single, unified system for handling all storage management tasks
  - Unparalleled flexibility and extensibility
- **Integrates Oracle Cluster File System 2 (OCFS2)**
  - Symmetrical parallel cluster file system
  - Optimized for fast access to large files
  - Joint development with Oracle
- **Heartbeat v2 Clustering Services**
  - Powerful resource dependency model based on XML
  - Modular design with new cluster resource manager
  - Large clusters: 16 nodes tested, no inherent limit
  - Resources actively monitored for health



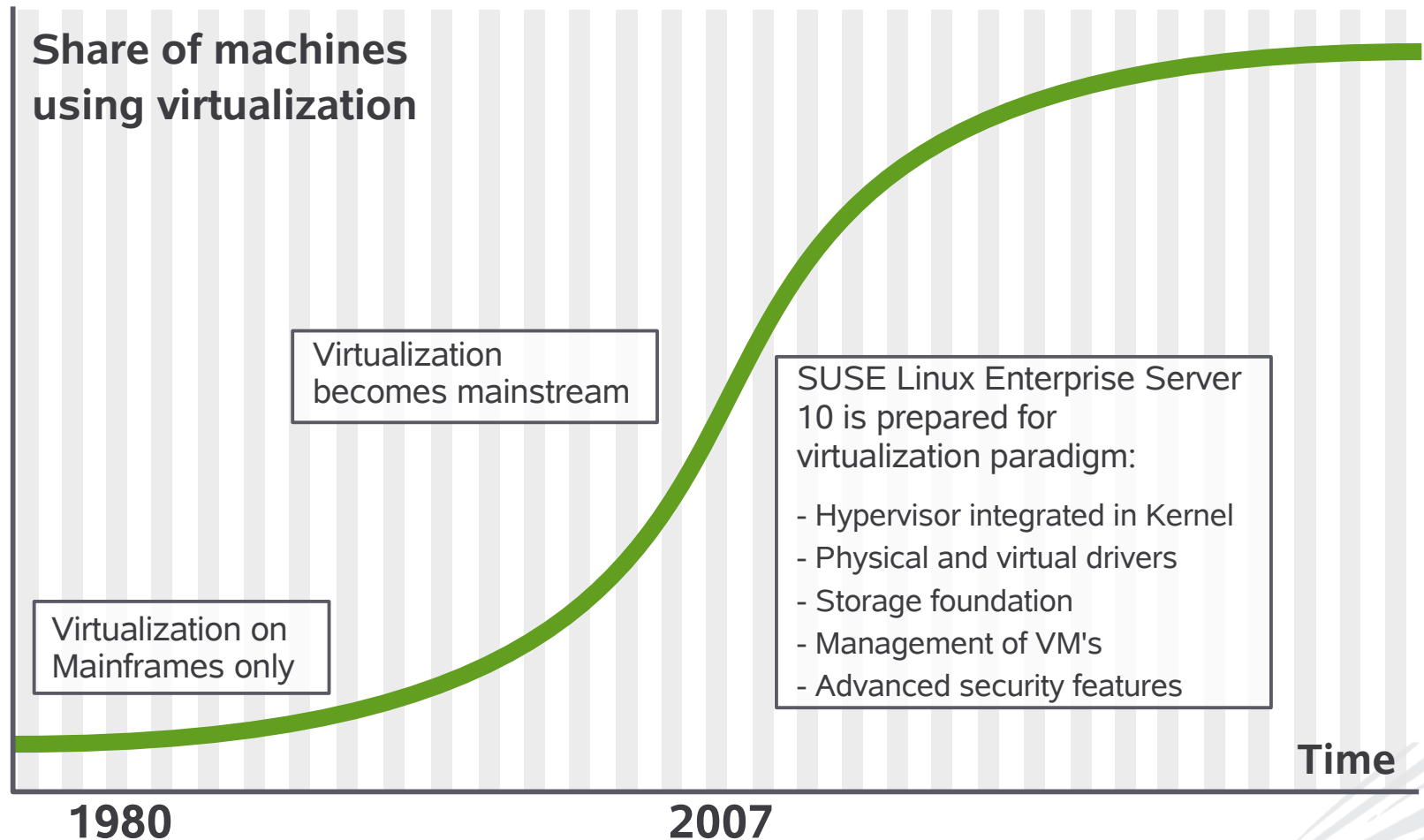


# SUSE Linux Enterprise Server 10

## Reduce HA complexity with GUI



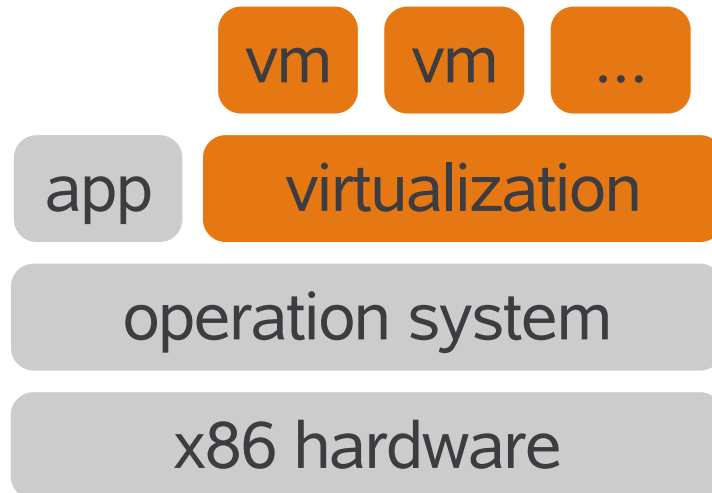
# Technology Trend: Virtualization



# Hosted vs. Bare Metal Virtualization

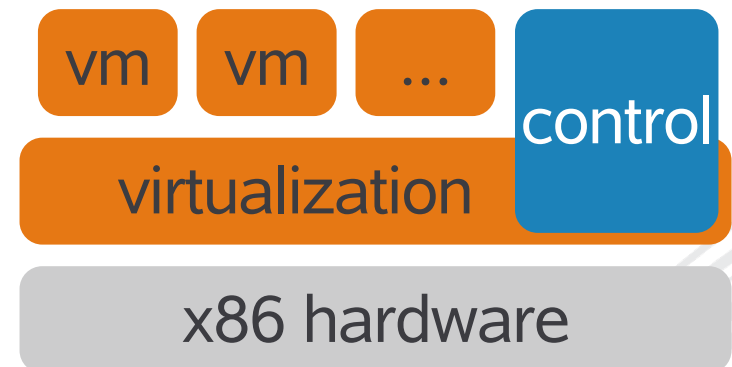
## Hosted

- Virtualization installs like an application rather than like an operating system
- Can run alongside conventional applications



