LDAP Implementation
AP561x KVM Switches

All content in this presentation is protected – © 2008 American Power Conversion Corporation

LDAP Implementation

- Does not require LDAP Schema to be touched!
- Uses existing Schema Attribute field to store configuration setting
- Allows easy implementation

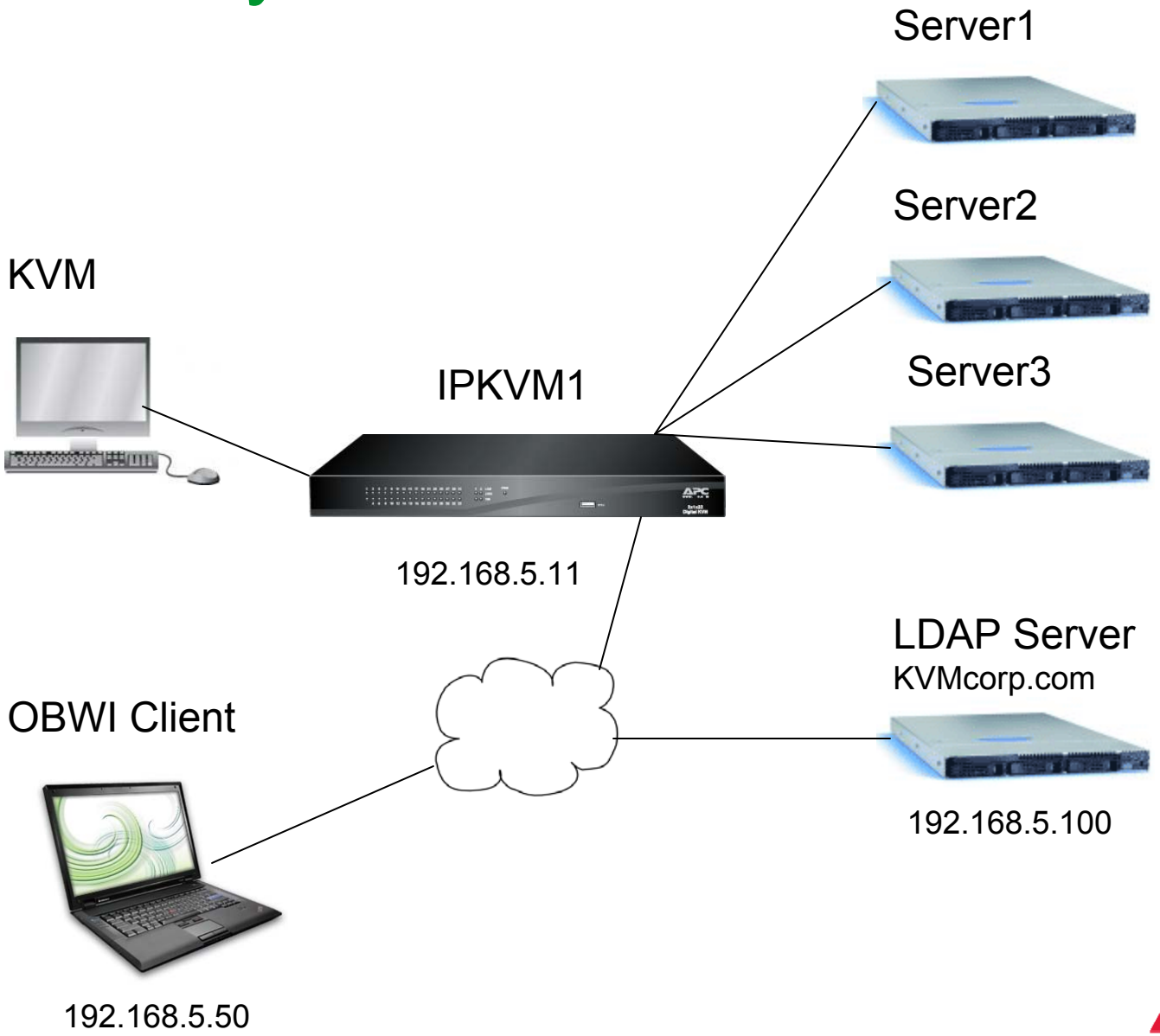
IP KVM authentication levels

- Basic
  - Very simple implementation that allows the KVM to browse the LDAP directory for user credentials. All users are administrators
- Attribute
  - Allow users in the LDAP directory to be distinguished as non-users, appliance administrators or users
- Group
  - Provides highly granular security down to the port level

Settings Used in this Lab

- The Microsoft® domain controller (Active Directory) acts as the DHCP server and DNS server in these examples.
- The domain is **kvmcorp.com**.
- The user account that is used to query the domain controller for authentication and access controls is **kvmldap**.
- The OU (Organizational Unit) for grouping APC IP KVM Switches and users is **IPKVM**.
- The IP Address of the IP KVM Switch is 192.168.5.11
- The IP Address of the AD Server is 192.168.5.100
- The IP Address of the Client is 192.168.5.50

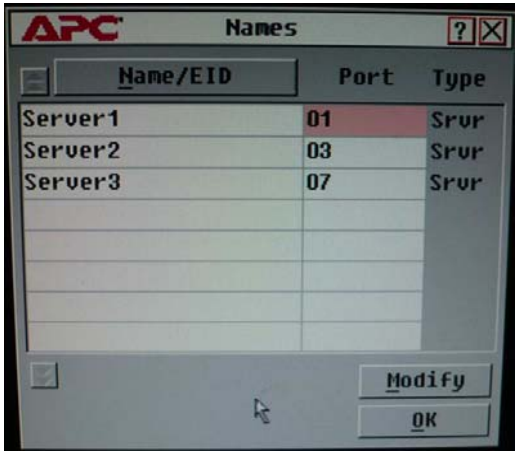
LDAP Lab Layout



Synchronize Server Module names to AD Computer Object names

- Name the Server Modules to match exactly the names of the computers with which they are connected. This must be done using the OSD from the local port on the IP KVM switch. The domain controller's server modules should have a different name than the domain controller. A computer with the same name representing the domain controller should be added separately to the directory for IP KVM access because the domain controllers are not listed under computers in the Active Directory, and the domain controllers folder is not browsable to the Admin accounts.
- For example, the interface adapter for the domain controller KVMcorp-AD is named KVMcorp-AD-SM, and a computer is created with the name KVMcorp-AD-SM. A standard user cannot authenticate for a domain controller.

