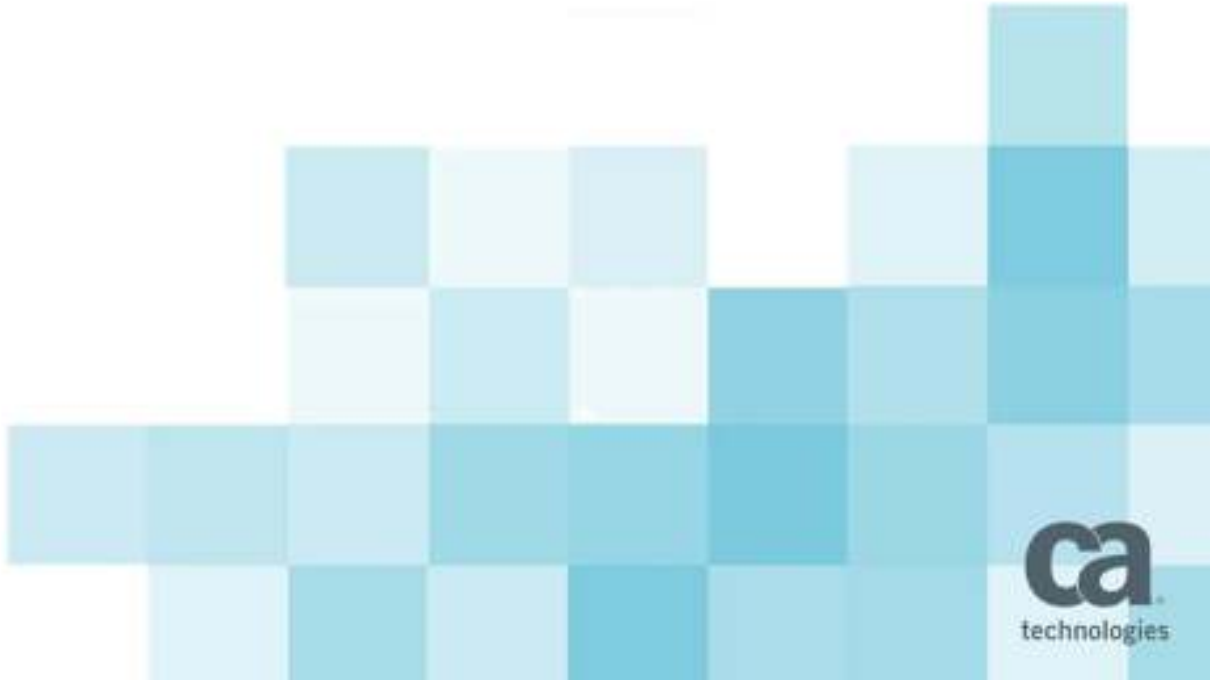
How to setup SiteMinder Kerberos Authentication – Part 1

Sung Hoon Kim

Date

14 January 2015



Setting up SiteMinder Kerberos Authentication

- ***This is for Setting up on Windows Environment***
- ***Index***
  - Overview
  - Pre-requisites
  - Use case
  - Configuration steps
  - Testing the setup
  - Troubleshooting
  - Misleading Instructions / Pitfalls

Overview

Kerberos Authentication offers seamless, trust based and fast authentication.

This guide is to help implement Kerberos authentication in siteminder environment.

There are differences in pure Kerberos setup and siteminder Kerberos setup.

In a pure Kerberos environment you need 3 parties(client, web/app server and KDC) but in case of SiteMinder Kerberos environment there is policy server in addition and there are delegation involved between webagent and policy server where it becomes a challenge in the implementation as it is not so much common in pure Kerberos environment.

Pre-requisites

- Reason for choosing Windows 2008 is it is current supported and policy server is not yet certified for Windows 2012.
- Reason for choosing R12.52SP1 is it is currently latest major release and has out of the box Kerberos Authentication Scheme.
- Reader must have SiteMinder Administration Knowledge as many trivial steps are not mentioned in detail.
- Reader must have knowledge on how Kerberos works.

Machine #1

- Machine 1: Windows Domain Controller
  - Windows Server 2008 R2 SP1
  - AD (KDC and UserStore)
  - DNS
  - Time Synchronization

Machine #2

- Machine 2: SiteMinder Policy Server
  - Windows Server 2008 R2 SP1
  - R12.52SP1 (Policy Server and AdminUI)
  - JDK 1.7.0_51 (32bit)

Machine #3

- Machine 3: SiteMinder Web Agent
  - Windows Server 2008 R2 SP1
  - IIS 7.5
  - R12.52QMR1

Machine #4

- Machine 4: End user desktop client
  - Windows 7 Enterprise or Ultimate
  - IE 11

Use case

KERBEROS REALM = AD DOMAIN = COOKIE DOMAIN

In this specific use case, it is pure windows environment.

- A Windows Domain user logon to his/her desktop.
- Open IE and navigate to siteminder protected resource (Intranet zone).
- IE performs Negotiate with webagent
- WebAgent delegates authentication to policy sever
- Policy Server Authenticates the user.
- WebAgent sets SMSESSION cookie and grant access to protected resource.