## Bare Metal

- Maximum performance with lowest overhead
- Highly efficient I/O pass-through architecture for network and disk
- only 100Ks of lines of code versus 10-25 million lines of host operating system code



# Virtualization Technologies for Linux



- ESX Server + VirtualSMP
- GSX Server → VMware Server
- Virtual Center + Vmotion
- P2V Assistance




## User Mode Linux

- Linux inside Linux
- Linux kernel runs as process in user space
- Hardware independent



- Isolated, secure virtual private servers (VPS) on a single OS kernel
- Commercially avl. as Virtuozzo

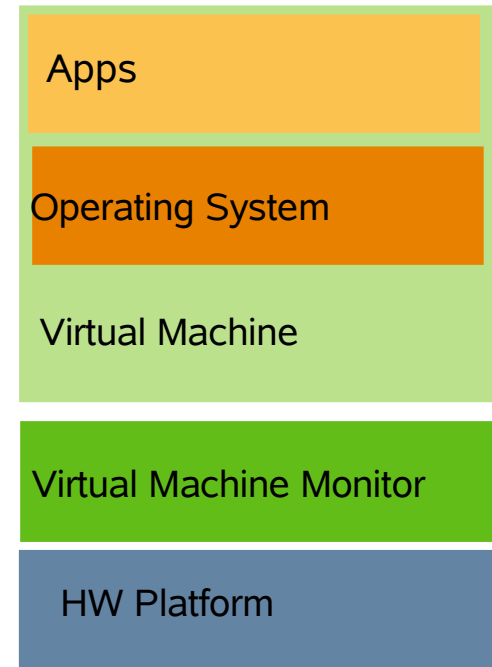
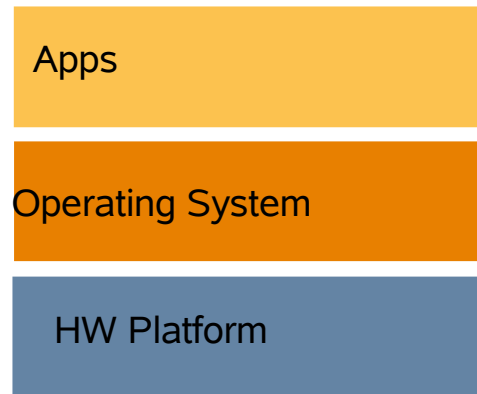


- 
- Hypervisor, Paravirtualization
  - High performance
  - Requires ported guest OS or HW virtualization technology
  - x86 architecture (32+64 Bit)

# IA-32 Privilege Levels

Unprivileged  
Rings 1-3

Privileged  
Ring-0



IA-32 provides 17 privileged instructions used by OS's to control critical platform resources (such as memory mapping)

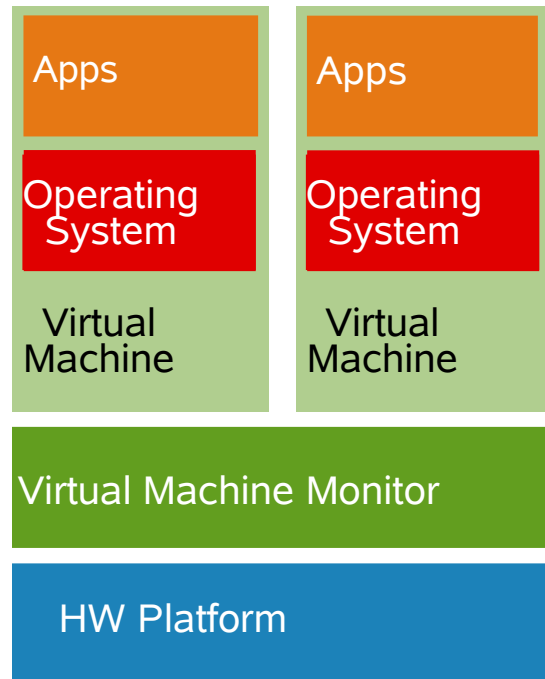
When the OS is not running in Ring-0, execution of any of these privileged instructions can create a conflict, causing system fault or errors.

There are two ways to deal with this problem ...

# SUSE Linux Enterprise Server 10

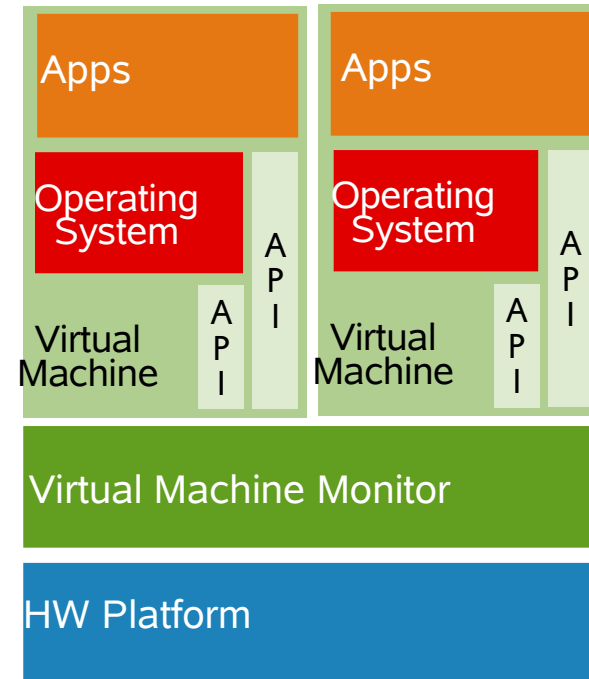
## Full & Paravirtualization Overview

### Full Virtualization



Runtime modification of Guest OS:  
VMM manages the conflict, then  
returns to OS

### Paravirtualization



Static modification of Guest OS prior to  
runtime: Privileged instruction calls are  
exchanged with API functions provided  
by the VMM