Name the Server Modules via the Local Port OSD



From the local OSD, press the **Print Scrn** key. The Main dialog box appears. Click the name you want to change, and click **Modify,** rename the server module and click **OK.**

Remember, the server names here must match the computer object names in the directory!

Active Directory Tasks

NOTE: In a production environment, work with your IT department to create the console query user account and add the IP KVM switches OU. You need a level of access that enables you to create, delete, modify groups, and add computer objects for interface adapters connected to non-domain systems within the IP KVM switches OU. Use the Microsoft® MMC to access the Active Directory from another server or a client workstation.

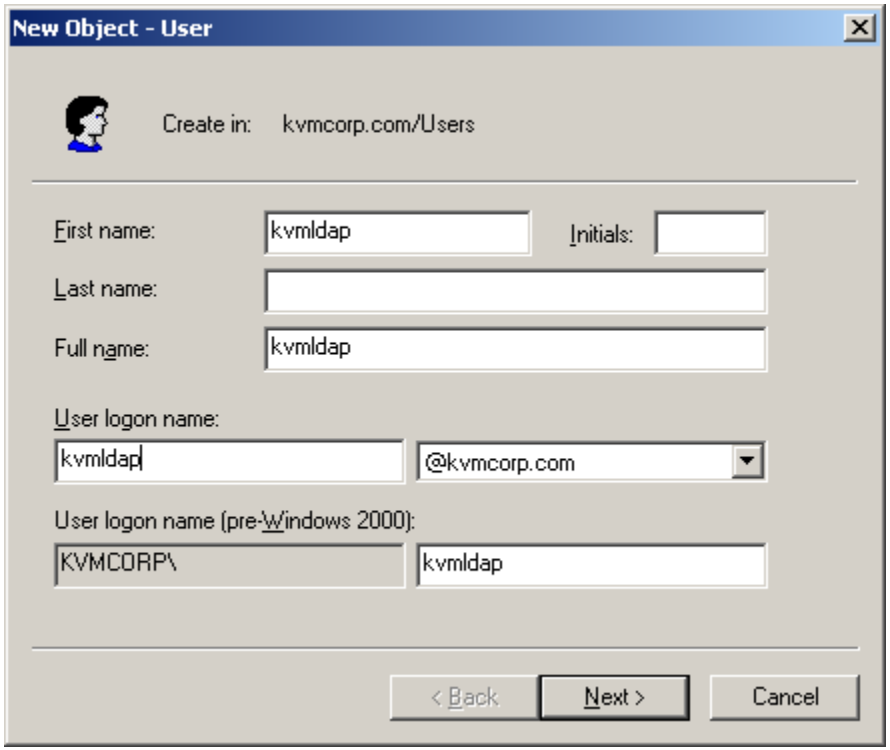
To administer the directory from the domain controller console, click **Start>Programs>Administrative Tools>Active Directory Users and Computers.**

On the domain controller, add an OU group container named **IPKVM** to Active Directory in the root of the domain for the IP KVM switch administrative groups.

1. Right-click **kvmcorp.com.**
2. Select **New Organizational Unit.**
3. Name it **IPKVM**
4. Click **OK.**

Create User to Browse the Directory

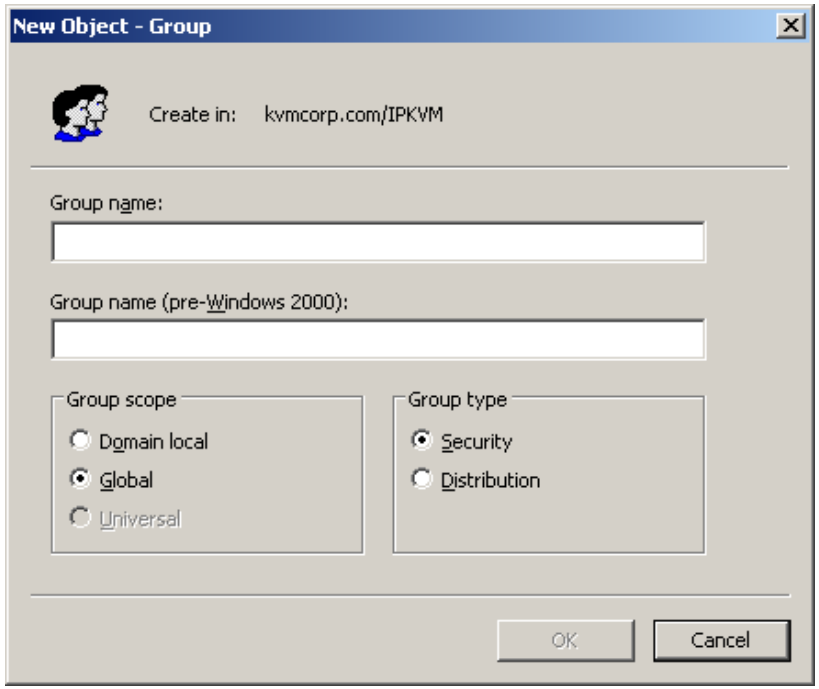
This is a special user account specifically for LDAP queries instead of using the Admin account



Create a user named **kvmldap**, and assign the password: **Password1**
Set the Password not to expire

Create two groups for IP KVM switch administrators and users.

