



Red Hat View on Kerberos

Interoperability in Mixed Environments

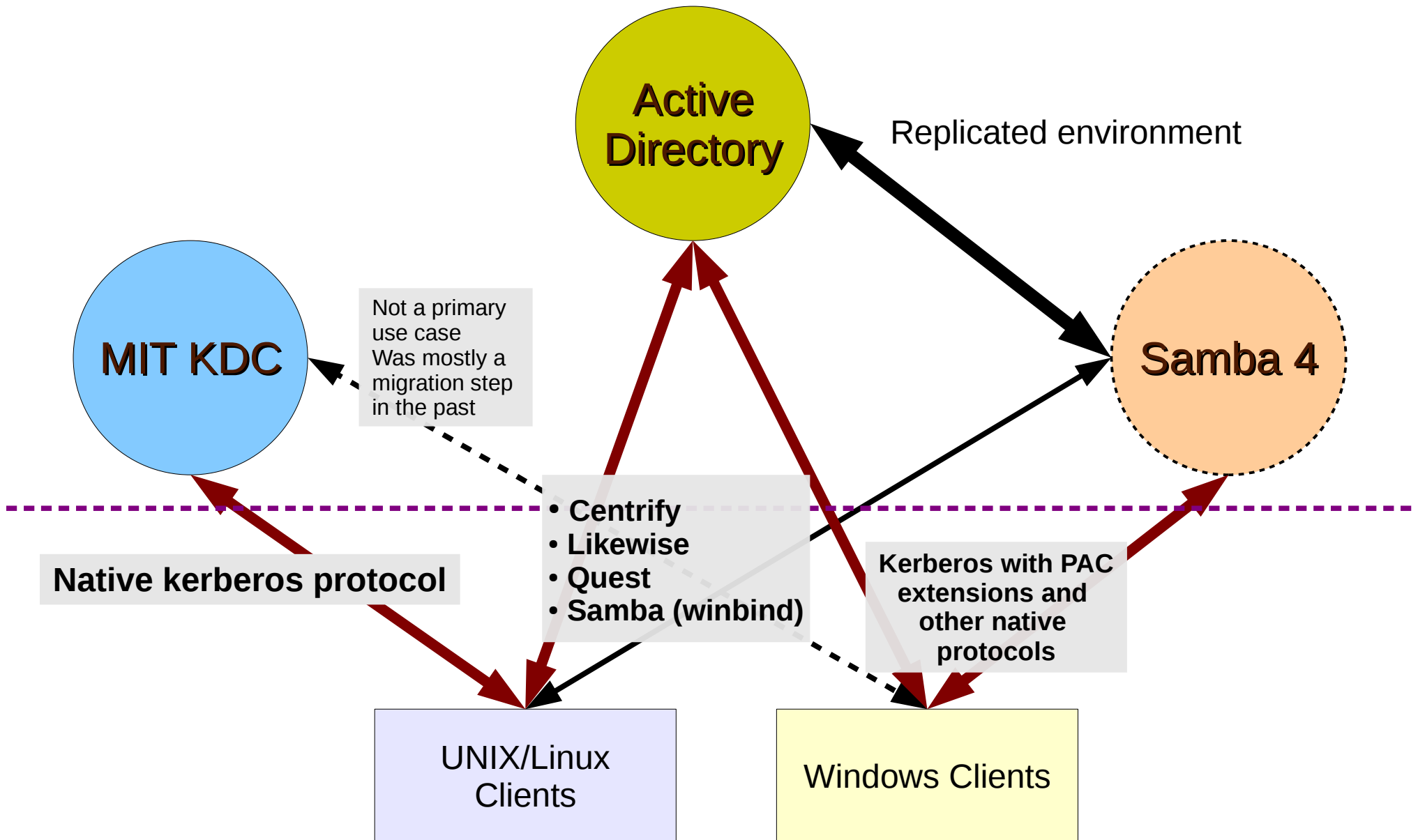
Dmitri Pal

Sr. Engineering Manager

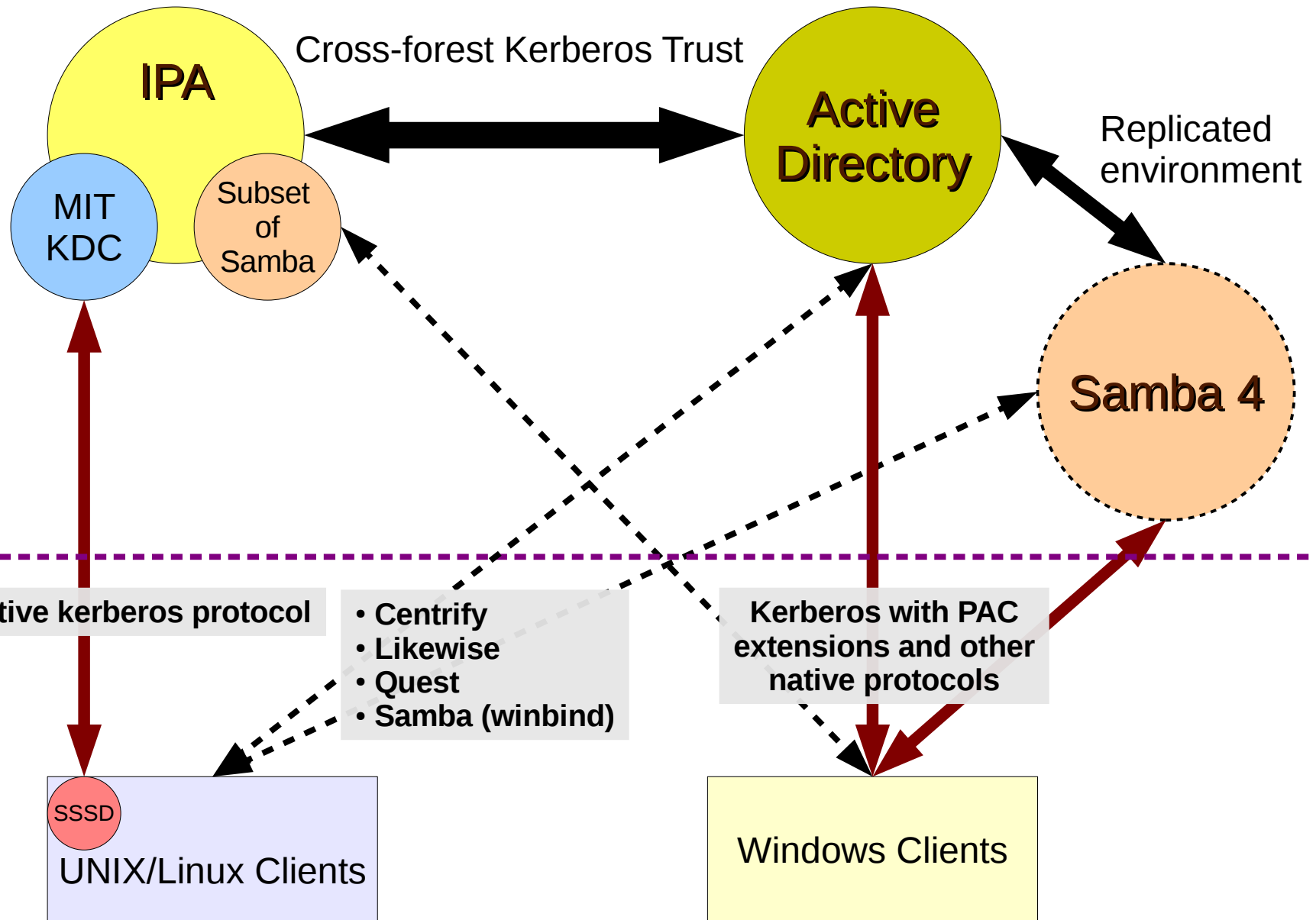
Red Hat Inc.

10/26/2010

Traditional view on Kerberos interoperability



Extended View



IPA

- Stands Identity Policy Audit mostly Identity and Some Policy. Audit is deferred for now.
- It is a domain controller for UNIX/Linux environments, successor of NIS and an alternative to pure LDAP or pure Kerberos solutions bringing the best of the two worlds together
- Glues MIT Kerberos with 389 Directory Server
- Open source project – freeIPA. Started about 3 years ago
- A Red Hat supported version of IPA is planned for for next calendar year. Will leverage MIT Kerberos 1.9.
- IPA adds unified Kerberos password handling via Kerberos protocol or LDAP
- Main features:
 - Host identity
 - DNS
 - Server Certs
 - HBAC
 - Automount
 - Netgroups
 - SUDO
 - etc.



