How to setup SiteMinder Kerberos Authentication – Part 1

Sung Hoon Kim

Date

14 January 2015



Setting up SiteMinder Kerberos Authentication



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





Machine 2: SiteMinder Policy Server

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





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





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





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





- 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)



SiteMinder Administrative UL: View	Oser Directory: Domain Users - Windows Internet	Dakrer		10 ×
🖉 🔍 🕷 https://univerti2.stores	Neb: 1947/www.internator.commule.iv/Timters.com/Tault.rentl.te	g=/weit.leeConstaryLeaverh.Subject.COI=CA.194%34%34/aarConstary%400e-708330074Pizi-4047-e545-eetethi22234rf	🗶 🔒 🦘 🗙 📴 🗠	191
Parostilles 🙀 🖉 SteMinder Admin	statie il			
StatAnder Administrative LE : Vew Use	r Directory: Do			Fage + Safety + Toole + 🔂 +
SiteMinder Adr	ninistrative UI		1 stemnder Server server02.domai	nJab Sign out • Help
Tasks -4	View User Directory: Domain Users			8
Infrastructure -	Bar Orentories + View User Directory: Domain U	1913		
Agent	General			
Brectory User Directories Sol, Daugu Schamer	Name Domain Users Description	•		
* Identity Nappings	Directory Setup			
* Cerbficate Mappings * Auth/Ag Nappings	Namanana	(DAR-		
* AuthValidate Directory Mappin		10111	View Contents	
XS02 Certificate Nanagement				
Policies	Secure Connection	r		
Federation +	Sector Chinecoory			-
Reports +	Administrative Conductive			
Administration +	Reconstruction of the second of the			
	Require Credentials			
	Usemane cn=administrator,cn=	ausers, dc=domain, dc=lab		
	Password			
	Confirm Password			
	LOAP Settlers			
	Resident Concerns. 400			
	LDAP Search	DAP User DN Lookup		
	Root dc=domain,dc=lab St	art (samaccountname=		
	Cone Level En	d)		
	Scope # Sub-Tree Ef	lective Lookup (samaccountriame=ID: From-Login)		2
	critiking in Q ad	About SiteMinder Administrative SIT	annancy, annalisy	
			No. No. Local Intranet Protected Mode: On	14 * 1000% *
Start Start				11:20 PM



Create agent identity as "agent.iis"

SiteMinder Administrative UI Age	ents - Window	es Internet Explorer				_101×
🚱 🔄 🖉 https://www.ti2.domai	n, leb: 0.447/1699/	hterender (consists 47) Index (p) Rock, lag – Manage Agen 5	= 1- 		💌 🎒 🕂 🗙 📴 Brid	PI
Parostins 🙀 🖉 SteMinder Adrie	ostatie ul					
SteMinder Administrative LE : Agents					○ · □ · □ · □ · · · · · · · · · · · · ·	Føge + Safety + Toole + 📦 +
SiteMinder Adr	ministrati	ive UI			# steminder Server server02.domai	ndab Sign out 🕈 Help
Taska -«	Agents					
Infrastructure =	STREET, DO					
Agent Search for an object of type Agent						
Apents Search for an object of type Agent Apent Groups where I Name Contains I Get Search Clear						
* Agent Configuration Objects	millere 3	Aname El concario El	Gy B			
Agent Instances	Search 6	Results				Create Agent
+ Authentication	Oelete A	Apart				1-3 of 3
+ Directory	E Select	t - Name	Description	Is 4x	Agent Type	
+ Hosts	Г	4x	Agent For FSSUL	4	Web Agent	1 ×
XSU9 Lettincate Management	Е	agent.apache			Web Agent	1 ×
Policies +	Г	agentias			Web Agent	/ X
Federation (*					100000070000	1-3 of 3
Reports						
						Los
	-	Copyright (5 3014 CA Tech	nologies, All rights reserved. Online Customer Support, SiteMin About SiteMinder Administrative Sit	der Upgrade Support, CA Daline Community, Sit	anitra ap	
All second second	n				S Local Intranat Protected Mode: On	FA * 1 300% *
('Start 🔏 🖬 🧮	2 6	Ð				* P % (b 11/21/2014





- KCCExt: .kcc
 - You can add this to IgnoreExt
- HttpServicePrincipal: <u>HTTP/server03.domain.lab@DOMAIN.LAB</u>
 - 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: <u>smps@server02.domain.lab</u>
 - 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.