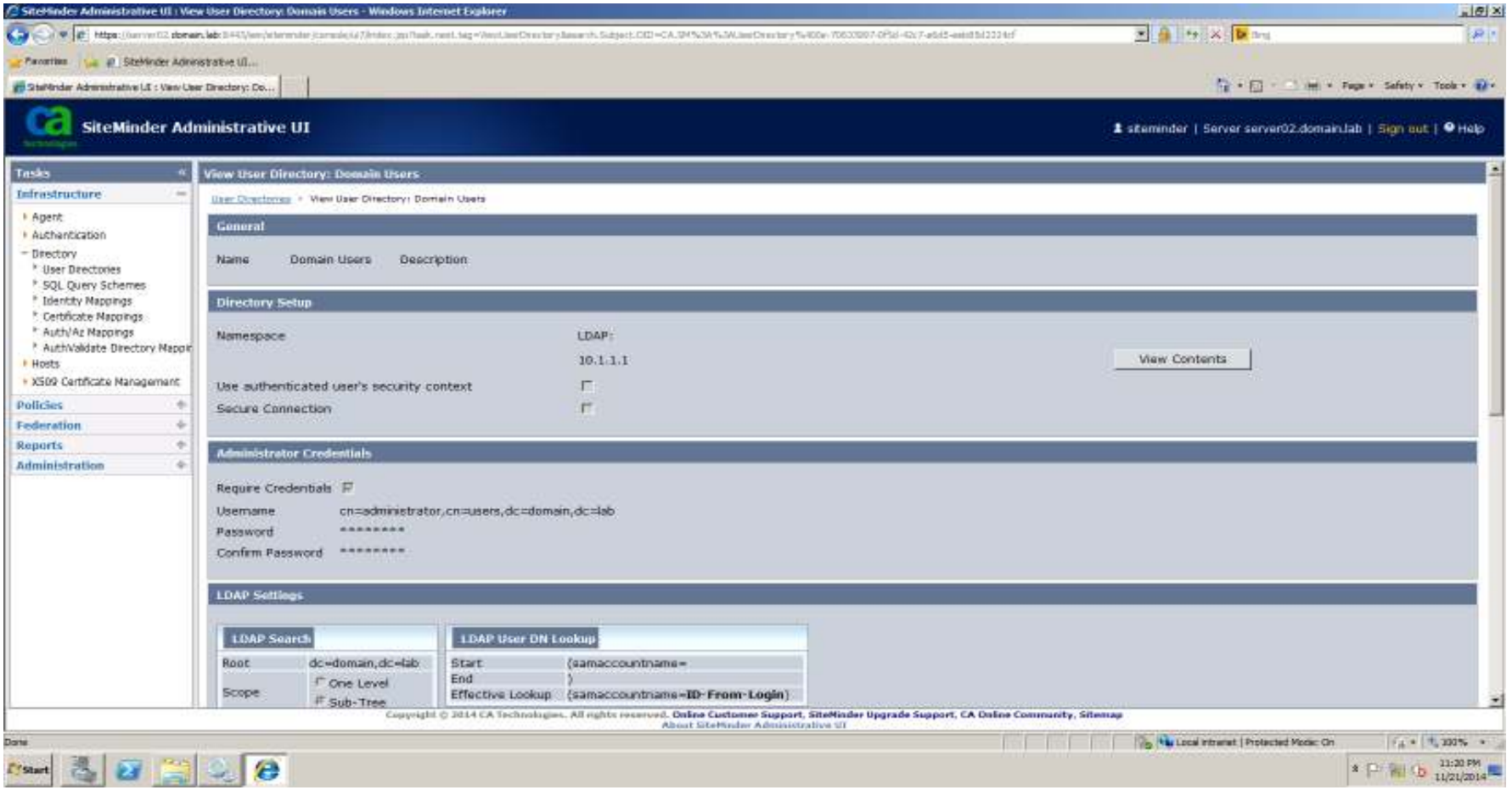
Configuration Steps – Machine #1 (KDC)

- Setup a vanilla Windows 2008 R2 Server and logged in as Administrator
- Hostname is “KDC”
- Set a static IP address (IP: 10.1.1.1, DNS: 10.1.1.1)
- Run “dcpromo” and promote to a domain controller
  - Domain Name: domain.lab
  - NetBIOS Name: DOMAIN
  - Install DNS server in this procedure
  - Reboot
- Login as DOMAIN\Administrator
- Create following domain users
  - smpsuser (check Password will not expire)
  - smwauser (check Password will not expire)
  - testuser

Configuration Steps – Machine #2 (PS)

- Setup a vanilla Windows 2008 Server and logged in as Administrator
- Hostname is “SERVER02”
- Set a static IP address (IP: 10.1.1.2, DNS: 10.1.1.1)
- Register domain
- Reboot
- Install supported 32bit JDK
- Install Policy Server (R12.52SP1)
- Reboot
- Manually configure AD as policy store(or you can choose your preferred policystore)
- Install matching version of SiteMinder AdminUI
- Verity siteminder user can logon to AdminUI
- Create AD userstore definition (Namespace does not matter, both AD or LDAP will work)

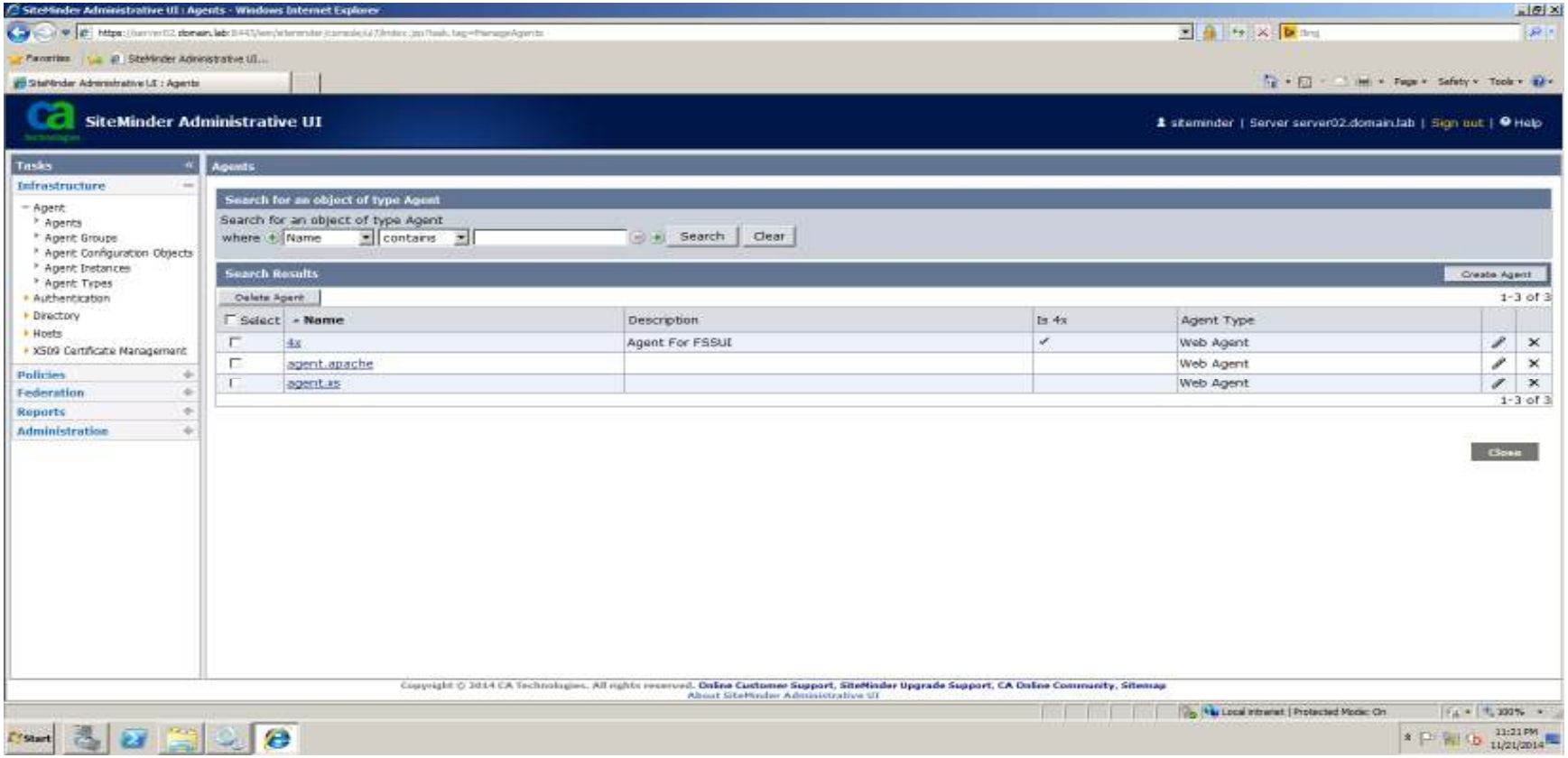
Configuration Steps – Machine #2 (PS) – cont.



ca technologies

Configuration Steps – Machine #2 (PS) – cont.