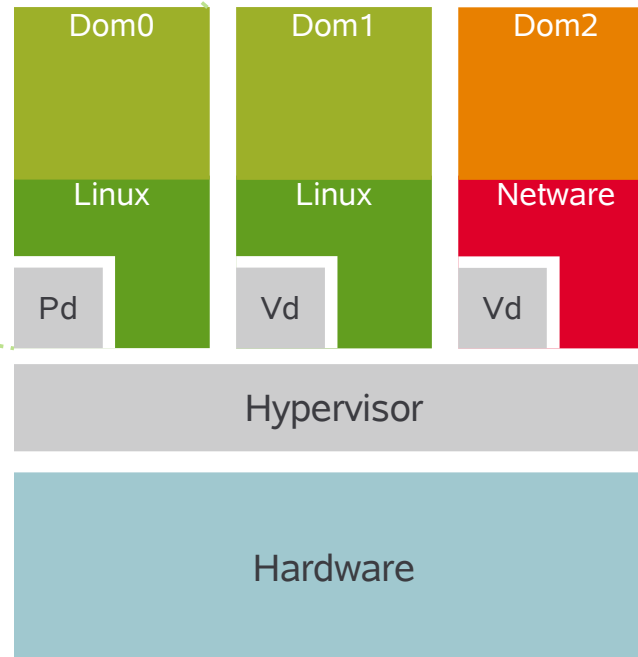
- Almost no performance degradation
- Significant scalability

# SUSE Linux Enterprise Server 10

## Xen Architecture – Simple View

Dom0 is the management domain for Xen guests

- controls compute resources dynamically (e.g. memory, CPU, I/O)
- provides interfaces to the physical server.
- provides administration tools and interfaces



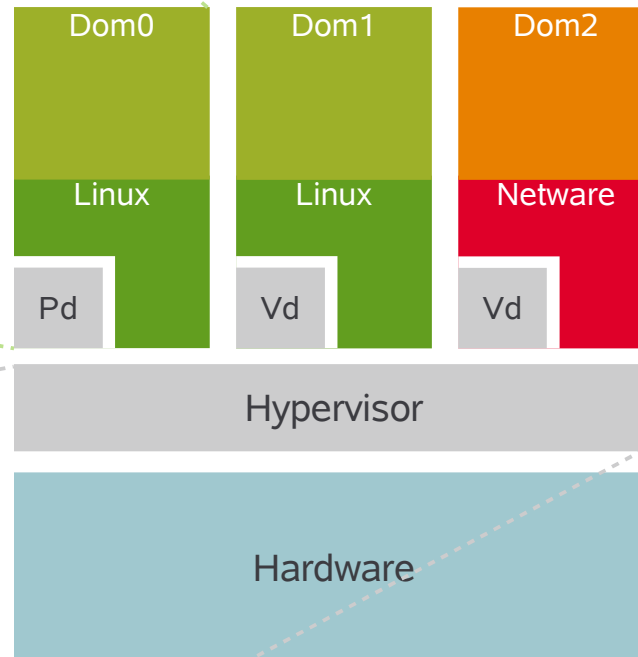
Pd = Physical Device Driver  
Vd = Virtual Device Driver

# SUSE Linux Enterprise Server 10

## Xen Architecture – Simple View

Dom0 is the management domain for Xen guests

- controls compute resources dynamically (e.g. memory, CPU, I/O)
- provides interfaces to the physical server.
- provides administration tools and interfaces



Hypervisor

- is the virtual interface to the hardware – virtualizes the hardware
- manages conflicts caused by OS access to privileged machine instructions

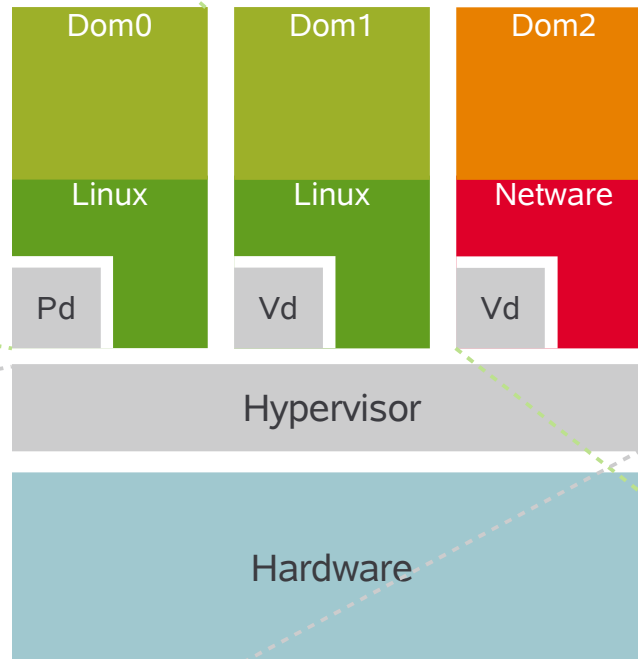
Pd = Physical Device Driver  
Vd = Virtual Device Driver

# SUSE Linux Enterprise Server 10

## Xen Architecture – Simple View

Dom0 is the management domain for Xen guests

- controls compute resources dynamically (e.g. memory, CPU, I/O)
- provides interfaces to the physical server.
- provides administration tools and interfaces



DomU is the guest OS

- hosts the application workloads
- typically uses virtual device drivers to connect to the physical drivers in Dom0 by the hypervisor.
- can also use physical device drivers directly
- can be stored in a file-image

Hypervisor

- is the virtual interface to the hardware – virtualizes the hardware
- manages conflicts caused by OS access to privileged machine instructions

Pd = Physical Device Driver  
Vd = Virtual Device Driver

# *SUSE Linux Enterprise Server 10* **Novell Virtual Server Facts**

- SUSE Linux Enterprise Server 10 includes Xen 3.0.2
- Supported hardware architectures: x86 (32bit), x86 PAE (32bit), x86-64 (64bit) including features to run unmodified OS
- Unmodified OS operation requires Intel Virtualization Technology (Intel VT) and AMD Virtualization (AMD-V) hardware
- One IO and system management VM, many application VMs
- Virtual Machine Server and Virtual Machine are verified layers by Novell YES certification
- Certified systems, solution stacks and their combinations are listed in YES certification bulletins

# *SUSE Linux Enterprise Server 10* **Xen 3.0.2 support status**

- Overview

- Runs both SLES 10 VM Server / SLES 10 VM (32/32bit and 64/64bit)
- VM server RAM support: x86 4GB, x86 PAE 16GB, x86-64 32GB
- Up to 16 CPUs, 8 NICs and 12.000 disks for VM Server
- Up to 4 vCPUs, 3 vNICs and 16 vDisks for VM
- Technical preview allows to run different unmodified OS if hardware support is present (full virtualization with Intel VT or AMD-V)

- Maintenance update Oct 2006

- Updated hypervisor to credit scheduler of Xen 3.0.3 for increased performance and scalability
- Several fixes to improve full virtualized OS installation and support

# No Operating System is Invulnerable

*Not even Linux...*

N.



