

Novell®

Privileged User Manager

Product Overview

Novell®

Security Breaches **Rising**

“The UK's tax authority has confirmed that it has paid an informant for data regarding British citizens who have accounts in tax haven Liechtenstein.”

- German government reportedly paid over \$6M for same data

- *InfoWorld, 07/21/2008*

Security Breaches

- * 80% are accidental
- * 20% are malicious

When it comes to resolution, there is no difference. You need to fix it and make sure it doesn't happen again

* FBI & Price Waterhouse

“...Terry Childs, a network administrator employed by the City of San Francisco, was arrested and taken into custody, charged with four counts of computer tampering.”

- *British Broadcasting Corporation, 02/24/2008*

Average Cost

\$50k – external breach
\$2.7m – internal breach

70% of breaches are internal !

Why Privileged User Management is Important

Security

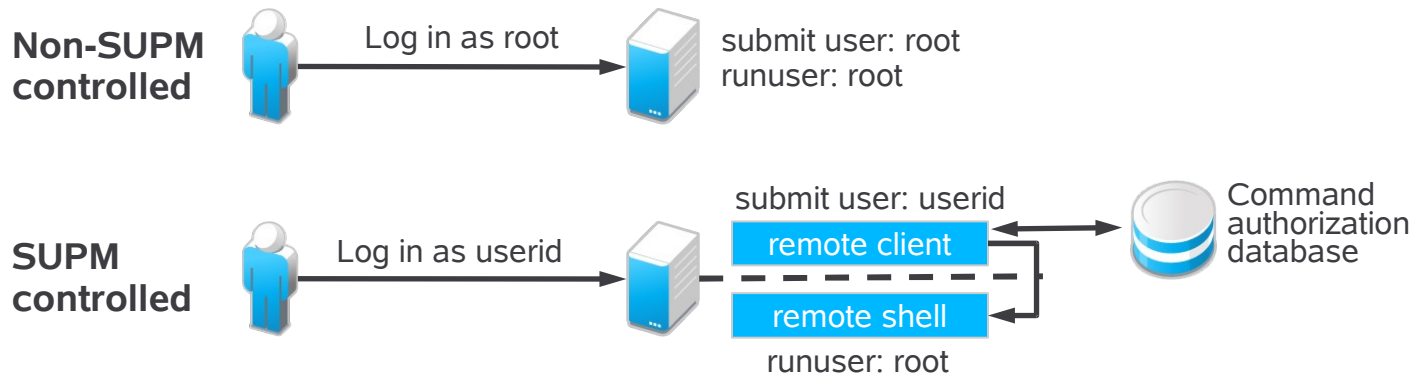
- UNIX and Linux systems act as the backbone of many mission-critical services
- Multiple users (IT admins, application developers and DBAs) may have *full* superuser privileges
- Most users only require limited access
- Organizations lack appropriate controls to manage user access to root accounts, leading to security breaches and regulatory rebuke

Cost

- Financial penalties and losses due to a security breach
- Damage to the organization's reputation
- Erosion of customer confidence

What is SUPM?

- **S**uper **U**ser **P**rivilege **M**anagement
 - The process of managing access to privileged accounts, (such as root) to mitigate risk exposure



- User logs in with own non-privileged account
- Commands authorized before being executed remotely
- Known as 'root delegation'

Security – Needs **Due Diligence**

- What is it?
 - Proactive checking of user activity
- Who does it?
 - Internal Managers / Auditors
- What do they do?
 - Sign off on activity sampled from their users
- How does this help?
 - Regulatory compliance proven to external auditors
 - Risk mitigation / deterrent
 - Customer peace of mind

Novell Privileged User Manager



- Control user access to root accounts
- Audit all user activity with 100% keystroke logging
- Analyze potential threats based on policy-based risk ratings
- Simplify audit reporting with the most relevant, context-based information
- Support compliance with internal policies and external regulations

3 Step UNIX/Linux Security Solution



- 100% privileged user keystroke recording
 - Automated grading of activity risk level
-