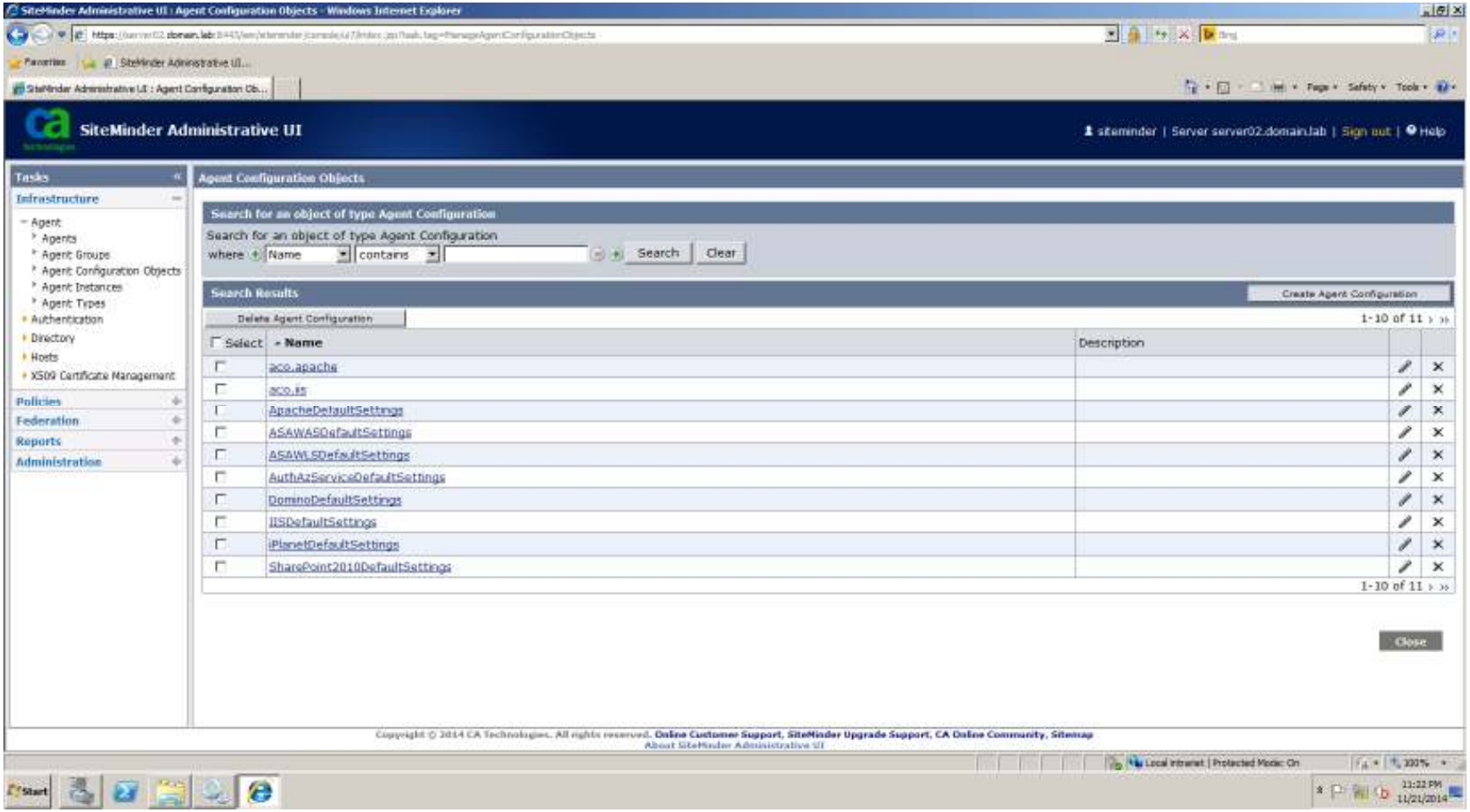
- Create agent identity as “agent.iis”



