

Tiger Directory Services Review

Changes in Tiger and Tiger Server

P224

Michael Bartosh
4AM-Media

Introduction

- Architectural Changes Affecting both Tiger and Tiger Server
- Server-specific changes and new features



Architectural Changes

- New Shadow Hash architecture
- Nested Groups
- ACL's
- Active Directory Plug-in



New Shadow Hash Architecture

- Old: NTLMv1 and SHA-1
 - New: Client only stores SHA-1 by default
 - Server stores NTLM (v1 and 2) by default, but supports everything needed to support authentication for Server Services.
 - Password Server is not running unless you upgraded.
 - Demo: hash architecture and pwpolicy



Nested Groups

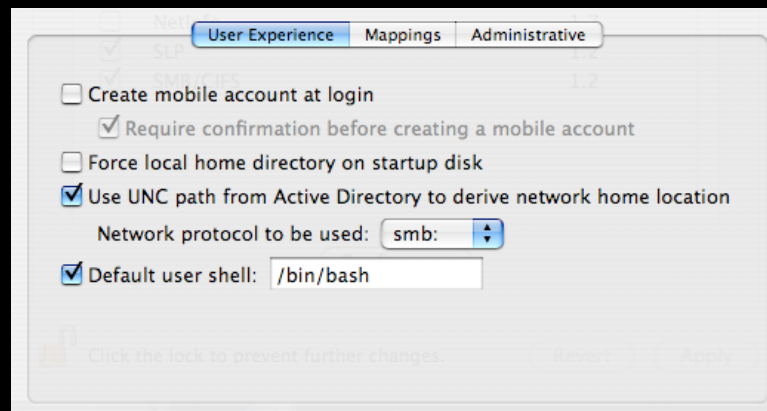
- Groups Within Groups
 - Nested groups, or subgroups
- GUI: Workgroup Manager
 - Demo
- cli: dseditgroup
 - Demo

```
localhost:~ mb$ dseditgroup -n /  
LDAPv3/127.0.0.1 -o edit -u 4am -p -a admin -t  
group www  
Please enter user password:
```



Active Directory

- Support for Nested Groups
- Static Mapping (good for Mail Server)
- NTLMv2
- “Kerberos” proxy authentication (good for VPN)
- GUI support for network homes and protocol choice
- -enablesso (server only)



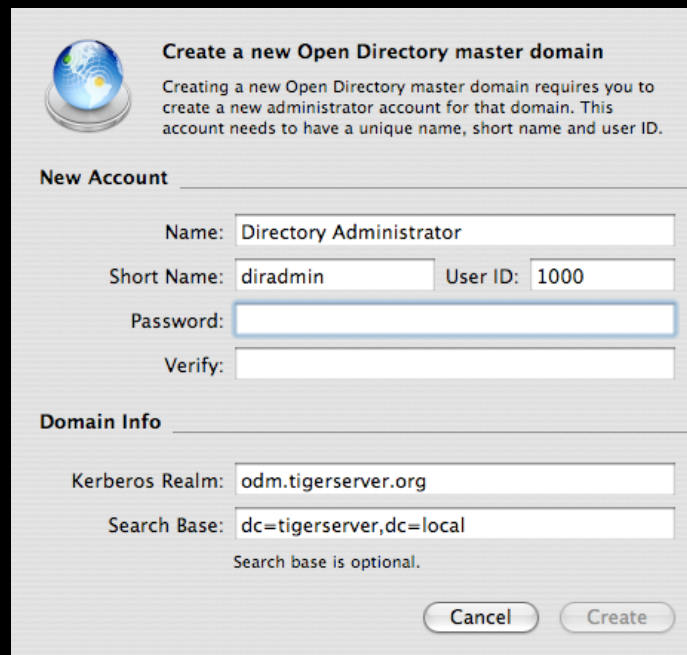
Server-Specific Changes


- No more naming conflicts
- in-directory ACL's
- kerberized LDAP
- Binding Policies
- Machine Accounts and Authenticated Binding



Master Creation Process

- Admin user no longer copied from local domain.
 - slapconfig -createldapmasterandadmin
- slapconfig log is more verbose and available in gui



 **Create a new Open Directory master domain**

Creating a new Open Directory master domain requires you to create a new administrator account for that domain. This account needs to have a unique name, short name and user ID.