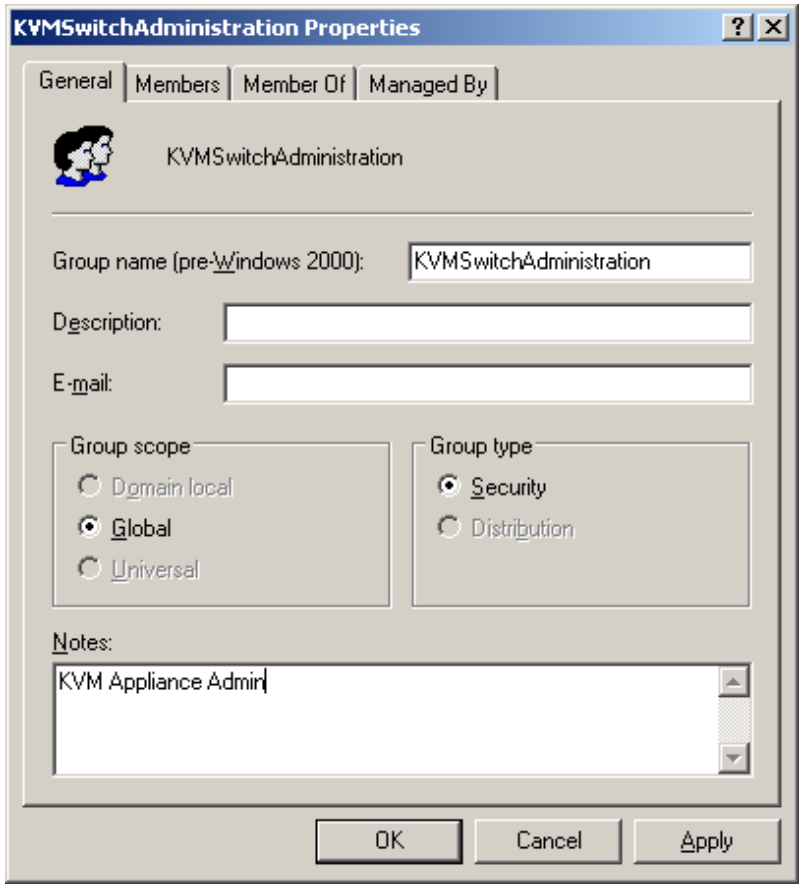
1. Right-click **IPKVM OU.**
2. Choose **New Group.**
3. Create groups names **KVMSwitchAdministration** and **ServerAdministration**.



NOTE: In a production environment, groups in the Active Directory IPKVM OU would match the organization's hierarchy, usually by function, geography, or a combination.

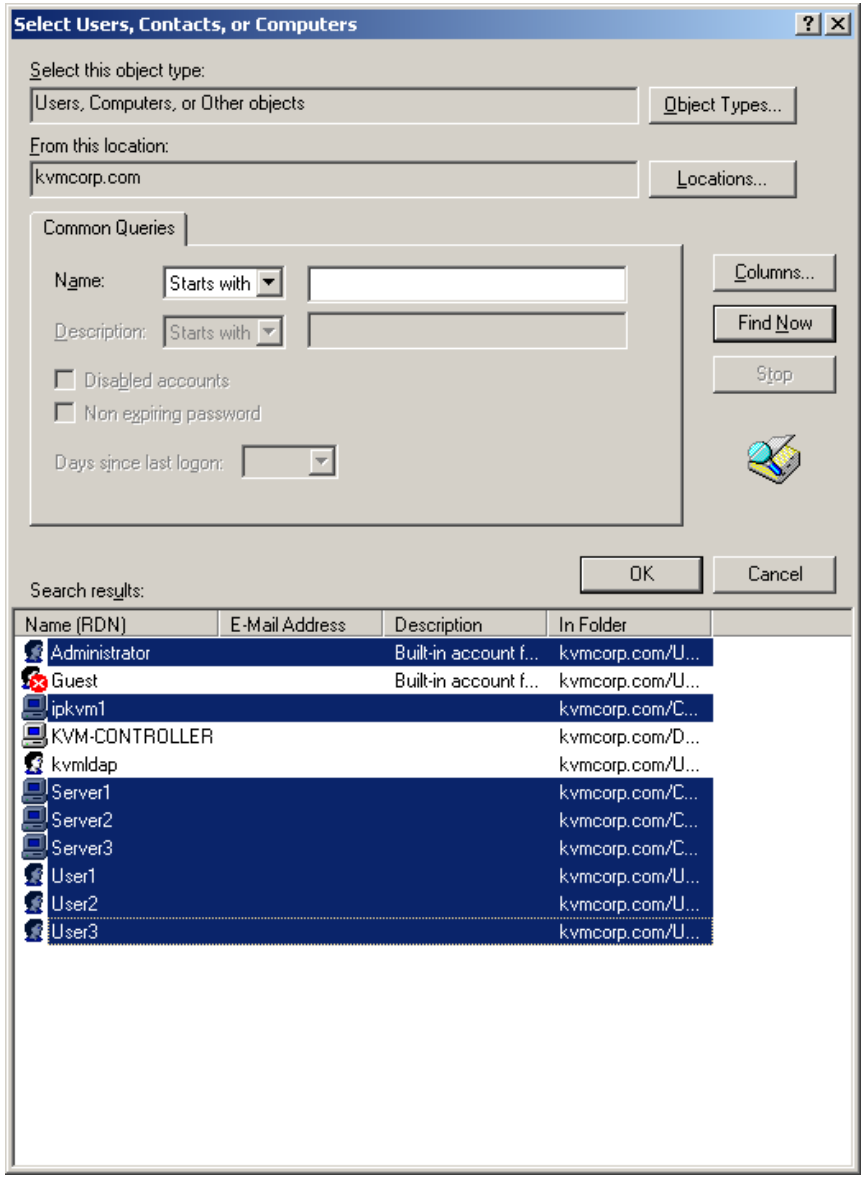
Set up the default access control for the Server Administration group by right-clicking the group object and selecting **Properties** for the group and entering **KVM User** in the group's notes field.

Set up the default access control for the IP KVM Administration group by right-clicking **Properties** for the group and entering **KVM Appliance Admin** in the group's notes field.