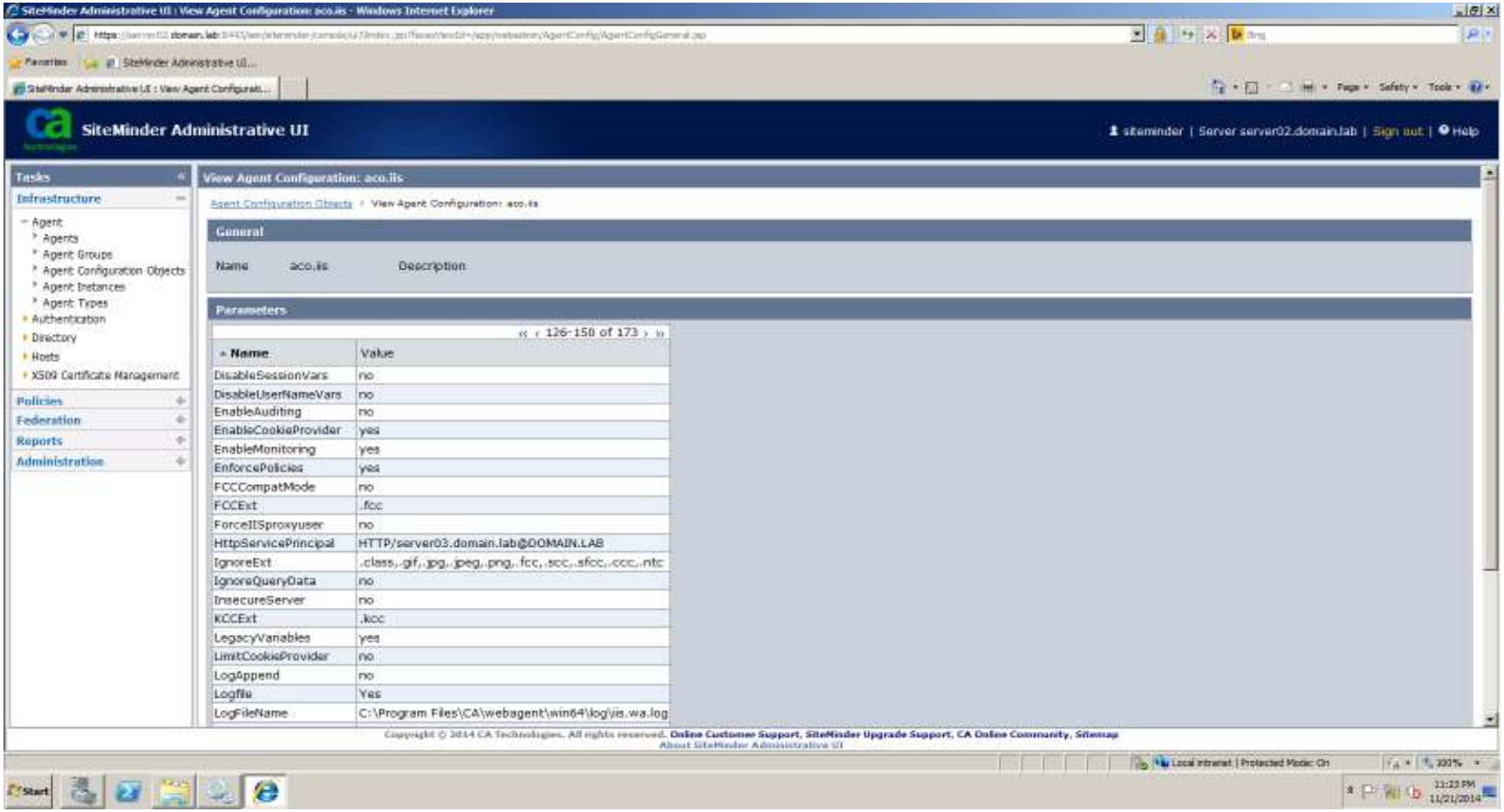
Configuration Steps – Machine #2 (PS) – cont.

- Duplicate default IIS ACO as “aco.iis” and update the following parameters
  - KCCExt: .kcc
    - You can add this to IgnoreExt
  - HttpServicePrincipal: HTTP/server03.domain.lab@DOMAIN.LAB
    - This format must be followed.
    - ServiceType is HTTP, it is case sensitive.
    - Followed by a slash to separate the FQHN of the WebAgent Server acting as the login server.
    - Followed by an @ and the Kerberos realm, this Kerberos realm MUST be in UPPER CASE.
  - SmpsServicePrincipal: smps@server02.domain.lab
    - This format must be followed.
    - This is a hardcoded name “smps”. It is not a username nor actual SPN of the smpsuser. It is not a service name. Just add “smps” as is.
    - Then followed by @ and the FQHN of the policy server that is dedicated for Kerberos authentication.

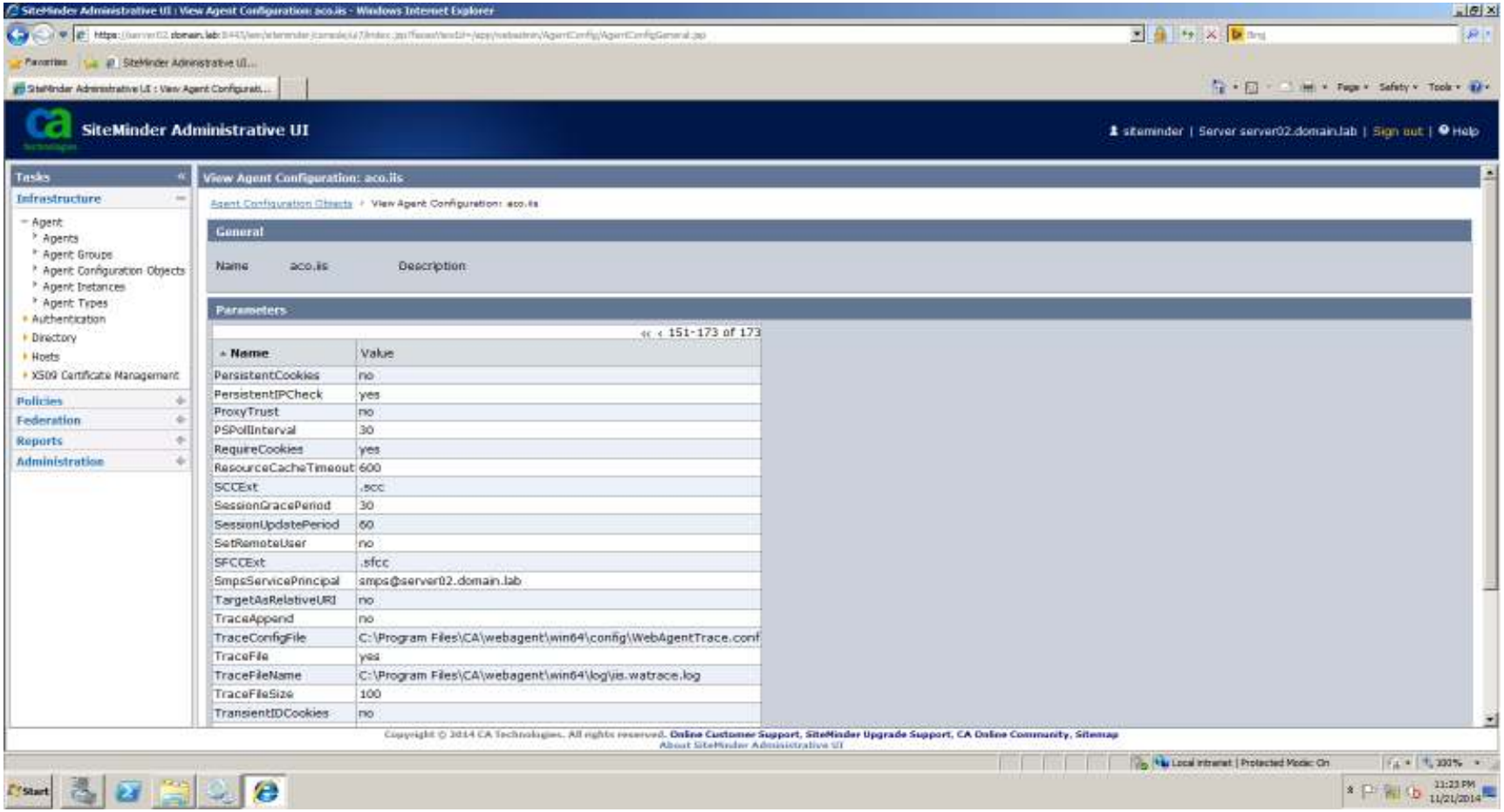
Configuration Steps – Machine #2 (PS) – cont.