Many bygone security flaws in Linux could have resulted in serious exploits if Linux had not had such strong community behind it

Few applications enjoy the same level of security scrutiny from the community

Each networked application introduces potential new exploits

**How do you mitigate for security flaws that you don't know about yet?**

# *SUSE Linux Enterprise Server 10*

## **Novell AppArmor**



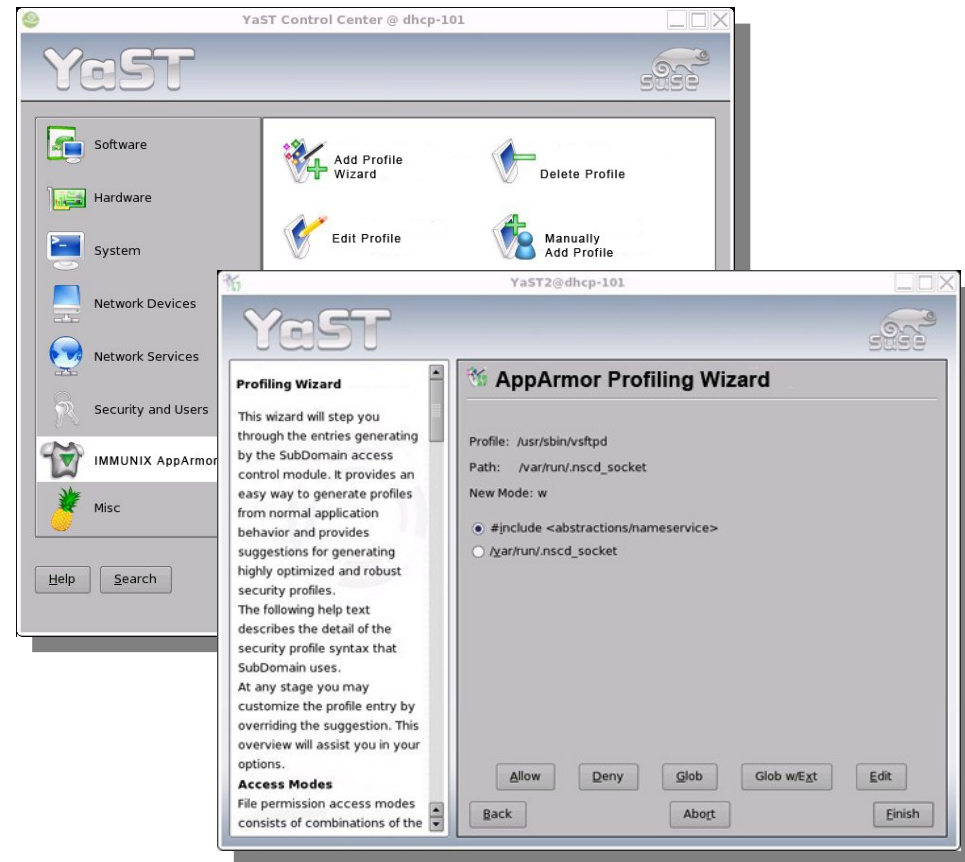
*Novell AppArmor is an application security tool that helps protect Linux systems from unknown security flaws*

- Designed for ease of use
- Deploy security policy in hours, not days
- Confine applications to do *only* what they are supposed to do—*and nothing else*

# SUSE Linux Enterprise Server 10

## Integrated Linux Application Security

- Creates “firewall” around any Linux program (custom, open source, third party)
- Prevents the exploitation of unknown or undiscovered application vulnerabilities
- Prevents unauthorized access to all system resources
- Doesn't rely on attack signature database
- Comprehensive YaST-based tool set
- Default policies included



# *SUSE Linux Enterprise Server 10*

## **A Closer Look at AppArmor**

### Security Model

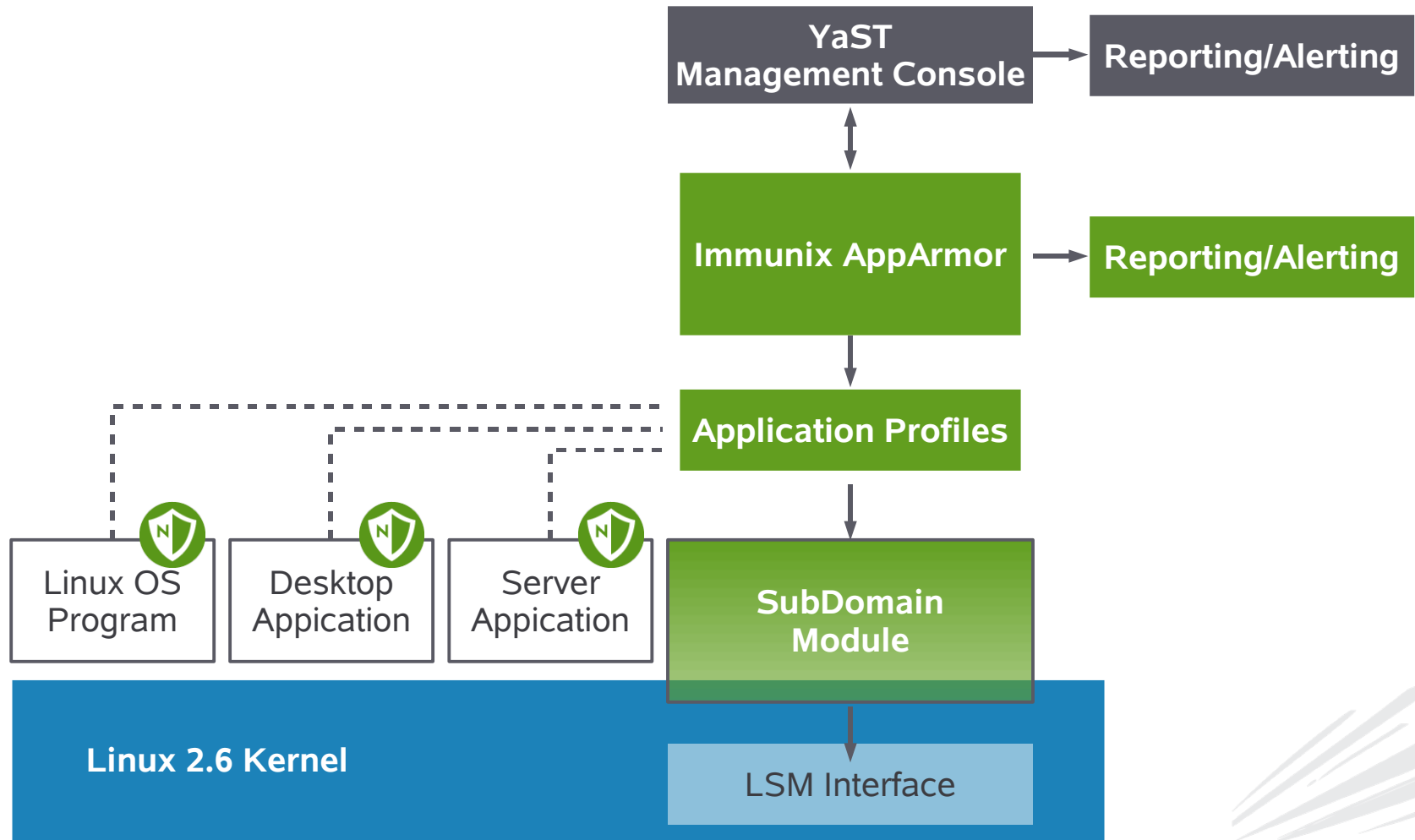
- Proactive “whitelist” approach, no attack signature database
- Profiles grant access to the minimal list of files/directories and POSIX capabilities required by the application
- Complete kernel-level mediation through Linux Security Module