harontina 🦕 🖉 SteMinder Adre SteMinder Adrenstrative Lit : Agent C	nstatie ill.		A A A A A A A A A A A A A A A A A A A		R
SteMinder Administrative LE : Agent C		Alley			
	Configuration	s., 5	0.0-34-	• Fage • Safety • Tool	a + 18
SiteMinder Ad	ministra	tive UI	1 steminder Server server02.doma	inJab Sign out 9	Help
» eke	Agent Co	enliguration Objects			
rastructure =	SPENDER OF				
Agent ¹ Agents ¹ Agent Groups ² Agent Configuration Directs	Search	for an object of type Agent Configuration ⊕ Name Contains Get Gear		_	
* Agent Instances	Search	h Results	Cr.	eate Agent Configuration	a.)
Agent Types Authentication	De	alata Agent Configuration		1-10 of 1	1
Directory	E Sele	ict + Name	Description	110.000	1
Hosts	Г	acolapache		1	×
GUY Lenncate Management	Г	8(0.15		1	×
icles +	Г	ApacheDetaultSettings		1	×
seration	Г	ASAWASDefaultSettings		1	×
norts +	Π.	ASAW, SDefaultSettings		1	×
ministration: +		AuthAzServiceDefaultSettings		1	>
	П	DominoDefaultSettings		1	>
	Г	IISDefaultSettings		1	×
	E.	PlanetDefaultSettings		1	3
	П	SharePoint2010Default5ettings		1	×
				1-10 of 1	11 0.0



SiteMinder Administra	ative UI View	w Agent Configuration: acous	- Windows Informet Explorer		E
Control Helipeting	amenti2 domain	n. 160: III - C. Verrije berender Starmale	u / Antios, an Theoretheo Dir-Yopi (netwithin Vigent Centry Vigent Centry General app		- Are
Parontine 100 (0.58	teMinder Admin	static il			
StatAndar Administrativ	e LE : Verv Age	int Configurati		🔓 • 🗇 - 🗆 Anni • Faga • Safaty •	Toola + 📦
SiteMi	nder Adı	ninistrative UI		1 stemmder Server server02.domaeulab Sign out	I 🛛 Help
Tasks	-46	View Agent Configuratio	n: aco.iis		
Infrastructure		Stant Configuration Object	View Americ Configurations, and its		
- Apent		Ballin Contractor and and			_
* Agents		General			
 Agent Groups Agent Configuration Agent Instances 	on Objects	Name aco.is	Description		
* Agent Types		Parameters			
 Authentication 			< < 126-150 of 173 > in		1
 Drectory Heate 		* Name	Vake		
 VS00 Contificatio Mar 	Stemane	Dispha Session/ars			
		Disable IserNameVars	10		
Policies		EnableAuditing	no		
Federation		EnableCookeProvider	yes		
Reports		EnableMonitoring	yes		
Administration	+	EnforcePolicies	yes		
		FCCCompatMode	no		
		FCCExt	foc		
		ForcellSproxyuser	no		
		HttpServicePrincipal	HTTP/server03.domain.lab@DOMAIN.LAB		
		IgnoreExt.	class, gif, jpg, jpeg, png, fcc, soc, afcc, ccc, ntc		
		IgnoreQueryData	no.		
		InsecureServer	no		
		KCCExt	.koc		
		Legacy/Variables	yes		
		LimitCookieProvider	no		
		LogAppend	10		
		Logfile	Yes		
		LogFileName	C:\Program Files\CA\webagent\win64\kog\iis.wa.log		
			Copyright () 3014 CA Technologies, All rights reserved. Online Customer Support, SiteMinder About Statigues Administration ST	Upgrade Support, CA Daline Community, Sitemap	_
		10		🖓 🖓 Local Intranet Protected Mode: On 🛛 🖓 🔹	, 333% *
	1 9.5	100 100			11:23 PM
Start Car Ca				x 1- MI (D	11/21/2014