Configuration Steps – Machine #2 (PS) – cont.



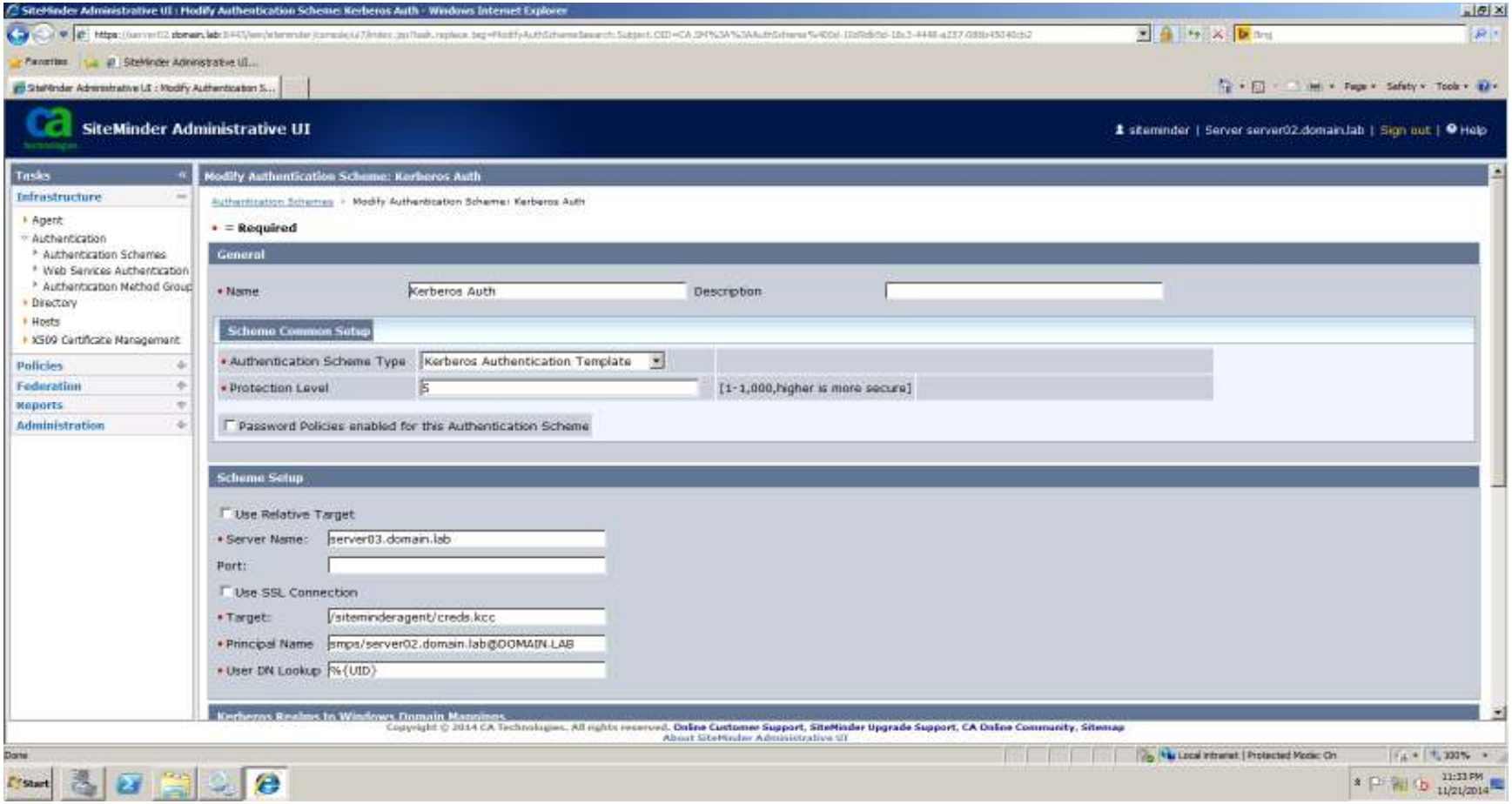
Configuration Steps – Machine #2 (PS) – cont.



Configuration Steps – Machine #2 (PS) – cont.