### Automated workflow for security profile generation

- Autoscan for open network ports
- Find applications listening to ports and check for existing profile
- Auto-generate profile template based on static analysis
- Auto learn mode: Automatically expands profile while running the application through normal operation
- Interactive optimizer assists in simplifying the profiles with regular expressions and foundation classes

# SUSE Linux Enterprise Server 10

## How AppArmor Works



# *SUSE Linux Enterprise Server 10*

## **AppArmor vs. SELinux**

### AppArmor

- Automated YaST-based tools make security profile development easy
- No application modifications
- Supports security policy for sub-processes
- Human-readable security policy with regular expression support
- Benchmarked performance overhead is 0-2%

### SELinux

- Limited tools for defining security policy, requires additional expertise
- Full support requires application changes
- Process is smallest unit of containment
- Policies are written in cumbersome type enforcement language
- Stated performance overhead is 7%

# Subprocess Confinement with Change\_Hat

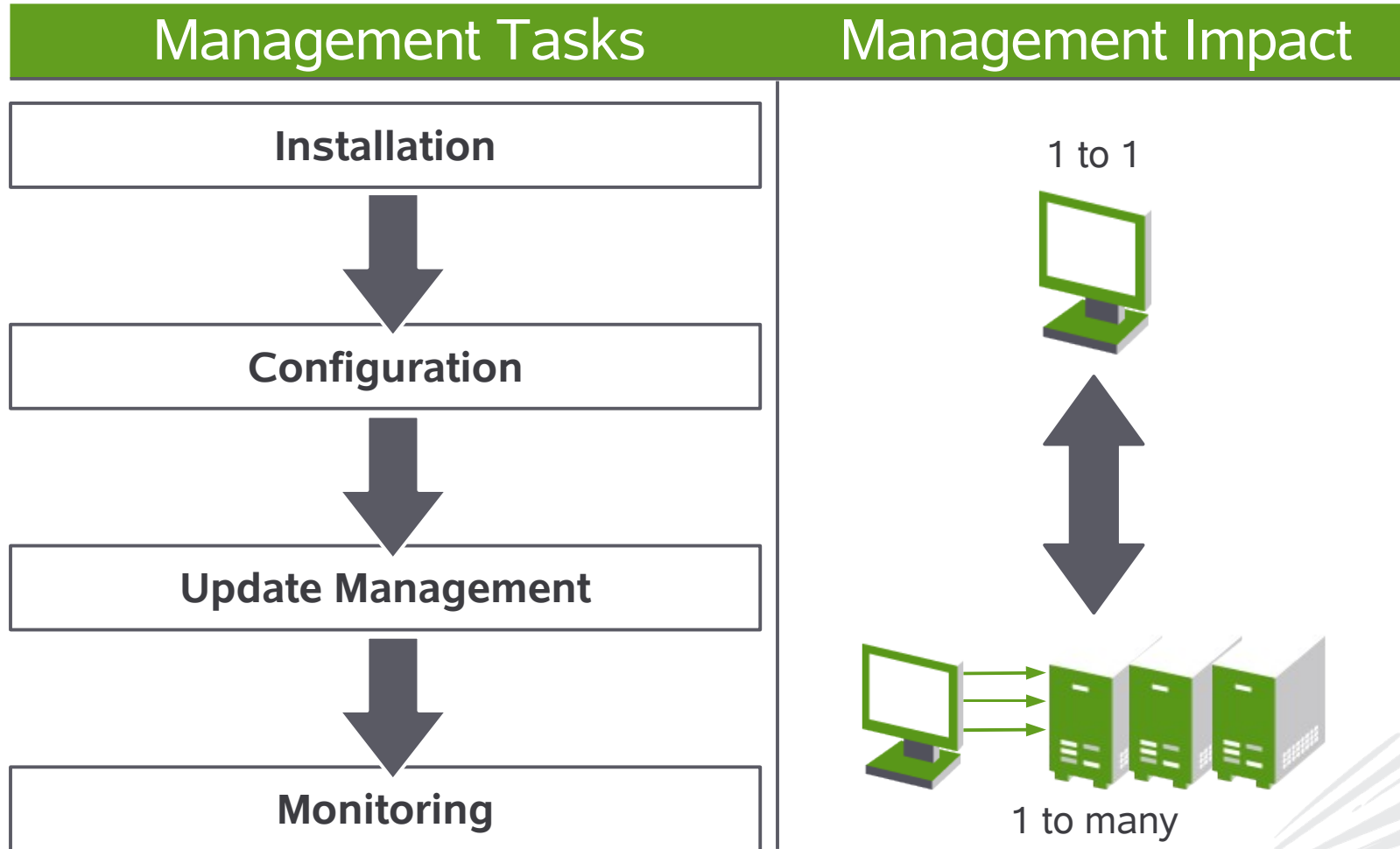
## Changing In to a Subprofile

- An AppArmor profile applies to an executable program
- If a portion of the program needs different access permissions than other portions, the program can "change hats" to a different role
- To change into a new hat, program calls the `change_hat()` function
- Passes in a pointer to the subprofile and a 32bit `magic_token`.

## Changing Out of a Subprofile

- To return to original profile, program calls `change_hat()` with a pointer to NULL as the subprofile, and the original `magic_token` value.
- If `magic_token` does not match the original `magic_token`, change back will not happen, and current task will be killed.
- If `magic_token` matches the original token, then the process will change back to the original profile.