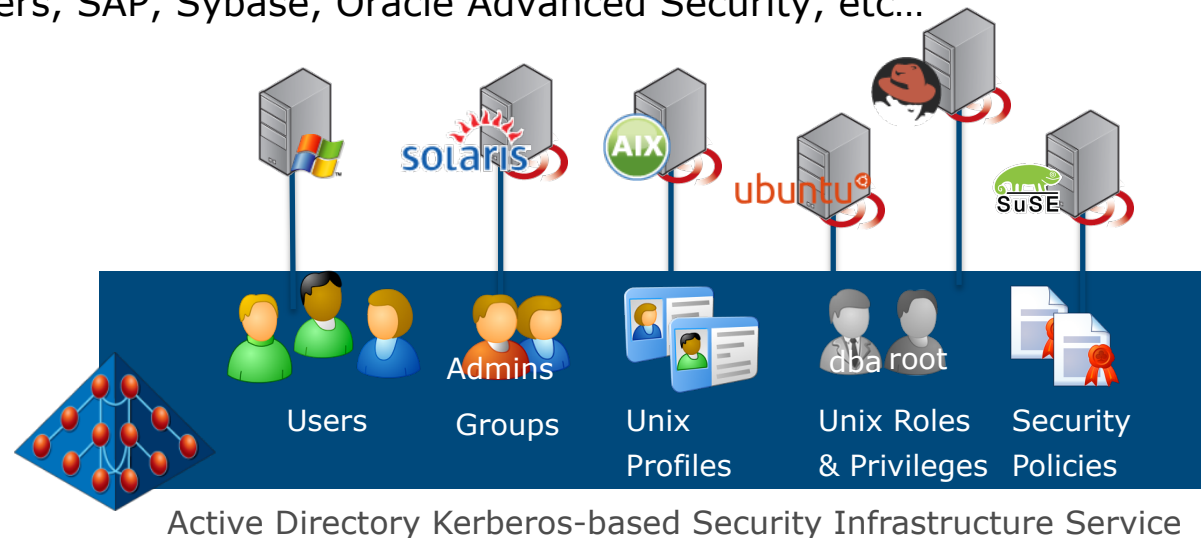


Cross Platform Kerberos Interoperability

David McNeely
Director of Product Management
Centrify Corporation
David.McNeely@Centrify.com
(408) 542-7518