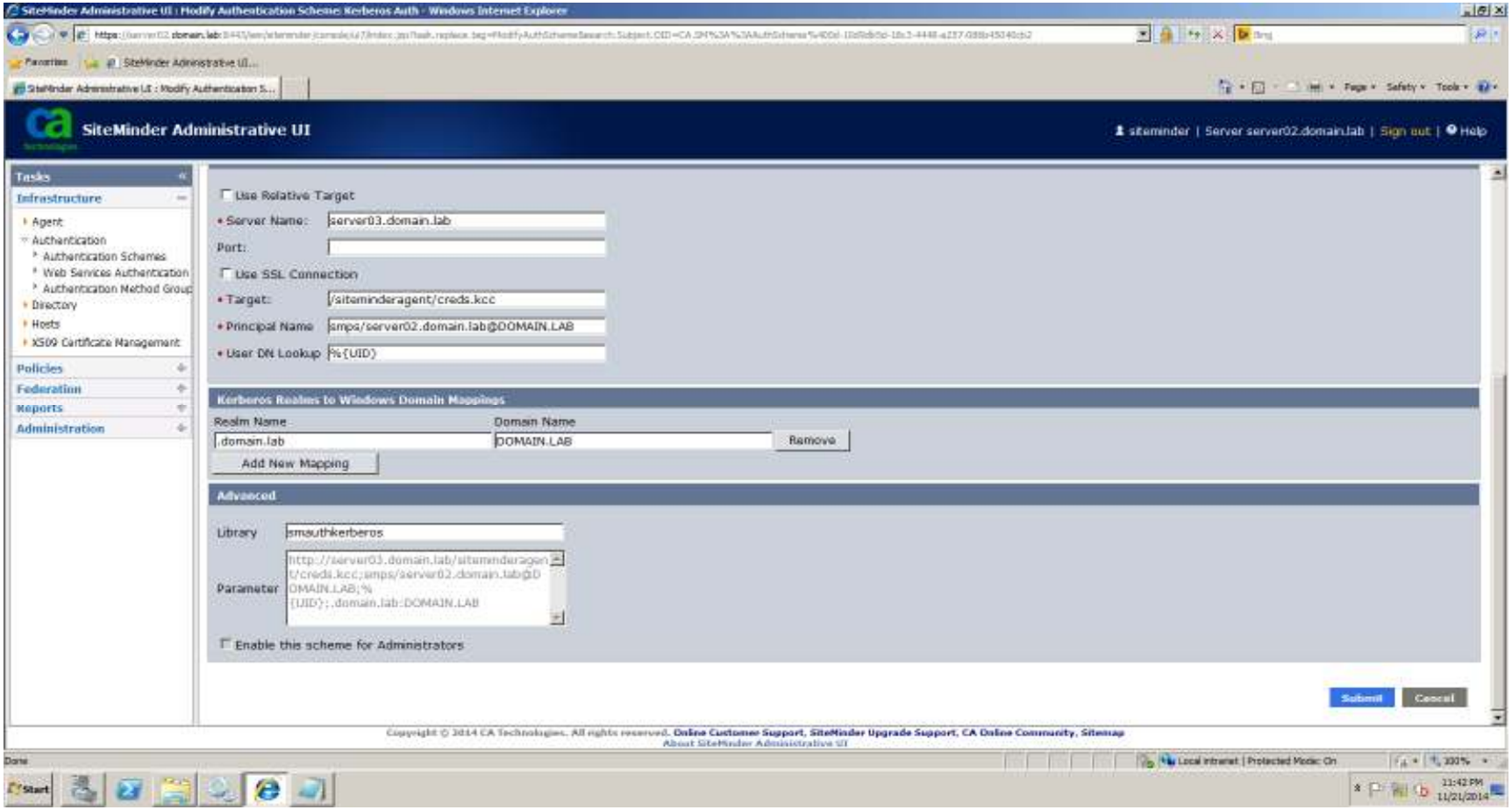
- Create HCO
- Create “Kerberos Authentication Scheme”
- Select “Kerberos Authentication Scheme” from drop down list.
- ServerName: Kerberos Login WebAgent FQHN. (server03.domain.lab)
- Target: /siteminderagent/creds.kcc
  - Do not create any virtual directory to enforce IIS native Kerberos authentication. Let the .kcc do it job. It is a virtual extension. The file does not exist.
  - However, if you do specify /<Path>/creds.kcc, you must ensure the <Path> exist and allows access, otherwise it can result in HTTP 404.
- PrincipalName: This is the actual SPN for the smpsuser followed by the Kerberos realm. (smps/server02.domain.lab@DOMAIN.LAB)
- UserDNLookup: %{UID} to fetch the userID (testuser@DOMAIN.LAB)
- Kerberos Realm to Windows Domain: .domain.lab DOMAIN.LAB
  - You may need to test this combination
- Library: smauthkerberos (leave it as is)
- Parameter: http://server03.domain.lab/siteminderagent/creds.kcc;smps/server02.domain.lab@DOMAIN.LAB;%{UID};.domain.lab:DOMAIN.LAB (It should be greyed out, leave it as is)

Configuration Steps – Machine #2 (PS) – cont.



ca technologies

Configuration Steps – Machine #2 (PS) – cont.



Configuration Steps – Machine #2 (PS) – cont.

- Create Domain, Realm(/kerberos/), Rule, Policy (or Application)

Configuration Steps – Machine #3 (WA)

- Setup a vanilla Windows 2008 Server and logged in as Administrator
- Hostname is “SERVER03”
- Set a static IP address (IP: 10.1.1.3, DNS: 10.1.1.1)
- Register domain
- Reboot
- Install IIS
- Install Web Agent
- Register Trusted host and Enable WebAgent.
- Reboot

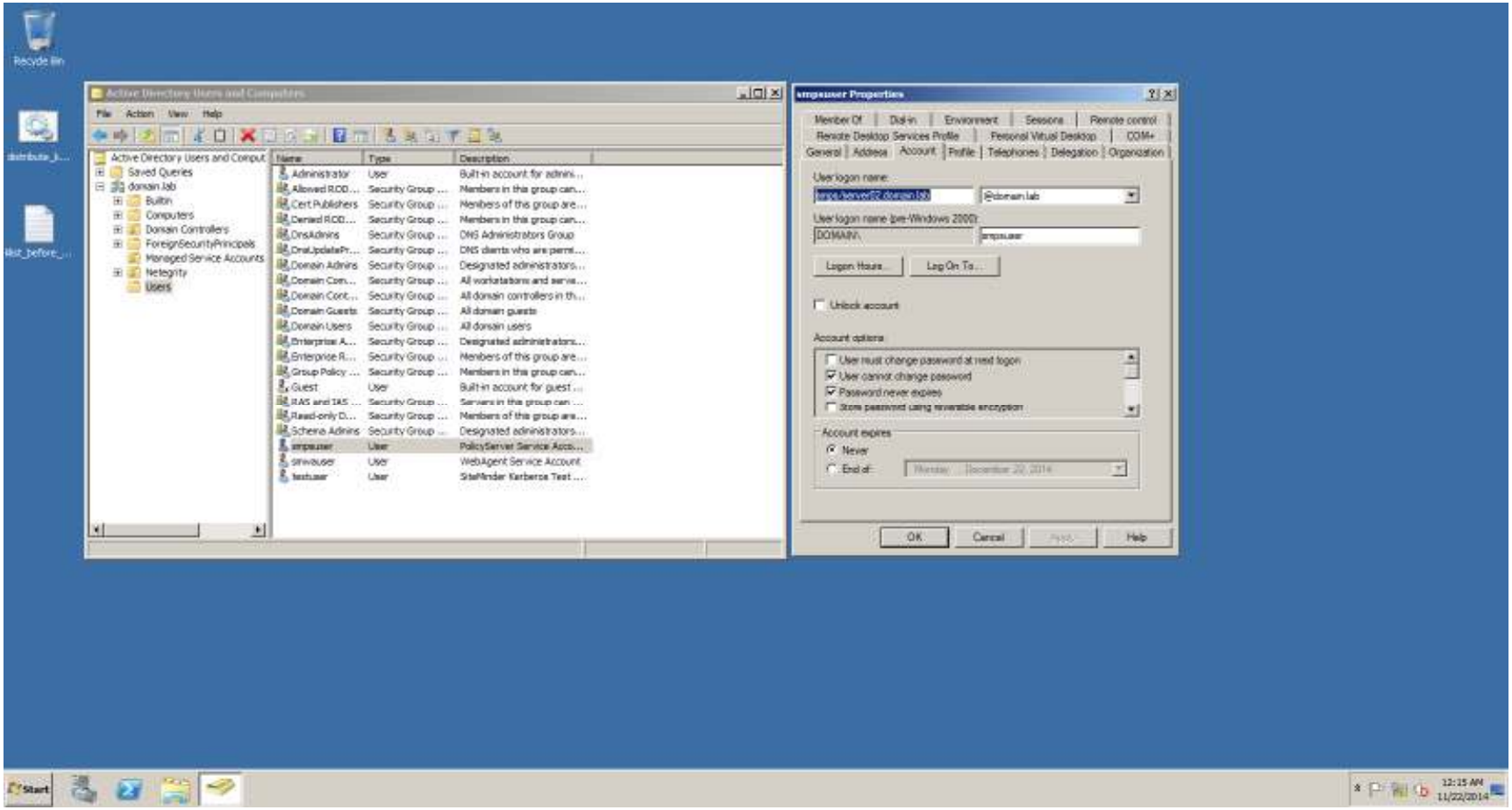
Configuration Steps – Machine #4 (DESKTOP CLIENT)