# SUSE Linux Enterprise 10 Management Lifecycle



# Management Lifecycle Installation

• 1 to 1

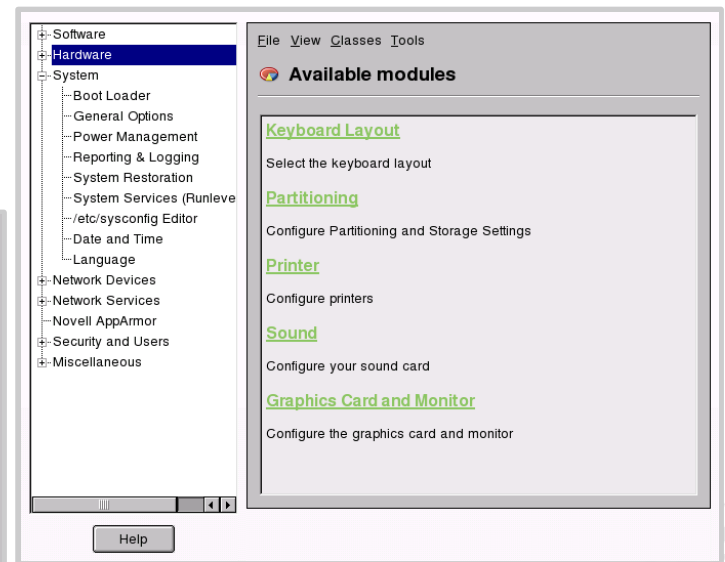
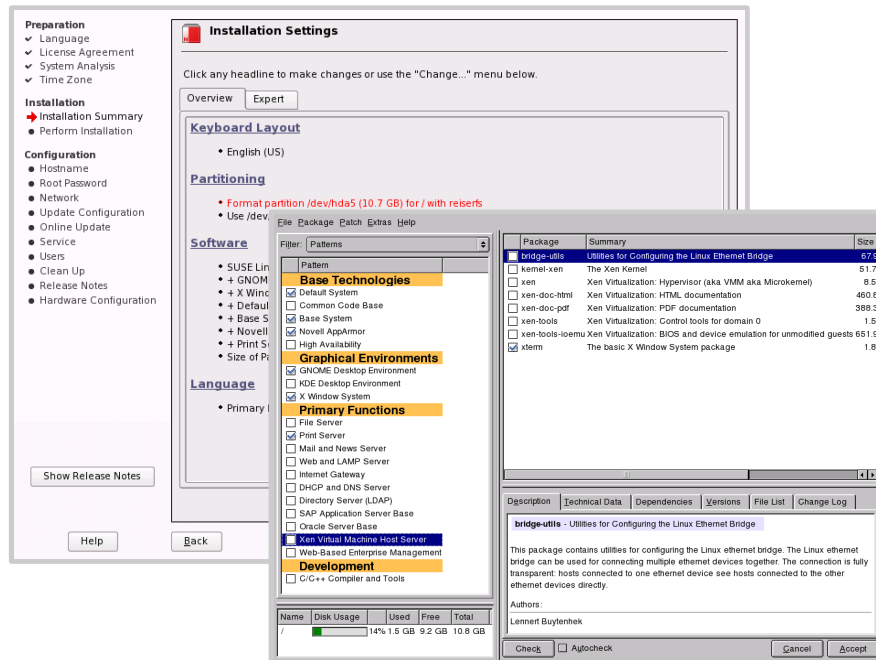


- YaST Installation Workflow
- Pattern based software deployment

• 1 to many



- AutoYaST
- ZENworks Linux Management

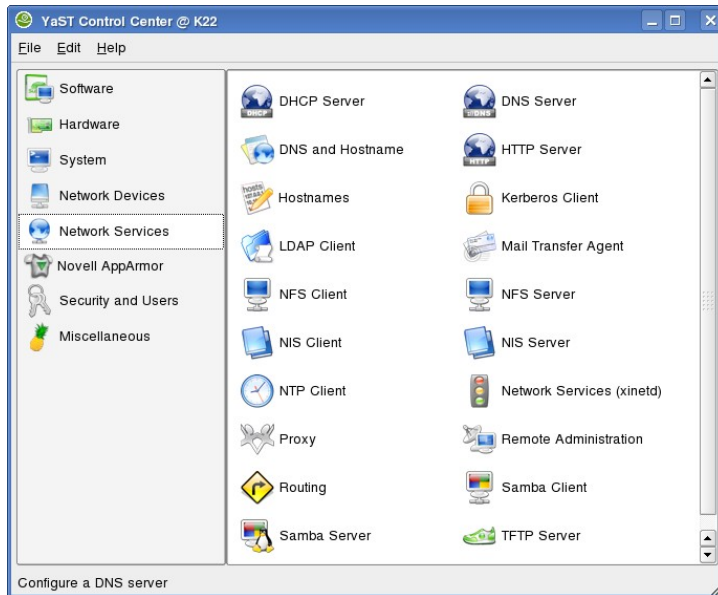


# Management Lifecycle Configuration

- 1 to 1



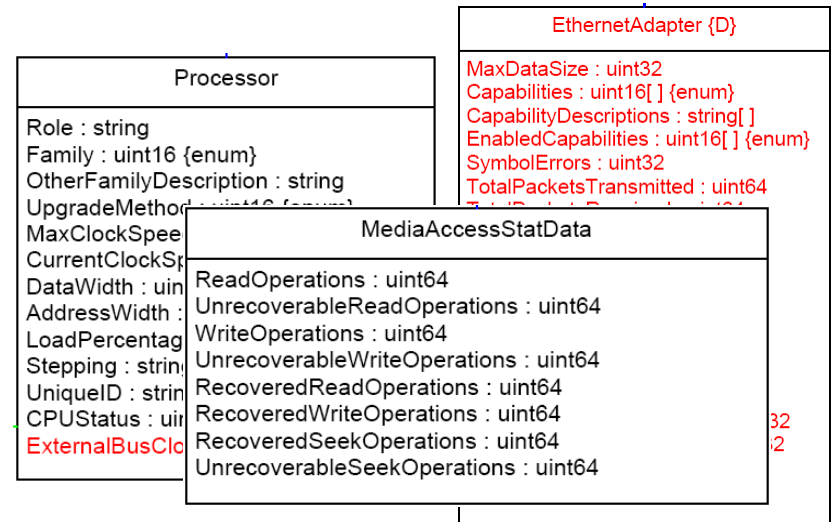
- YaST Control Center
  - > Module based
  - > Categorized