- C + the https://w	marti2 domain	labelli - Allen Antonio de Carrado	147 Entire an Finant/section Association / Association for Association for General and		(p)
Contraction of the second					1421
Parontine he # Sty	erinder Admini	static ul			a sa
Staffinder Adventitative	LE : Very Agen	nt Configurati		B.D.O.M.	Føge + Safety + Toole + 🖬
SiteMin	ider Adn	ninistrative UI		1 steminder Server server02.domain	Jab Sign out 🕈 Help
Tasks	4	View Agent Configuratio	m: aco.iis		
Infrastructure		Agent Configuration Object	View Apent Configuration: eco.4s		
- Agent		EPROPERTY.			
Agents		General			
* Agent Groups * Agent Configuration * Agent Instances	n Objects	Name aco,is	Description		
* Agent Types		Parameters			
Authentication			er < 151-173 of 173		1
- Deeccory		+ Name	Value		
 x500 Certificate Marc 	atemant	PersistentCockies	00		
		PersistentIPCheck	ves		
Policies		ProxyTrust	10		
Federation		PSPollinterval	30		
Reports		RequireCookies	yes		
Administration	+	ResourceCacheTimeou	it 600		
		SCCExt	.50C		
		SessionGracePeriod	30		
		SessionUpdatePeriod	60		
		SetRemoteUser	ne		
		SFCCExt	sfcc		
		SmpsServicePrincipal	smps@server02.domain.lab		
		TargetAsRelativeURI	no		
		TraceAppend	no		
		TraceConfigFile	C:\Program Files\CA\webagent\win64\config\WebAgentTrace.conf		
		TraceFile	yes		
		TraceFileName	C:\Program Files\CA\webagent\win64\log\is.watrace.log		
		TraceFileSize	100		
		TransientIDCookies	10		
	11		Coupyright () 3014 CA Technologies, All rights reserved. Online Customer Support, SiteMinder Upgrade	Support, CA Daline Community, Sitemap	
			Nexus and the second se	Se Ha Local Intranet Protected Mode: On	Fa . 1, 200% .
	1 9.5	10 CA			11:22 PM
Start 🔄 🛃		- C			A 11/21/2014





- 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 (<u>testuser@DOMAIN.LAB</u>)
- 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)



COV It https://www.clip.covar	n, bebe 10.4477/som /schernmister (Carmisio, 6477/status, 2001	haik, replace, beg «Plottfy-AuthScheme Texas ch. Subject. Of	D =CA_294%3A%2AAutr5d1eeus%4R0d; D3Rd63c-18c2-4448-4237-038643340;52		[P	
Starfinder Administrative LE : Modify A	erarse ul			\$.0·□	Fuge + Safety + Tools + 👔	
SiteMinder Adr	ninistrative UI			1 steminder Server server02.dom	indati (Sign out (🔍 Help	
Tasks «	Nodily Authentication Scheme: Ke	rboros Auth				
Infrastructure -	Authentitation Schemes + Modify Auth	entitation Scheme: Kerberox Auth				
I Agent	• = Required					
* Authentication Schemes	General					
 Web Services Authentication Authentication Method Group Directory 	• Name	Cerberos Auth	Description			
Hosts X509 Cartificate Nanagement	Scheme Common Setup					
Policies +	Authentication Scheme Type	Kerberos Authentication Template				
Federation +	Protection Level	ß	[1-1,000,higher is more secure]			
Administration +	Password Policies enabled for	this Authentication Scheme				
	Scheme Setup					
	Use Relative Target					
	• Server Name: server03.dom	ain.lab				
	Port:					
	Use SSL Connection					
	•Target: //siteminderag	ent/creds.kcc				
	Principal Name smps/server0	2.domain lab@OOMAIN LAB				
	• User DN Lookup (%(UID)					
	Kerberns Realins In Windows Dr	unain Manalines. Add © 2014 CA Technologies, All eghts receiver	. Online Customer Support, SiteMinder Upgrade Support, CA Online Communit	y, Silemay		
ne	(c.c.)		About SiteMindar Administrative SI	Die Ne Local intranet Protected Moder Cr	1 14 1 2005	
and the second sec					1. H L L L L L L L L L L L L L L L L L L	