- Setup a vanilla Windows 7 and logged in as local Admin account.
- Hostname is “CLIENT”
- Set a static IP address (IP: 10.1.1.101 DNS: 10.1.1.1)
- Register domain
- Reboot
- Login as “DOMAIN\testuser”
- Open IE and register “*.domain.lab” as intranet zone.

Setup the rest of the configuration

- Go back to Machine 1 (KDC) and login as Administrator.
- Create keytab file for smpsuser
  - Following is a single line.
  - “ktpass -out smpsuser.keytab -princ smps/server02.domain.lab@DOMAIN.LAB -mapuser DOMAIN\smpsuser -mapOp set -pass Siteminder1 -crypto RC4-HMAC-NT”
  - Ex) Ktpass –out <output keytab filename> -princ <desired SPN: “smps” + “/” + “FQHN of Policy Server DNS name” + “@” + “Kerberos Domain”> –mapuser <DOMAIN\Username> … -crypto RC4-HMAC-NT
  - smpsuser’s SPN is updated as below. (screenshot at next page)

Setup the rest of the configuration

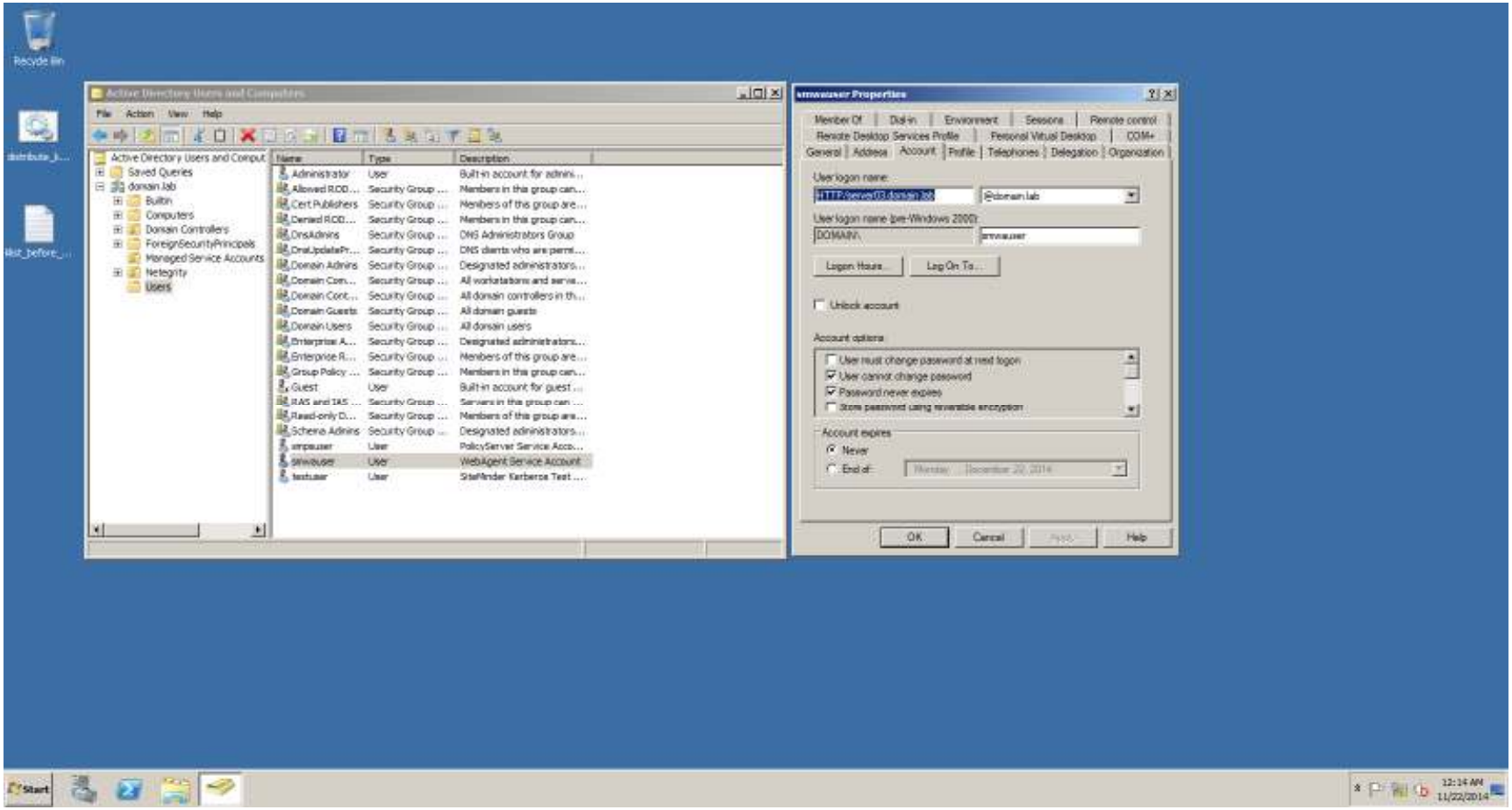


ca technologies

Setup the rest of the configuration

- Create keytab file for smwauser
  - Following is single line.
  - “ktpass -out smwauser.keytab -princ HTTP/server03.domain.lab@DOMAIN.LAB -mapuser DOMAIN\smwauser -mapOp set -pass Siteminder1 -crypto RC4-HMAC-NT”
  - smwauser’s SPN is updated as below (screenshot at next page)

Setup the rest of the configuration



ca technologies

Setup the rest of the configuration

- Create smpsuser.krb5.ini file for Machine 2(Policy Server, SERVER02)
- [libdefaults]
- default_realm = DOMAIN.LAB
- default_keytab_name = C:\WINDOWS\smpsuser.keytab
- default_tkt_enctypes = RC4-HMAC
- default_tgs_enctypes = RC4-HMAC
- [realms]
- DOMAIN.LAB = {
- kdc = kdc.domain.lab
- default_domain = domain.lab
- }
- [domain_realm]
- .domain.lab = DOMAIN.LAB