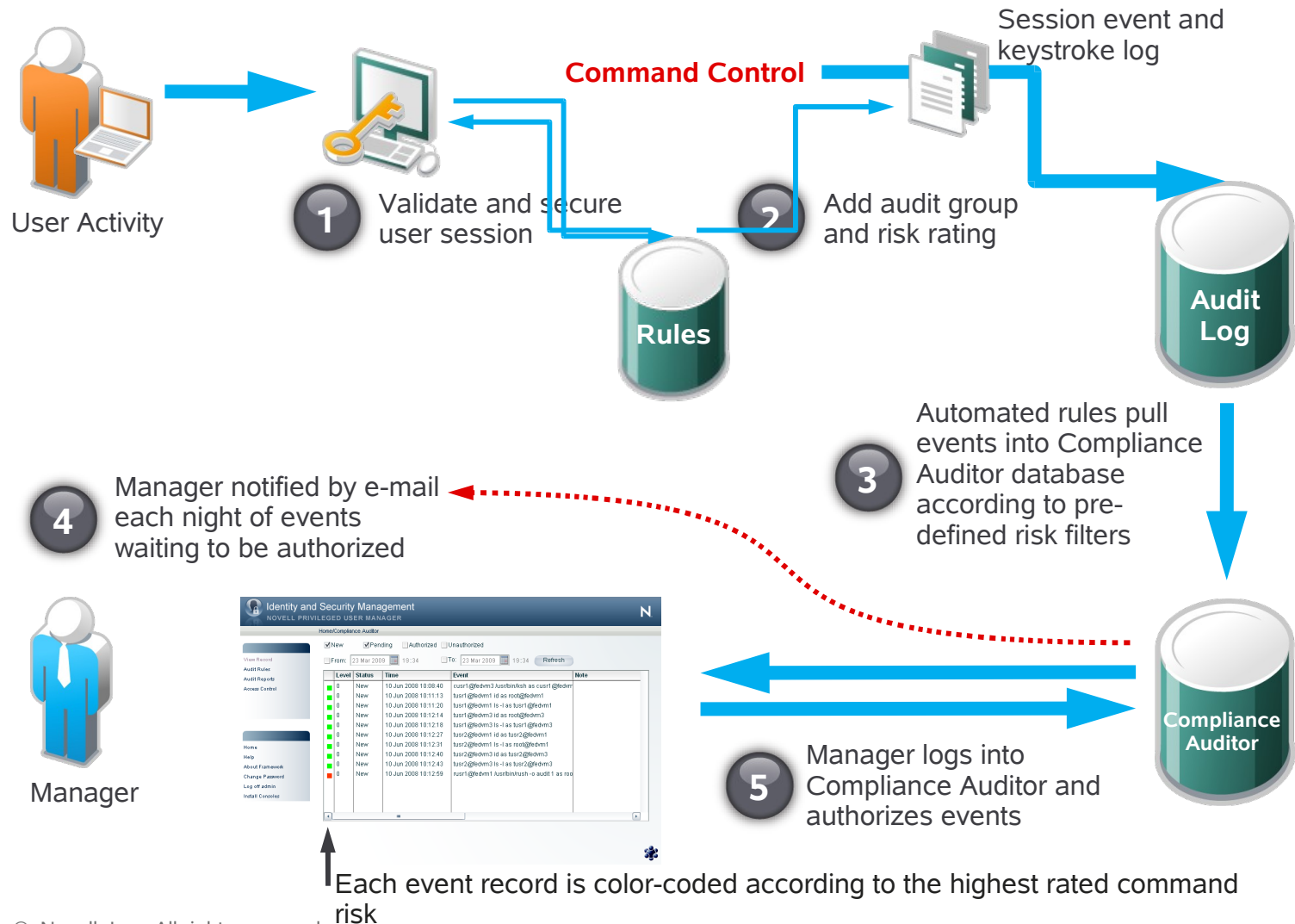


- Super user privilege management
 - Real-time control and alerting
-



- Proactive compliance management
- Auditing the auditor

Workflow for Due Diligence



Auditing for Compliance

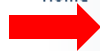
View Keystroke Log

File: /var/log/pb.bsilvers.bash.KqvLdT

Terminal Foreground: Black

Symark
PowerBroker Auditing

Novell® Auditing



Home

About Framework

Change Password

Built-in Risk Analysis Engine -
Each event record is color-coded according to the highest rated command risk ranging from Green (low) to Red (high)..