- 1 to many

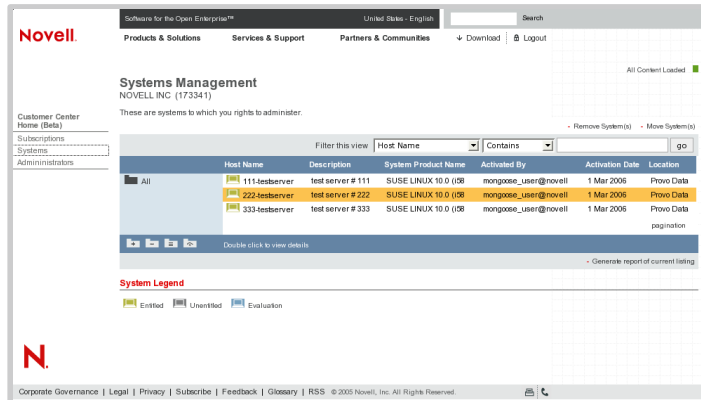



- AutoYaST
- ZENworks Linux Management
  - > Machine lock down
  - > AppArmor profile deployment
- OpenWBEM / CIM support

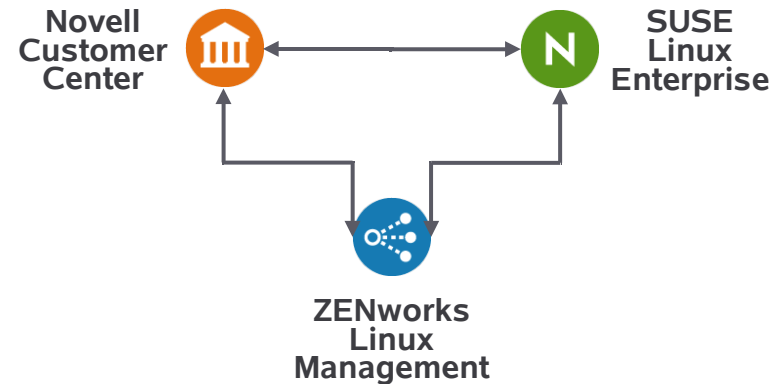


# Management Lifecycle Updates

- 1 to 1 
  - YaST Package Manager
  - ZENworks Tools
    - > zmd
    - > rug
    - > zen-updater
  - Novell Customer Center
    - > Automatic Configuration
    - > Registration and Entitlement Management



- 1 to many 
  - Use ZENworks Linux Management as a remote server



# Management Lifecycle Monitoring

- 1 to 1

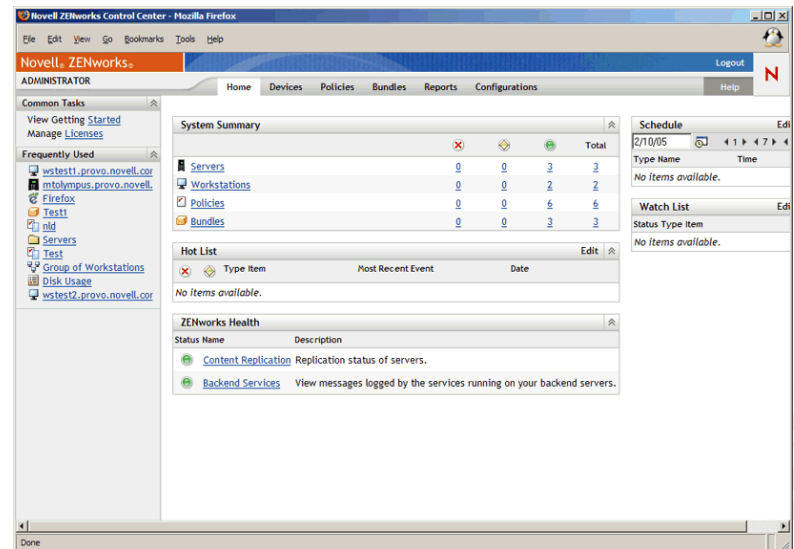
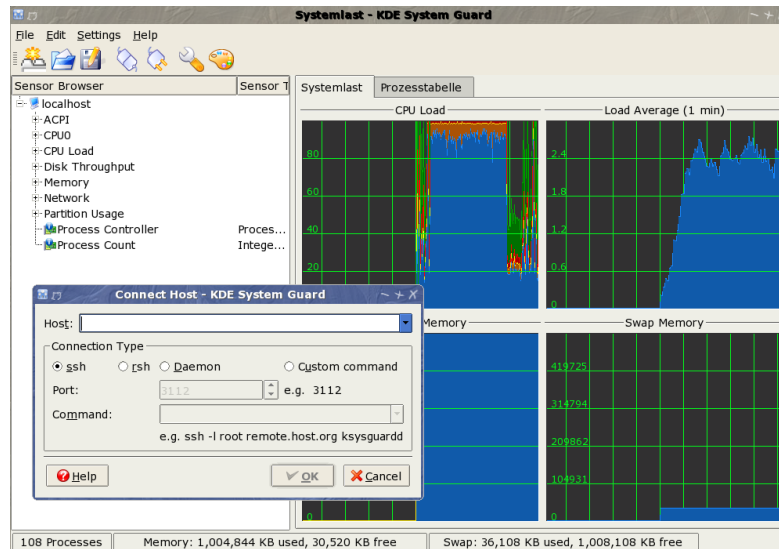


- sysstat-package for decent low level monitoring
- ksysguard using graphical frontend
  - > Local
  - > Remote

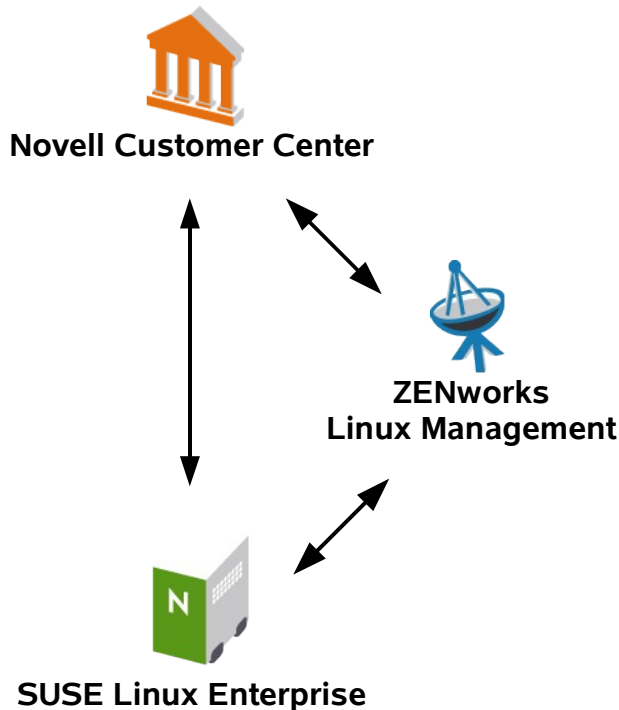
- 1 to many



- nagios
- OpenWBEM / CIM support
- ZENworks®



# *SUSE Linux Enterprise 10* **Novell® Customer Center**



## **Subscription and update service**

- One tool to manage purchase, renewal, expirations.
- Easy reporting on compliance and forecast future purchasing needs
- Integrated patch management and update service, powered by ZENworks