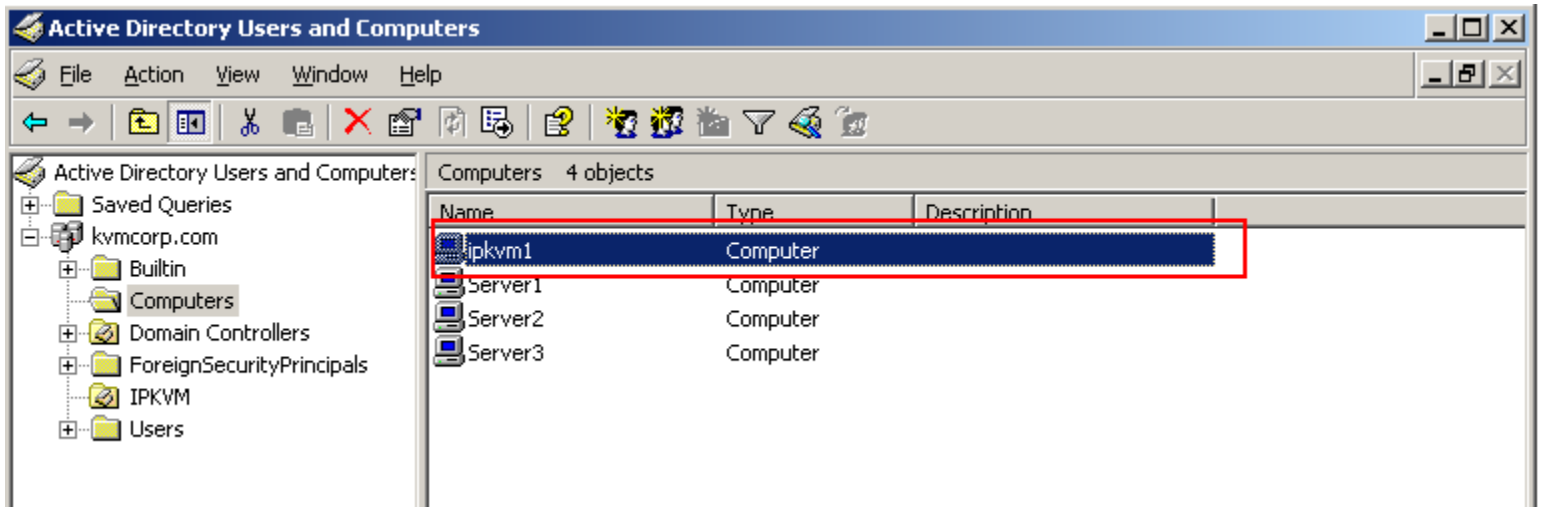


Add the users and Server Modules to the appropriate groups that associate them

1. Right-click each of the two new groups.
2. Click **Properties.**
3. Click the **Members** tab.
4. Click **Add.**
5. Click **Object Types.**
6. Select **Computers and Users.**
7. Click **OK.**
8. Click **Advanced>Find Now.**
9. Add the computer and users that should belong together in the group by clicking the first object holding the **Ctrl** key while clicking the others. Include the KVM switch
10. Click **OK.**



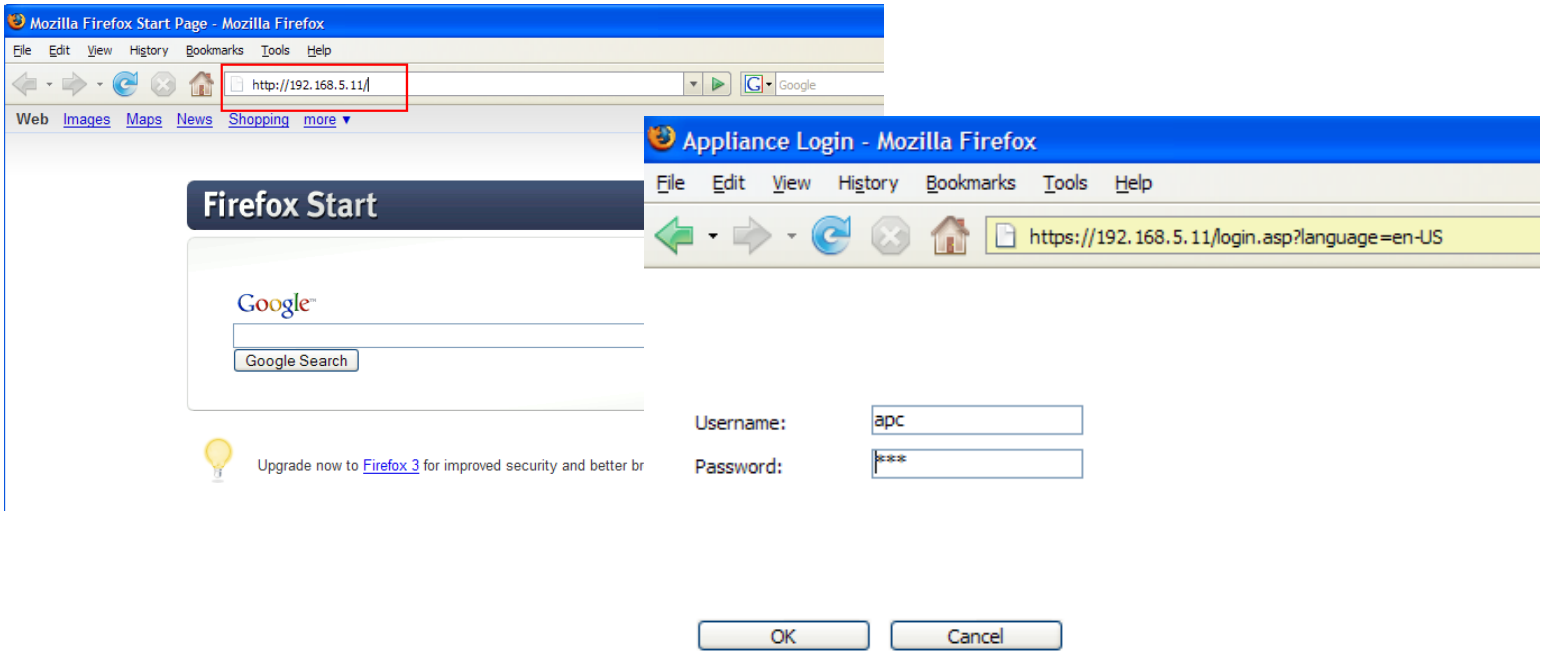
Create Computer Object in AD for the IP KVM Switch



Create a computer object in the directory for each IP KVM switch with the same name as you will give it in the SNMP panel for the switch.