Identity and Security Management
NOVELL PRIVILEGED USER MANAGER

Home/Compliance Auditor

New Pending Authorized Unauthorized

From: 23 Mar 2009 19:34 To: 23 Mar 2009 19:34 Refresh

Level	Status	Time	Event	Note
0	New	10 Jun 2008 10:08:40	cusr1@fedvm3 /usr/bin/ksh as cusr1@fedvm3	
0	New	10 Jun 2008 10:11:13	tusr1@fedvm1 id as root@fedvm1	
0	New	10 Jun 2008 10:11:20	tusr1@fedvm1 ls -l as tusr1@fedvm1	
0	New	10 Jun 2008 10:12:14	tusr1@fedvm3 id as root@fedvm3	
0	New	10 Jun 2008 10:12:18	tusr1@fedvm3 ls -l as tusr1@fedvm3	
0	New	10 Jun 2008 10:12:27	tusr2@fedvm1 id as tusr2@fedvm1	
0	New	10 Jun 2008 10:12:31	tusr2@fedvm1 ls -l as root@fedvm1	
0	New	10 Jun 2008 10:12:40	tusr2@fedvm3 id as tusr2@fedvm3	
0	New	10 Jun 2008 10:12:43	tusr2@fedvm3 ls -l as tusr2@fedvm3	
0	New	10 Jun 2008 10:12:59	rusr1@fedvm1 /usr/bin/rush -o audit 1 as root@fedvm1	



How Would You Prefer to Administer?

```

1  #! /bin/ksh
2  PATH=/usr/bin:/usr/local/bin:.
3  export PATH
4  if (( $# < 2 )); then
5      print -u2 "Usage: $0 client command";
6      exit 1
7  else
8      typeset MYACCOUNT=$1;
9      typeset -x LOGNAME=$1;
10     typeset ARGV=$2;
11 fi
12
13 if [ "$X$MYACCOUNT" = "Xcicdg"
14     typeset HOME_DIR="/fi
15 else
16     typeset -l -R2 CLNT=$
17     typeset HOME_DIR="/fi
18 fi
19
20 if [ ! -d $HOME_DIR ]; then
21     print -u2 "Error: can
22     exit 1;
23 elif [ ! -f "$HOME_DIR/.pro
24     print -u2 "Error: can
25     exit 2;
26 fi
27
28 HOME=$HOME_DIR
29 export HOME
30 cd $HOME
31 . /.profile;
32 jj=$(date "+%C%y%m%d.%H%M%S
33 jt=$EBSLOGS/sj.$ARGV.$jj
34 ksh -vx ujes $ARGV >> $jt
35