## **Access to Novell Support**

- Easy-to-use portal for support
- One location for access to knowledge base, electronic support requests, and downloads.

## **Intuitive management console**

- One console to discover, update and manage Linux

**Novell Customer Center makes it easy to register, update, secure and monitor all Linux systems on the network, from the desktop to the data center.**

# Impressions of the Novell® Customer Center

Novell.

Software For The Open Enterprise
United States - English

Search

Products & Solutions
Training & Support
Partners & Communities
↓ Download
🔒 Login

## Novell Customer Center

Sheet Music Inc., 1601 W 820 N, SLC, Utah 84...

◀ Change Organization

→ view/edit details

Welcome to the Novell Customer Center. With this tool you can easily manage all aspects of your business relationship with Novell. And we can customize any welcome text for first time users or veteran users or new functionality as it comes online. etc. etc. etc.

▶ Products/Subscriptions	▶ Systems	▶ Support Requests	Alerts																								
<table style="width: 100%; border-collapse: collapse;"> <tr><td>Total:</td><td style="text-align: right;">10</td></tr> <tr><td>New:</td><td style="text-align: right;">1</td></tr> <tr><td>Evaluation:</td><td style="text-align: right;">3</td></tr> <tr><td>Active:</td><td style="text-align: right;">5</td></tr> <tr><td>Expired:</td><td style="text-align: right;">1</td></tr> <tr><td>Available Activations:</td><td style="text-align: right;">-22</td></tr> </table>	Total:	10	New:	1	Evaluation:	3	Active:	5	Expired:	1	Available Activations:	-22	<table style="width: 100%; border-collapse: collapse;"> <tr><td>Total:</td><td style="text-align: right;">432</td></tr> <tr><td>Subscribed:</td><td style="text-align: right;">368</td></tr> <tr><td>Unsubscribed:</td><td style="text-align: right;">45</td></tr> <tr><td>Evaluation:</td><td style="text-align: right;">14</td></tr> </table>	Total:	432	Subscribed:	368	Unsubscribed:	45	Evaluation:	14	<table style="width: 100%; border-collapse: collapse;"> <tr><td>Open SRs:</td><td style="text-align: right;">12</td></tr> <tr><td>Closed SRs:</td><td style="text-align: right;">17</td></tr> </table>	Open SRs:	12	Closed SRs:	17	<ul style="list-style-type: none"> <li>▶ 32 Subscriptions to renew this month.</li> <li>▶ 1 Subscription has expired.</li> <li>▶ 105 Systems activated above your subscriptions level.</li> <li>▶ 22 Evaluation subscriptions</li> </ul>
Total:	10																										
New:	1																										
Evaluation:	3																										
Active:	5																										
Expired:	1																										
Available Activations:	-22																										
Total:	432																										
Subscribed:	368																										
Unsubscribed:	45																										
Evaluation:	14																										
Open SRs:	12																										
Closed SRs:	17																										

▶ My Profile	▶ Order History	▶ Partner Memberships				
<p><b>Cori Jones</b> Provo, UT</p> <p>Edit login information. See your notification preferences. See your certifications. See estimates you have saved. Manage your organizations.</p>	<table style="width: 100%; border-collapse: collapse;"> <tr><td>Deliveries pending:</td><td style="text-align: right;">5</td></tr> <tr><td>Recent orders:</td><td style="text-align: right;">2</td></tr> </table> <p>Check the status of an order. Link to download purchased items. View your previous purchase transactions.</p>	Deliveries pending:	5	Recent orders:	2	<p>See your partner memberships and all the glorious benefits of being a member and anything else apertaining to the maintenance, management, or membership of this section.</p>
Deliveries pending:	5					
Recent orders:	2					

1.800.529.3400

- Local Numbers
- Request Call
- Buy

32

ready

# Impressions of the Novell® Customer Center

The screenshot shows the Novell Customer Center interface. At the top, there's a navigation bar with the Novell logo and links for Products & Solutions, Services & Support, and Partners & Communities. A search bar is also present. The main content area is titled "Products & Subscriptions" and shows a message: "SRHOADES-NOVELL-COM (UC619) These are the purchased products, product and service subscriptions to which you have rights to administer. Double-click on any line item to view details." Below this is a table with columns for Name, Usage, Expire Date, Type, Status, and Action. The table currently displays "0 records returned for selected criteria". There are also links for "All", "Product Subscriptions", "Purchased Products", "Service Subscriptions", and "Entitled Products". A sidebar on the left contains "Customer Center Home", "My Profile", and "My Contacts" sections. The browser's address bar shows the URL: https://secure-www.novell.com/center/regadmin/jsps/sub\_app.jsp?topic=list&clearFilter=true.



Live Demo



# SUSE Linux Enterprise Desktop

# How to buy

- Novell Sales - Large customers, special deals
- Novell Online - [shop.novell.ch](http://shop.novell.ch)
- Novell Partner - [www.novell.com/partnerlocator](http://www.novell.com/partnerlocator)
- Or just ask us!

# Questions?

- Ask now!
- Ask later:
  - **Torsten Hallmann**  
*Technology Specialist*  
torsten.hallmann@novell.com  
+41 43 299 75 58
  - **Andreas Pfenninger**  
*Linux Sales*  
andreas.pfenninger@novell.com  
+41 43 299 78 17



**Novell®**

### **Unpublished Work of Novell, Inc. All Rights Reserved.**

This work is an unpublished work and contains confidential, proprietary, and trade secret information of Novell, Inc. Access to this work is restricted to Novell employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of Novell, Inc. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

### **General Disclaimer**

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. Novell, Inc., makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Novell marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.