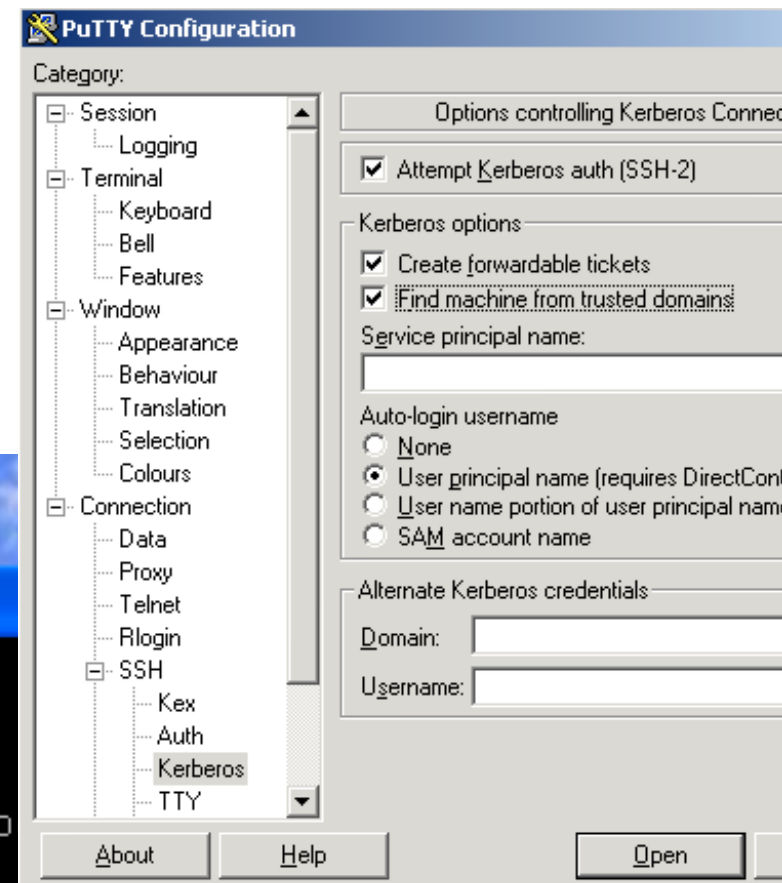
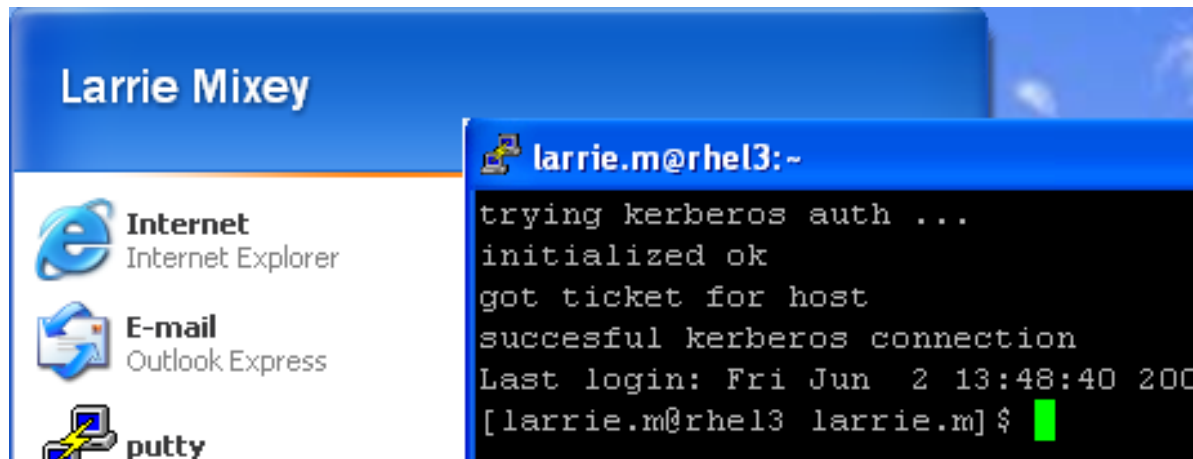
Cross Platform Kerberos Interoperability

- Integration into UNIX, Linux and Mac for Windows interoperability
 - Kerberos services support cross platform interoperability for strong authentication
 - Centrify Suite modifies MIT Kerberos to ensure smooth AD interoperation (domain detection, suppress DNS traffic, transient trust support,...)
- Integration into UNIX/Linux services via automated Kerberos config:
 - OpenSSH, Samba, NFSv4, etc...
 - Apache, J2EE App Servers, SAP, Sybase, Oracle Advanced Security, etc...