```



Symark PowerBroker / Quest UPM / Sudo



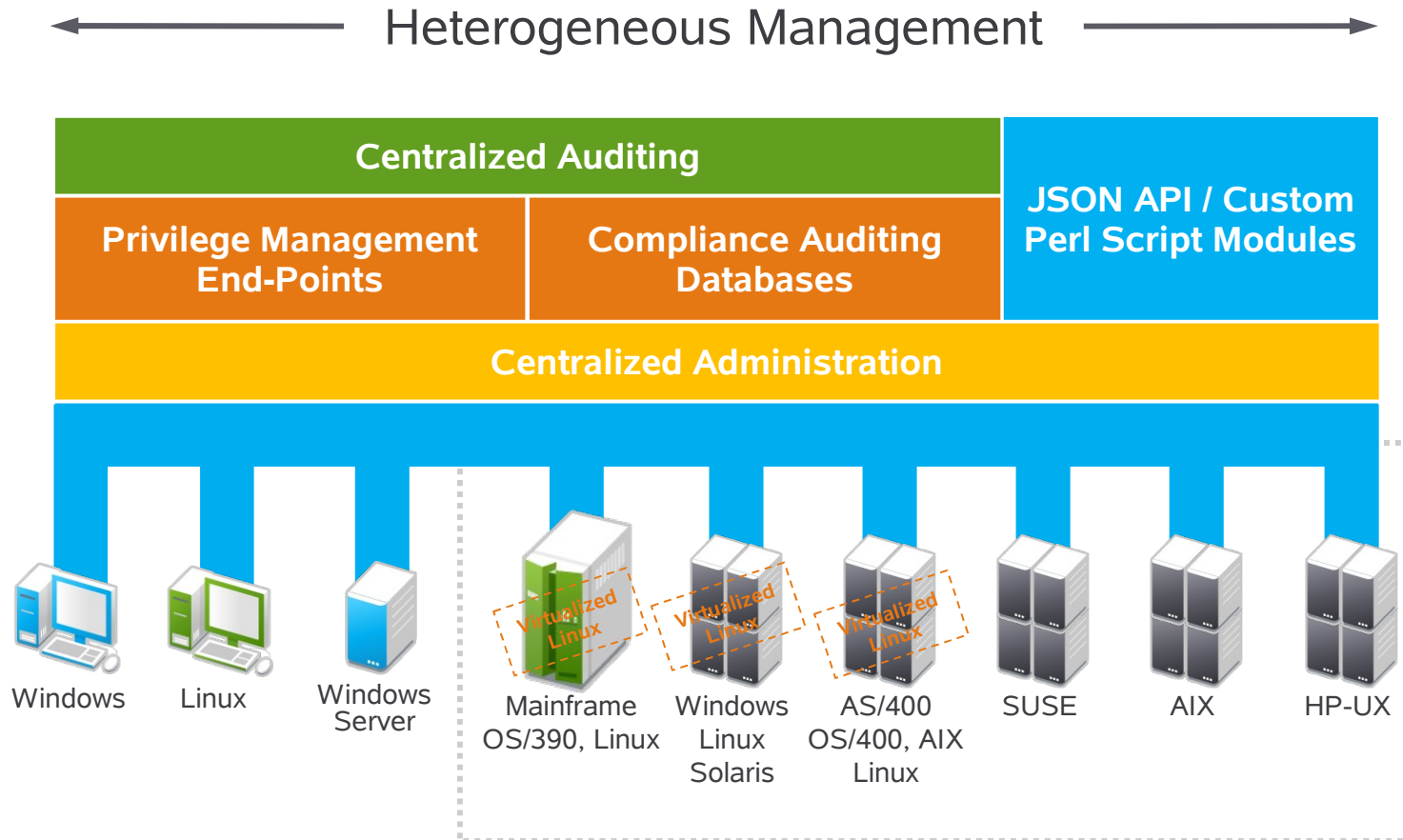
Novell® Privileged User Manager

Command Control Manager: usma-vfc1

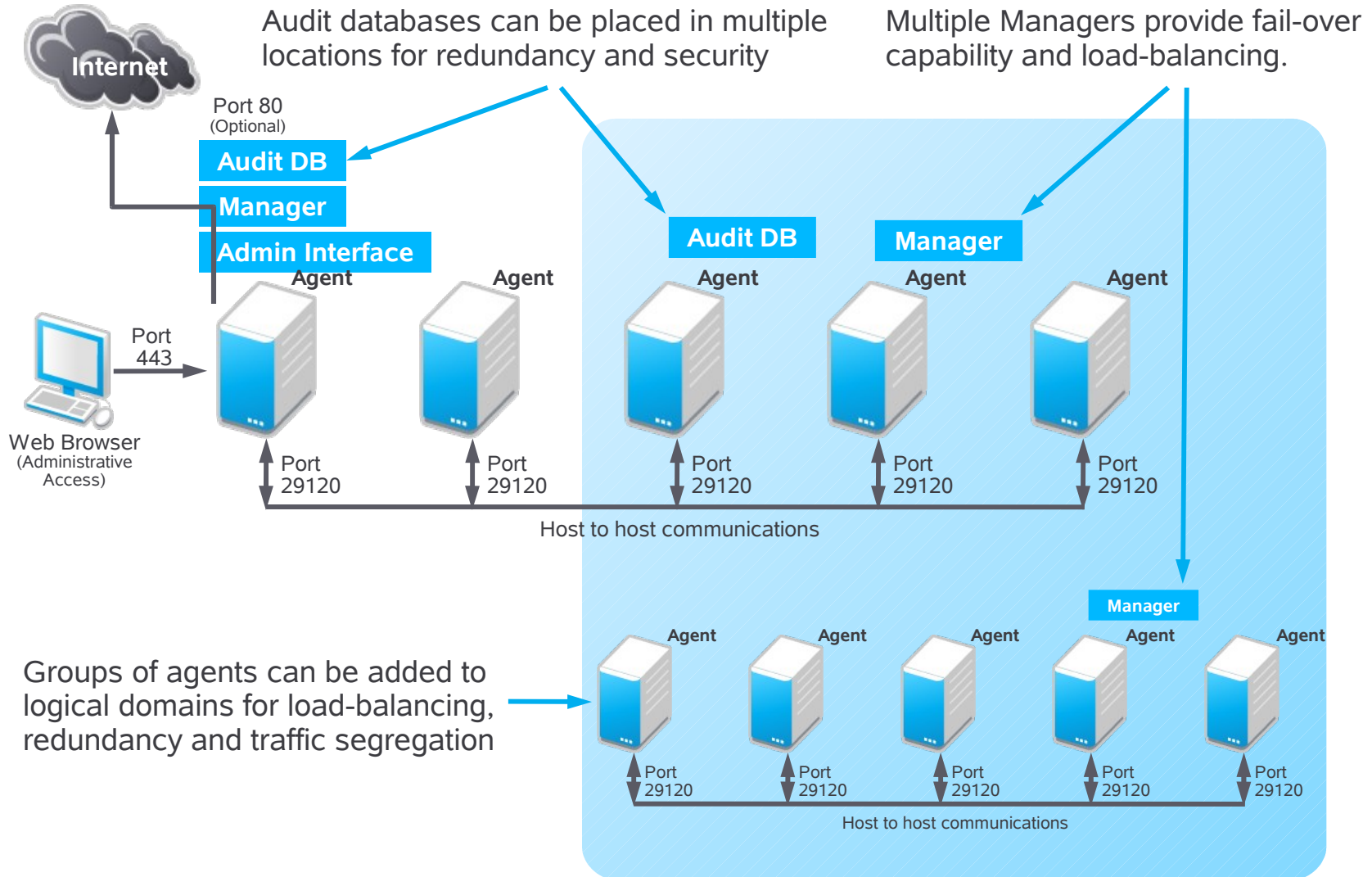


Architecture

Centralized Management



Underlying **Modular** Architecture



Architectural **Advantage**

- Robust and scalable architecture with inbuilt redundancy to provide 100% availability of service
- Modular components are deployed and updated through management console
- Centralized management of multiple Unix/Linux security policies across multiple sites
- Comprehensive audit capabilities for complete compliance management and forensic analysis
- Novell® Privileged User Manager brings security to Real-Time with **Actionable Risk Management**

Customer Success

The slide features a solid blue background. At the bottom, there are several horizontal white lines of varying lengths and thicknesses, creating a decorative effect. The text 'Customer Success' is centered in the upper right quadrant of the slide.

Novell® Privileged User Manager

Customers Include:



Customer Success Stories

- Barclays

- Large environment, >4500 UNIX servers worldwide
- Replacement of PassGo/Quest UPM product
- Currently rolling out to all divisions worldwide
- Maintenance windows reduced to 12% of original

- ING (Institutional Plan Services)

- Replacement of Symark PowerBroker
- Deemed important enough to be the only capital purchase for 2008
- Met all new auditing requirements
- Audit time reduced from 45 mins to <5 mins per session

Customer Observations

- Fulfills all SOX requirements
- Instead of doing a validation every six seconds, it's doing ***six every second***
- Can migrate to Novell® Privileged User Manager gradually (will co-exist with other solutions)
- Light footprint on servers
- Superior encryption

What Makes Novell® Privileged User Manager So Different?

- Scalability (thousands of hosts per framework)
- Proactive Compliance (managing due diligence)
 - Color-coded Risk Analysis highlights harmful activity
- Fast Forensics (searchable user activity, log file management)
- Graphical admin (no proprietary scripting languages)
 - Less administration + faster audit = ROI
- Easy Deployment (very fast, centrally managed, non-invasive)
- Technology (written from the ground up for speed and security)
- No downtime (auto failover even during product updates)

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. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. 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. The development, release, and timing of features or functionality described for Novell products remains at the sole discretion of Novell. 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.