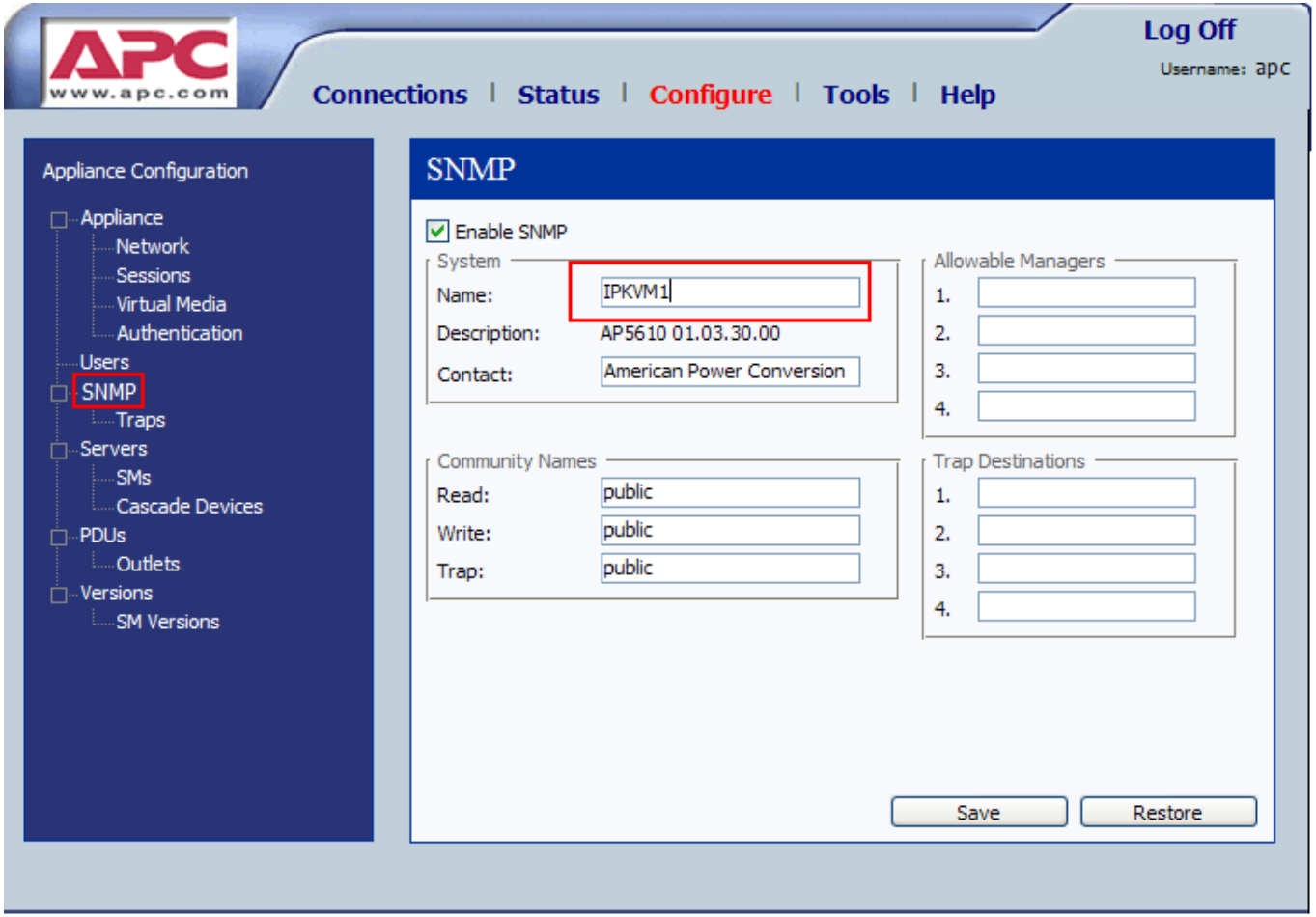
In this Lab, create a computer object named **IPKVM1**. You will give the same name to the IP KVM switch later in this lab.

Log into the Switch



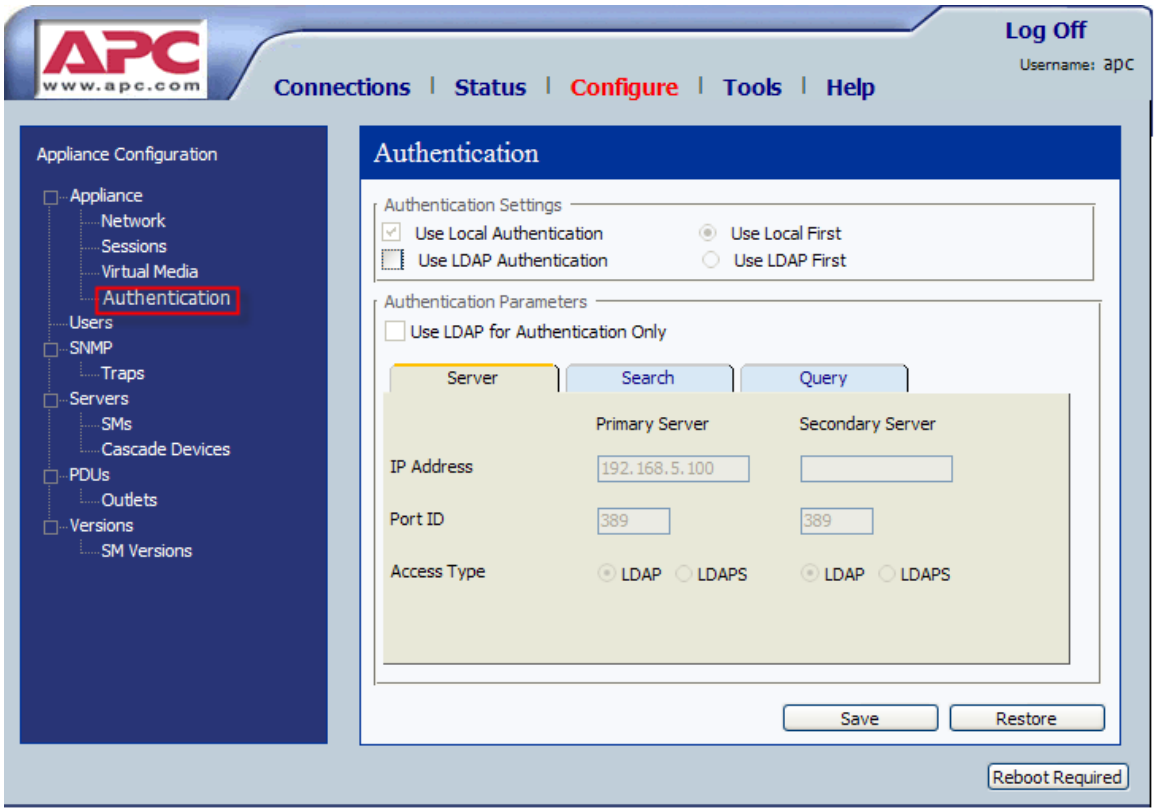
Launch your web browser and point it to the IP address of the IP KVM Switch and login with the default Admin user name & PW: apc and apc