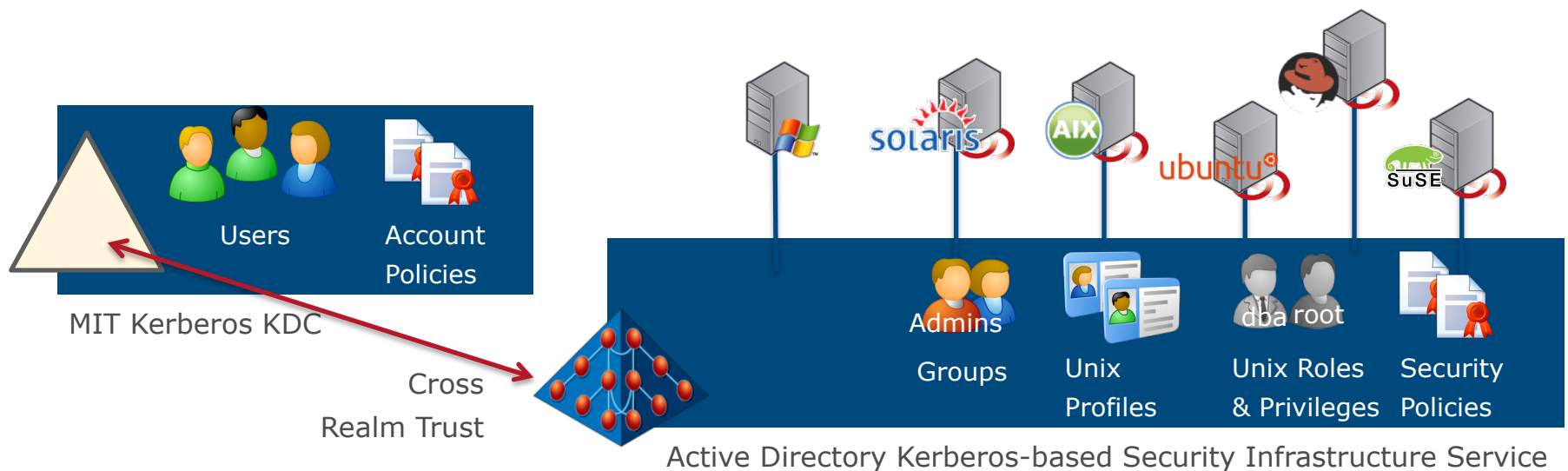
Kerberizing OpenSSH and PuTTY

- OpenSSH is linked with the DirectControl's Kerberos libraries
 - Aware of Kerberos tickets and PAM
 - No need for a .k5login file
 - Works with any of the computer's valid hostnames
- PuTTY is linked with Windows Kerberos library
- Windows users provided Single Sign-On to UNIX



Cross Platform KDC Interoperability

- KDC interoperability is provided through 2-way cross trusts
 - Active Directory KDC is used to manage resource accounts and security policies
 - Users from MIT KDC can login to authorized AD computers and applications



F5-ARX and Kerberos

MIT Kerberos Consortium 2010

JC Ferguson
Director/Architect - Product Development
Lowell, Massachusetts
email: jc@f5.com

October 2010



Product overview

- Storage virtualization product:
 - Started as Acopia Networks in 2002.
- Adds a second ‘tier’ to storage architectures positioned between clients and file servers.
- Supports both NFS and CIFS network file-access protocols.
- Benefits:
 - Global namespace / single mount point
 - Cost savings by tiering old data to cheaper storage
 - Vendor mobility – seamless migration from one vendor to another vendor’s storage device.

