AD/Linux Desktop

Improving the Experience

Jim McDonough

Novell/SuSE Labs
Samba Team Lead

jmcdonough@suse.de

jmcd@samba.org

Novell®

AD Linux Desktop: The Current State

Current State: Basic integration

- User and group definitions
  - Trusts
  - Nested groups
- Login authentication
- Domain-based password policies
- Ticket creation
- Offline logins

© Novell, Inc. All rights reserved.

Current State: User experience

- Common Userid and Password
- Password policy messages
- Authentication through Kerberized applications
  - Firefox
  - Commandline utilities
- Automatic access to shared folders
  - Through desktop
    - Gnome: Nautilus, gvfs, stored in gconf
    - KDE: Konqueror, kwin, kio
  - Through text-based logins
    - Automount
    - pam_mount

© Novell, Inc. All rights reserved.

Current State: Admin Experience

- User and group definition through AD tools
  - Common authentication possible for some apps
- Secure DNS updates
- Application settings for Desktops (and even Linux servers) independent of AD
  - Combination of text files, XML, LDAP, scripts
  - Parallel administration of Linux systems

© Novell, Inc. All rights reserved.

Current State: Examples

- Automatic shares
  - By user:
    - desktop window managers
  - By administrator:
    - Automounter:
      - stores plaintext passwords
      - Unmount is timeout based
    - pam_mount:
      - Obtain password through pam stack or:
      - Use kerberos tickets
      - Unmount on logout

© Novell, Inc. All rights reserved.

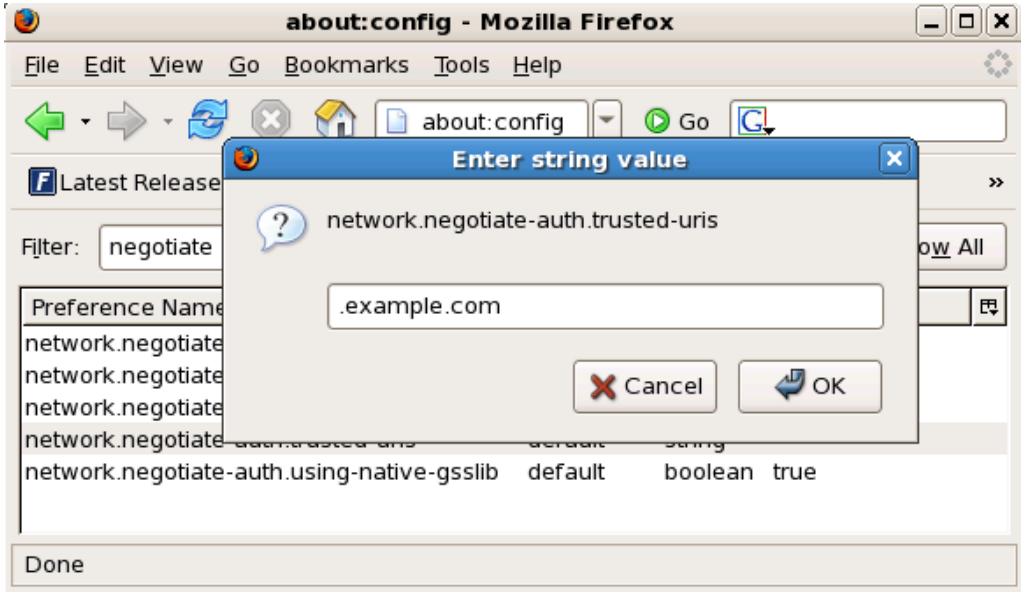
Current State: Examples

- Apache + mod_auth_kerb
  - **Net ads keytab create/add HTTP**
  - .htaccess:
    - AuthType Kerberos
    - AuthName "Krb5 Auth"
    - KrbServiceName HTTP
    - KrbVerifyKDC On
    - Krb5Keytab /etc/krb5.keytab
    - KrbAuthRealms EXAMPLE.COM
    - KrbMethodNegotiate on
    - KrbMethodK5Passwd on
    - require valid-user

© Novell, Inc. All rights reserved.

Current State: Examples

- Firefox
  - about:config or prefs.js:
    - network-negotiate-auth.delegation-uris
    - network-negotiate-auth.trusted-uris



© Novell, Inc. All rights reserved.

Centralizing Administration

Centralizing Administration

- CIM/WBEM (e.g. SBLIM, OpenWBEM, OpenPegasus)
  - Standards-based (DMTF)
  - Provides monitoring, management, configuration
  - Large entry effort
- Puppet - http://projects.puppetlabs.com
  - Open source management of dozens of software projects
  - Linux, Unix, Mac
  - Parallel administration to Windows

© Novell, Inc. All rights reserved.

Group Policy

- Flexibly apply policies to users, machines, groups
- Freedom to leave partial local control
- Once infrastructure is in place, simple to develop basic templates, extensions, and snap-ins
- Common aspects of Windows and Linux managed in one place
- Also applies to server
- And...we have a prototype (thanks to Günther Deschner, see 2007 and 2008 SambaXP archives)

© Novell, Inc. All rights reserved.

Group Policy in Samba

- Current prototype state:
  - Download policies and templates
  - Store some settings in registry config
  - Separate winbind child or net command queries and applies policies
  - Run startup, shutdown, logon, logoff scripts

© Novell, Inc. All rights reserved.