Name the Switch

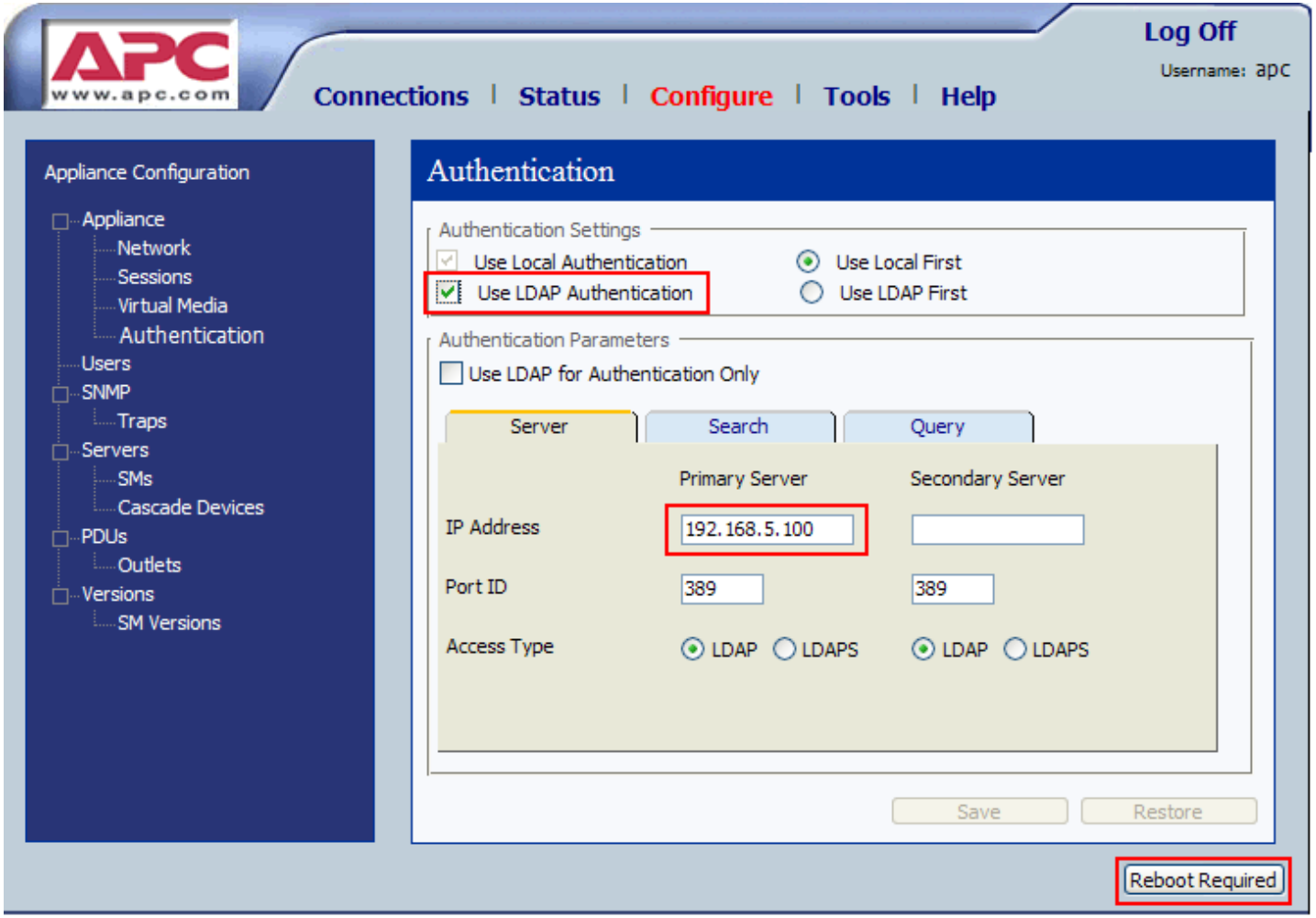


From the Configure screen, select SNMP and name the switch **IPKVM1**

Enable LDAP Authentication



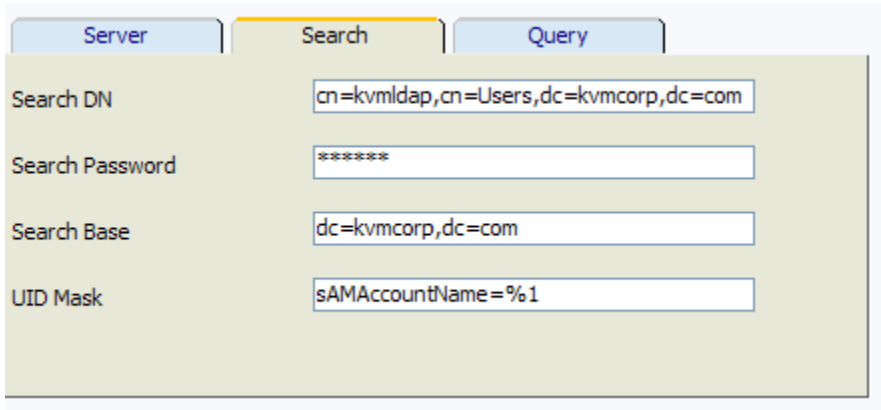
Click on Authentication under Appliance in the Configuration Menu



Check the Use LDAP Authentication box. On the Server Parameters tab, enter the IP address of the **Primary Server: 192.168.5.100** (domain controller).

After this, a reboot of the switch is required. Reboot and log back in as apc with apc as the password and return to the Authentication screen.