New Account

Name:

Short Name: User ID:

Password:

Verify:

Domain Info

Kerberos Realm:

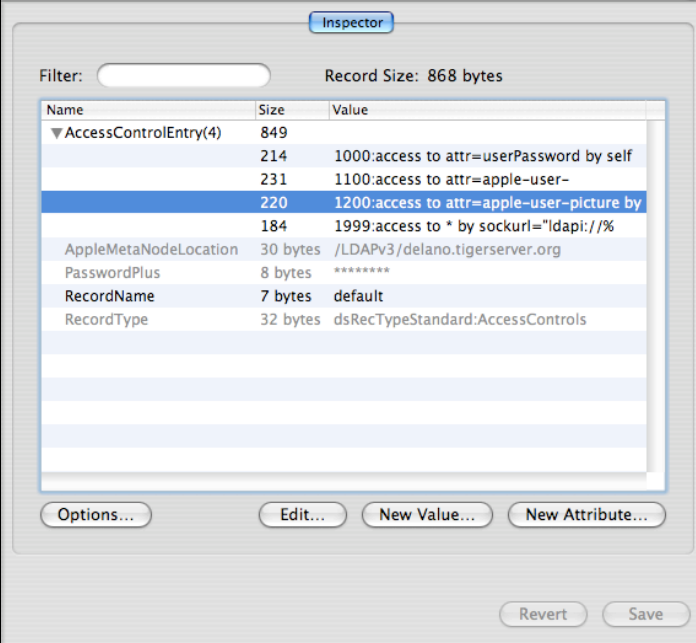
Search Base:

Search base is optional.



In-directory ACL's

- Access controls are stored in LDAP database
- This means they are replicated.
- Paves the way for more granular control to the directory



Inspector

Filter: Record Size: 868 bytes

| Name | Size | Value |
|-------------------------|----------|---|
| ▼ AccessControlEntry(4) | 849 | |
| | 214 | 1000:access to attr=userPassword by self |
| | 231 | 1100:access to attr=apple-user- |
| | 220 | 1200:access to attr=apple-user-picture by |
| | 184 | 1999:access to * by sockurl="ldapi://% |
| AppleMetaNodeLocation | 30 bytes | /LDAPv3/delano.tigerserver.org |
| PasswordPlus | 8 bytes | ***** |
| RecordName | 7 bytes | default |
| RecordType | 32 bytes | dsRecTypeStandard:AccessControls |

Options... Edit... New Value... New Attribute...

Revert Save



Kerberized LDAP

- After kinit, easily modify the directory securely using ldapadd, etc.



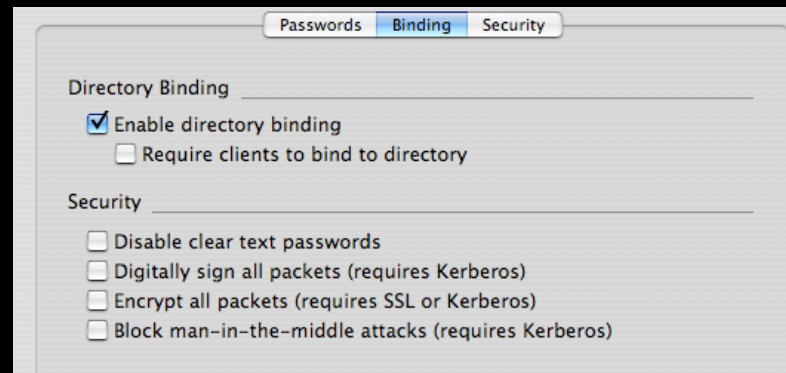
Machine Accounts and Authenticated Binding

- Directory no longer has to be world readable
- Machines maintain unique account with domain; it is used to query the directory
- Much like Active Directory



Binding Policies

- Variety of Security Options
 - Disable clear text passwords
 - Digitally sign all packets
 - Encrypt all packets
 - Block man-in-the-middle attacks
- THESE ARE ADVISORY. ANOYMOUS ACCESS IS STILL ENABLED.



Distributed Authorization in Open Directory

- What is it?
 - delegate certain administrative tasks to non-admins
 - permit use of Workgroup Manager
 - Make use of OU's
- How?
 - Essentially, a combination of custom mappings and ACL's



Distributed Authorization in Open Directory

- create OU's (phpldapadmin is a nice tool)
- Delegate administration using LDAP ACL's
 - Use WGM's All Records tab to add another value to the AccessControlEntry attribute on the default AccessControl entry

```
-1300:access to dn.sub="ou=marketing,dc=example,dc=com" by group/posixGroup/  
memberUid="cn=admin,cn=groups,ou=marketing,dc=example,dc=com" write by * read
```

- Custom mappings
- WGM unlocks if you can authenticate as a user in the “admin” group, even if it is not the domain-level admin group.



Distributed Authorization: Custom Mappings

| Record Type | Mapping |
|----------------|--|
| Users | cn=Users,dc=example,dc=com |
| AccessControls | cn=accesscontrols, dc=example,dc=com |
| Groups | cn=Groups,ou=marketing,dc=example,dc=com |
| Computers | cn=Computers,ou=marketing,dc=example,dc=com |
| Computer_Lists | cn=Computer_Lists,ou=marketing,dc=example,dc=com |



Tiger Directory Services Review

Changes in Tiger and Tiger Server

P224

Michael Bartosh
4AM-Media