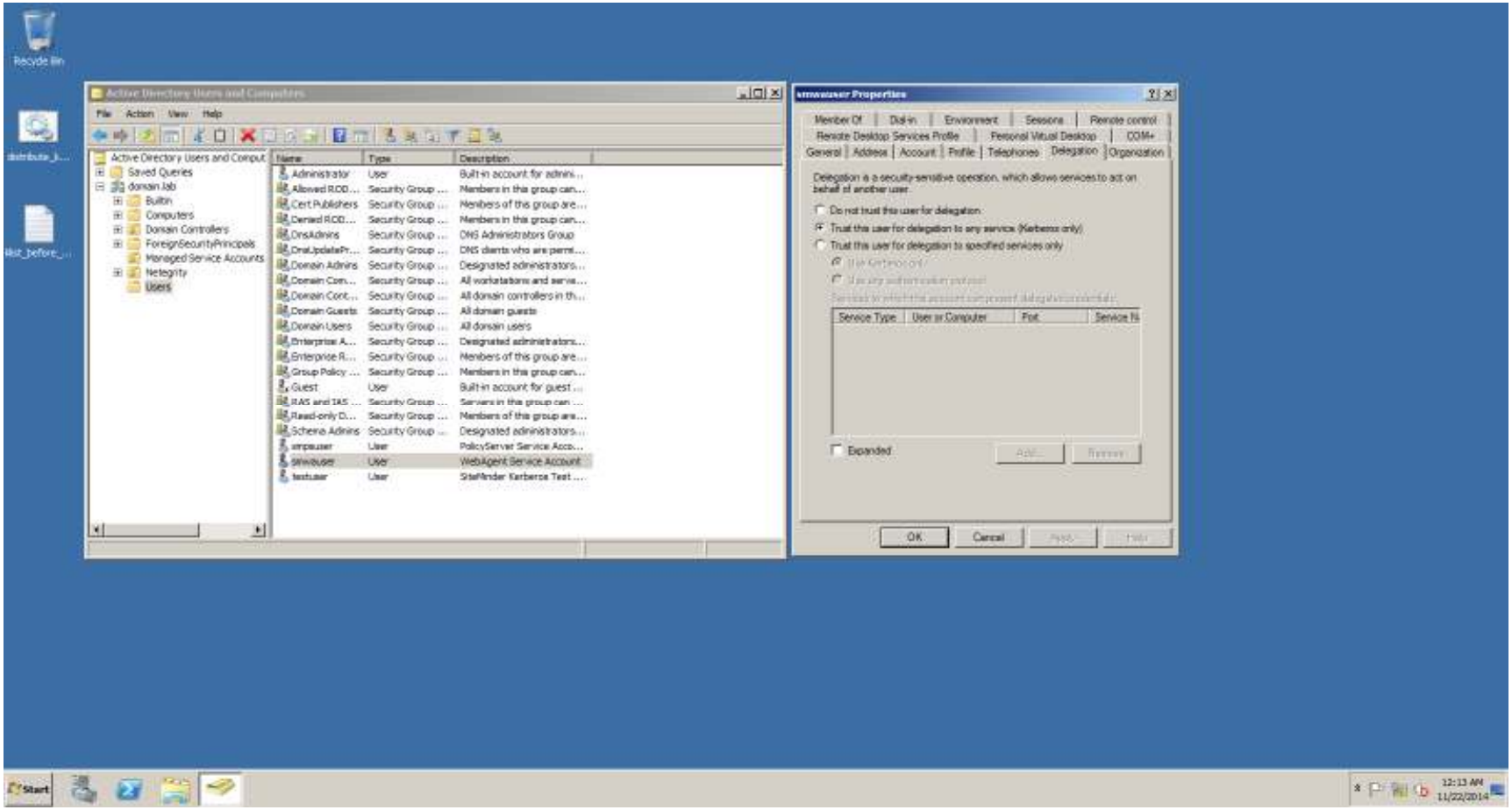
Setup the rest of the configuration

- Create smwauser.krb5.ini file for Machine 3(Web Agent, SERVER03)
- [libdefaults]
- default_realm = DOMAIN.LAB
- default_keytab_name = C:\WINDOWS\smwauser.keytab
- default_tkt_enctypes = RC4-HMAC
- default_tgs_enctypes = RC4-HMAC
- [realms]
- DOMAIN.LAB = {
- kdc = kdc.domain.lab
- default_domain = domain.lab
- }
- [domain_realm]
- .domain.lab = DOMAIN.LAB

Setup the rest of the configuration

- Copy smpsuser.keytab file to Machine 2 (C:\WINDOWS\smpsuser.keytab)
- Copy smwauser.keytab file to Machine 3 (C:\WINDOWS\smwauser.keytab)
- Copy smpsuser.krb5.ini file to Machine 2 (C:\WINDOWS\krb5.ini, note the name change)
- Copy smwauser.krb5.ini file to Machine 3 (C:\WINDOWS\krb5.ini, note the name change)
- Load “Active Directory Users and Computers” and update the smwauser’s delegation tab and select “Trust this user for delegation to any service (Kerberos only)”. (screenshot at next page)

Setup the rest of the configuration



ca technologies

Setup the rest of the configuration

- Reboot all the machines.
  - Any changes to krb5.ini file or the keytab files requires reboot of that particular machine.

Testing the setup

- Ensure the Policy Server and WebAgent services are running.
- Logon to CLIENT machine as testuser.
- Open IE and natvate to http://server03.domain.lab/kerberos/
- If you get access to the resource then check the webagent trace to confirm the user is authenticated.
- If you get basic popup challenge or HTTP 500, there is a misconfiguration.

Helpful tools

1. Microsoft Network Monitor 3.4
2. Kerberos Authentication Test Tool by Michel Barneveld
http://blog.michelbarneveld.nl/media/p/33.aspx

In case if you are using Kerberos Authentication Tool, the test url should be the http://server03.domain.lab/siteminderagent/creds.kcc?xxxx

Also, it is advisable to delete the Kerberos tokens before each test.

Misleading information

- Following are list of **misleading** information that I collected
  - IIS or its application pool must be run as the Service Account created for Kerberos
  - Policy Server must run as the Service Account created for Kerberos.
  - Policy Server Service Account must also enable delegation
  - Krb5.ini file default_keytab_name parameter on windows should have FILE:///C:/WINDOWS/krb5.ini format.
    - This prevents webagent and policy server from loading the keytab files thus fail to find the matching SPN. You would also get “File not found” error in the webagent trace log.