Configure LDAP Search Parameters



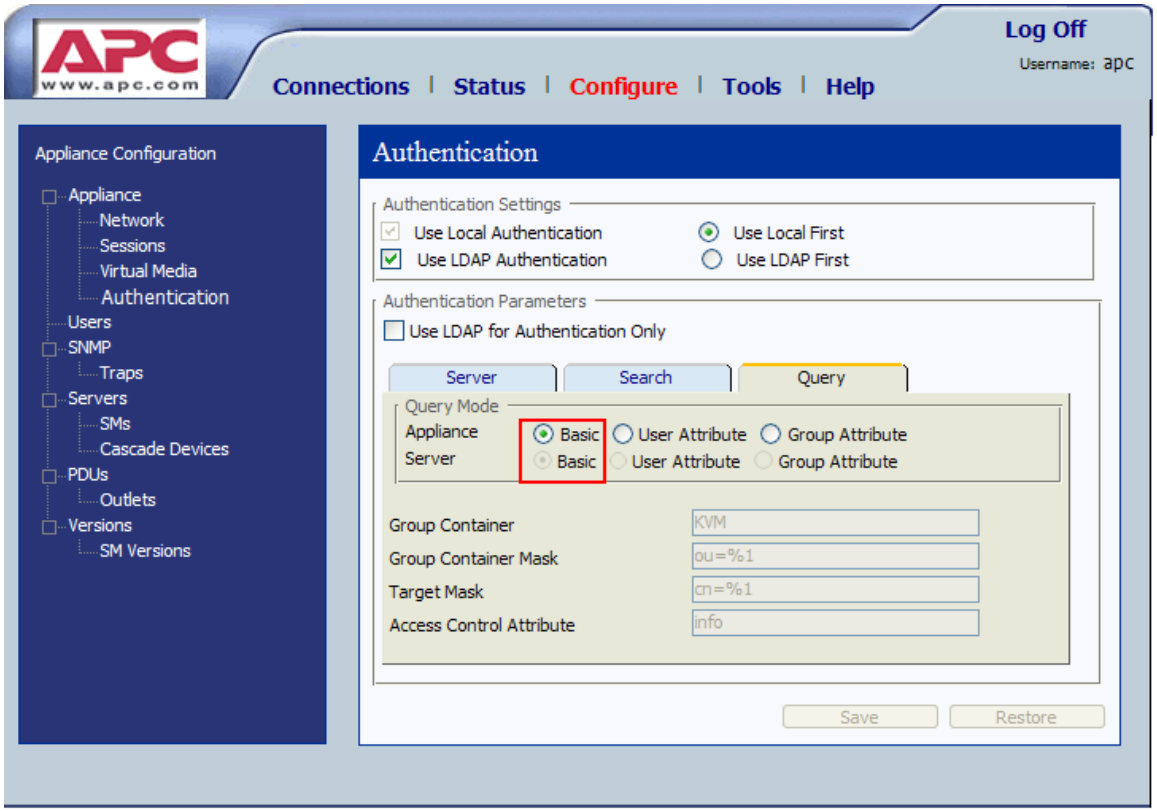
On the Search Parameters tab, enter the Search DN:
cn=kvmldap,cn=users,dc=kvmcorp,dc=com

NOTE: The first cn field must match the full name of the user, not the login name. For example, if the user name is John Doe, then *cn=John Doe* (note the space in the name).

Enter the search password for the kvmldap user account. (*Password1*)
Enter the search base: dc=kvmcorp,dc=com.

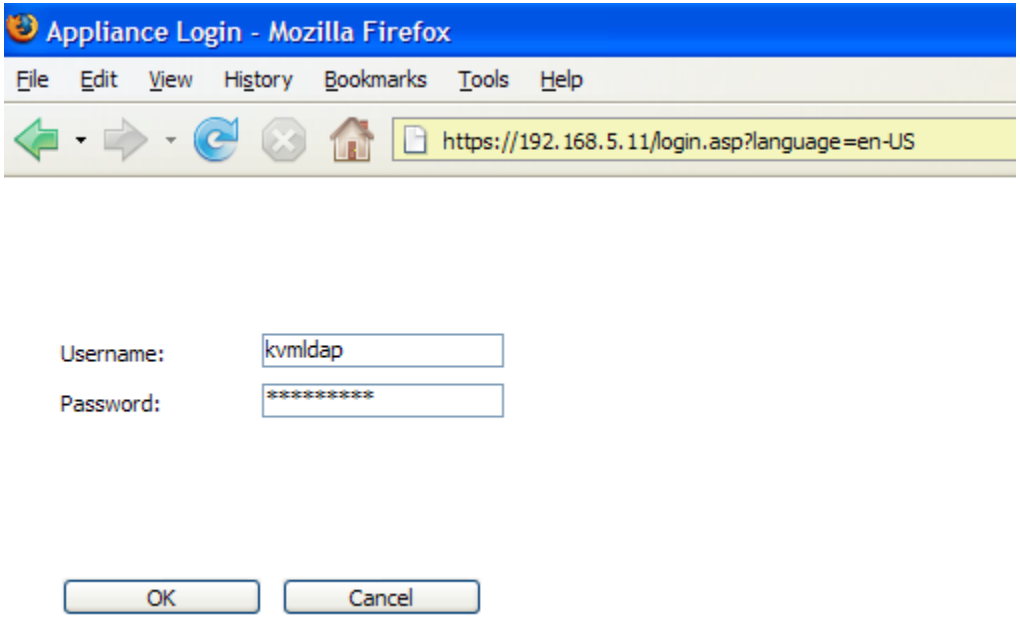
NOTE: The search base should always be at the root of the domain.

Leave Query Parameter at Basic



IMPORTANT: This query mode should be used to test your LDAP configuration only. After the basic LDAP communications configuration is successfully tested, change the query mode because Basic mode gives full administration authorization to all IP KVM switches and all attached servers.

Test the basic LDAP Authentication



Log out of the APC Web Interface and go back to the login prompt. Log in as: kvmldap with the password Password1

(the user you created earlier to browse the network.) It should load the APC Management Page if the switch can communicate to the Directory.

You should also be able to log in with any user name and password that exists in the Directory