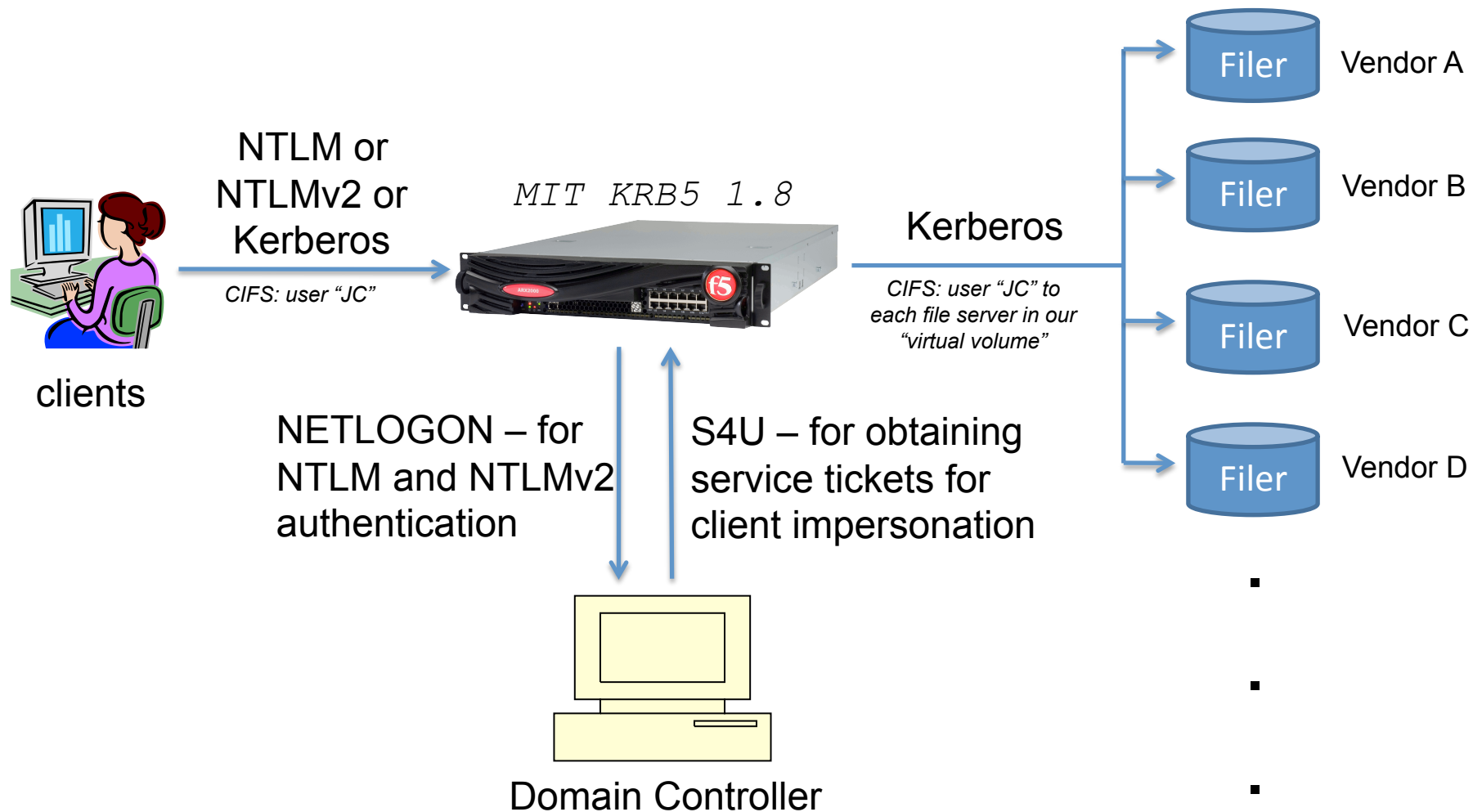


Challenge: Authentication model

- As a proxy device, we really had two choices:
 - Do all authentication and authorization to file objects on the F5-ARX device.
 - Do initial authentication on the F5-ARX device and defer authorization to file objects to the file servers.
- The former would require us to read and process ACLs on file objects:
 - Would require a lot of interaction with Active Directory.
 - Getting it incorrect would have negative consequences.
- We ultimately chose the latter (next slide)



F5-ARX Authentication Architecture



Hadoop's Kerberos Interoperability



Owen O'Malley
owen@yahoo-inc.com
Yahoo's Hadoop Development

Kerberos Conference 2010



What is Hadoop?

- A framework for big data computation
 - Supports 4,000 machine clusters, 10's of PB
 - Mixes distributed storage and computation for very high throughput.
 - Critical to Yahoo!, Facebook, Twitter, LinkedIn
 - 40,000 dedicated Hadoop machines at Yahoo!
 - Runs on Linux, Solaris, MacOS, or Windows
 - Written primarily in Java
 - Possible to run in Amazon's EC2



Java Challenges

- Implemented their own code instead of linking with C library.
 - Configuration file differences (`udp_preference_limit = 1`)
 - Way too many OS switches (Win, Sun, Linux)
 - Need “extra” files installed in JVM to
- Shipped with JVM, very hard to change
- Most of the Kerberos classes are private
 - Compiler warnings if you use them instead of JAAS
 - Not portable between JVMs
- Thank goodness for OpenJDK!



HTTP Challenges

- Mostly use RPC, but HTTP is important
- SPNEGO
 - Service Principal Name: *HTTP/hostname*
 - Supported by most browsers
 - Requires configured white list of URLs on each client
 - No Java Support
- TLS/Kerberos
 - Service Principal Name: *HOST/hostname*
 - Not supported by browsers
 - Client Java support