Next Implementation Steps

To-dos: Group Policy

- Complete prototype
  - Clean up and complete registry interface
  - Determine interaction between system settings and policies
  - Recognize more common settings
  - Define CSE interface
  - Common source!
- Provide sample Administrative Templates
  - Store settings in samba registry
  - Accompanying scripts
  - Common system utilities, e.g. sudo, firewall

© Novell, Inc. All rights reserved.

To-dos: Group Policy

- Implement desktop CSE
  - gconf (or ksyscoca, etc.)
  - Short term: simple registry-style interface
  - Longer term: snap-in
- Samba registry-backed API
  - Enable Linux applications to query policy settings

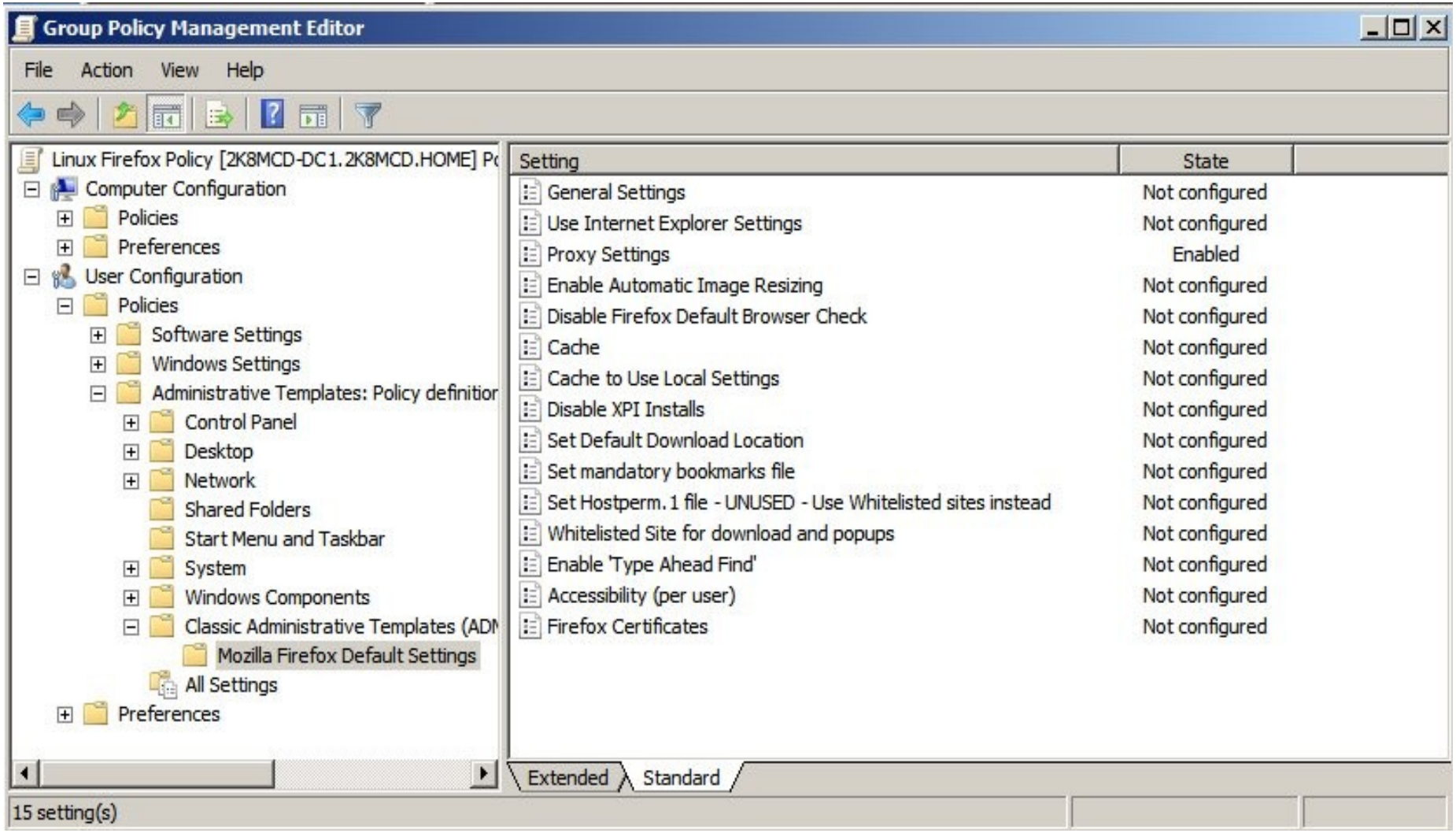
© Novell, Inc. All rights reserved.

To-dos: Group Policy

- Firefox
  - Administrative template
    - Default settings
    - Lockdown
    - Per-user settings
  - Script manipulation of .js files
- Openoffice
  - Administrative template
  - Manipulation of xml files
  - Snapin ?

© Novell, Inc. All rights reserved.

Sample Firefox template



© Novell, Inc. All rights reserved.

To-dos: Group Policy

- Create client extensions for many preferences (Windows 2008)
  - Mapped drives
  - Power options
  - Environment variables
  - Lots more...

© Novell, Inc. All rights reserved.

Questions?

© Novell, Inc. All rights reserved.

He’ll be standing up here in just a moment...

© Novell, Inc. All rights reserved.


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.