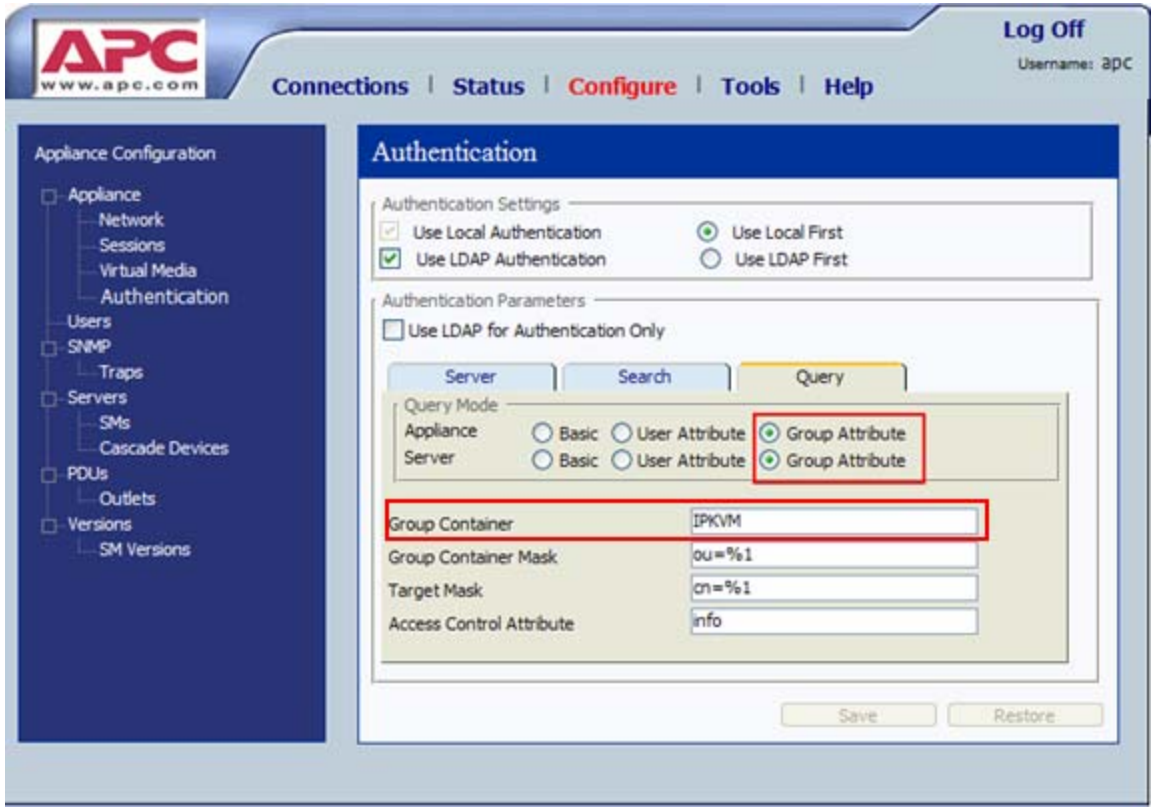
Basic Summary

- Very basic
- Quick to set up
- All users have administrator rights
- Use the “Search Base” in the “LDAP Parameters” to limit user access by adding an OU such as “MIS” or “Administrators”
- Ideal for smaller customers

Group Based Authentication

All content in this presentation is protected – © 2008 American Power Conversion Corporation

Change LDAP Query to Group



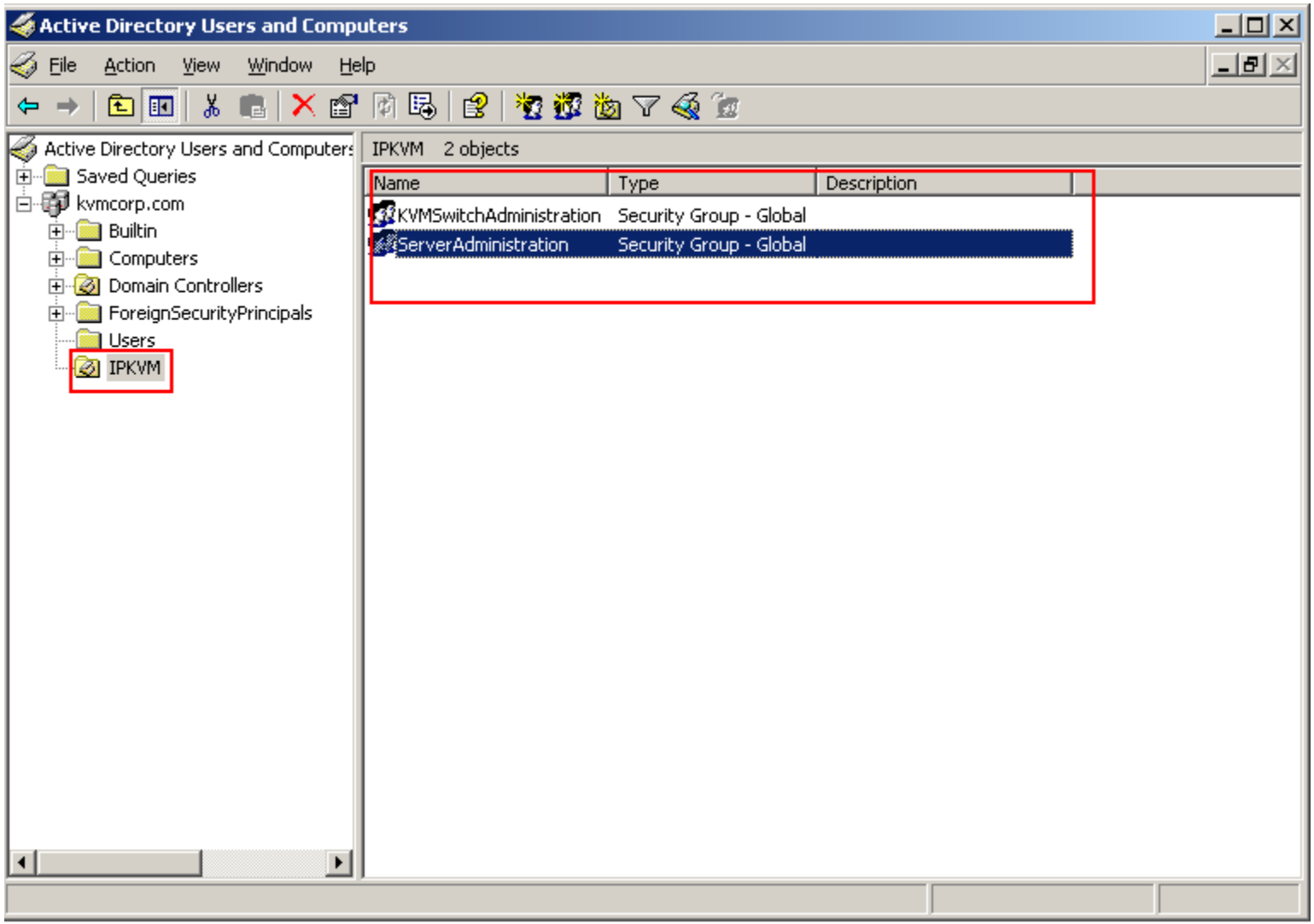
After the basic LDAP communication test succeeds, Log off, then log in to the IP KVM switch as apc with apc as the password.

Click on Configure

Click **Global>Authentication.**

On the Query Parameters tab, click **Group Attribute for Query Mode (IP KVM Switch)** and **Group Attribute for Query Mode (Server).**

Enter the Group Container **IPKVM** and test again



To add or take away rights, just add the Server Module Computer Objects and the Users as members of the respective group. Be sure to include the computer object for the IP KVM Switch as well.

Group Summary

- Highly granular security
- Port level control
- Attributes set to groups rather than individual users
- Hugely scalable
- Ideal for Enterprise customers

Conclusion

- LDAP allows you to integrate your KVM with your security infrastructure to provide an easy to use yet powerful management tool to keep your servers up and running