Site and evaluates to allow 01 1 Hoo	INTY AND CHURCHEN INCOME INTERIOS AND A WHOMAS DREPHER LIGHTER		210
Cale It Https://www.calesa	A MD 144 (very thermale samples) / Index applicating #RadhyAuthOnered assert: Subject CD #A 24%24% NauthOnered %#Corl (1898) 55-18.3 4444 4277		194
Carontina Vie @ Steffinder Admin	statie II	Bue course	and the second
StaPinder Adversitrative LE : Modify A	utheritation 5	N.D. Ser.	ege · Safety · Toos · U
SiteMinder Adr	ministrative UI	1 steminder Server server02.domain.	lab Sign out 🕈 Help
rasks «			
mfrastructure -	Lise Relative Target		
Agent Alebantication	Server Name: server03.domain.lab		
* Authentication Schemes	Port:		
* Web Services Authentication * Authentication Method Group	Use SSL Connection		
Directory	Target: //siteminderagent/creds.kcc		
Hosts	* Principal Name smps/server02.domain.lab@DOMAIN.LAB		
talicies de	• User DN Lookup (% (UID)		
ederation +			
teports +	Kerberos Reales to Windows Domain Mappings		
Administration +	Realm Name Domain Name Reprinted		
	Add New Macong		
	Advanced		
	Library smauthkerberos		
	http://iarvur03.domain.lab/ulturinduragen		
	Voreda.kccjumps/server02.domain.tabigt0		
	(UID);.domain.lab.DOMAIN.LAB		
	Frank all shows to the second		
	· Endle dis sciene in Automodativs		
			Contraction of the local division of the loc
			abmil Cescul
	Copyright () 3014 CA Technologies, All rights reserved. Online Cuctomer Support, SteMinder Upgrade Support, C About SteMinder Administrative ST	A Online Community, Sitemap	
E grander of the second se		Second Interest (Protected Mode: On	Fil + 1, 200% +
	Name and American A American American Am		



 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.





- 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)



Active Directory Users and Cam	pattes	Ampenant Properties 21×1
	IS NEW AND TON	Menter Of Did-in Environment Sessons Pentoe commit
Active Directory Users and Comput B Saved Queries B dama. Nab H B Baitin H C Builtin H C Donisin Controllers H C DONIS H C	Name Type Description Administrator User Bult in account for athms	General Addresi Abourt Perific Telephones Delegation Organization User logon name Bardiacoscientation Pedomaniads Pedomaniad
× ×		OK Cercal Heb





- 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)



Action Unrectory Uters and Care Ne Actor Vew Help		Al C X Menter Of Dal in Environment Sensoria Periode control
Active Directory Users and Comput Served Queries Served Queries Biological	Name Type Description Administratory Use Built account for administratory Administratory Use Built account for administratory Cert Publichers Security Group Members in the group care Cert Publichers Security Group Members in the group care Cert Publichers Security Group Members in the group care Constructions Security Group Otto deministratory Group Oreadpalaters Security Group Otto deministratory Comen Core Security Group All domain corribules in th Comen Core Security Group All domain parent Corean Core Security Group Members in the group care Corean Core Security Group Members in the group care Corean Core Security Group Members of this	Herade Decision Services Profile Precision Visual Decision COMM General J. Addess Account [Prufile] Telephones] Decision] Organization User logon name Image: Communication User hours Image: Communication User hours Image: Communication Wer name Image: Communication Memory Televier End off Televier
<u>× </u>		OK Gercel Neb





- [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





- [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





- 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)



Active Unrefore Unread Cam	polities	Ammalaner Properties
Pile Action View Help Image: Action Image: Action Image: Action Image: Action	Name Type Description Administrator User Built in account for admin Administrator User Built in account for admin Administrator Security Group Members in the group arc Constructions Security Group Members in the group arc Constructions Security Group ONS Administrators Group Constructions Security Group ONS Administrators Group Constructions Security Group ONS Administrators Group Constructions Security Group Administrators and server Constructions Security Group Ministrators and server Constructions Security Group Ministrators Constructions Security Group Ministrators	Hender IV Datin Environment Sessons Periode control Hender Destings Services Profile Periode Unital Desting COHe General Addees Account Fulle Telephanes Delspition Organization Delspition is a security sensitive operation, which allows services to act on before user Diversities affect delegation is any services (Nathema only) That this user for delegation is any services (Nathema only) That this user for delegation is any services (Nathema only) That this user for delegation is any services (Nathema only) That this user for delegation is any services (Nathema only) That this user for delegation is any services (Nathema only) That this user for delegation is any services (Nathema only) That this user for delegation is any services (Nathema only) That this user for delegation is any services (Nathema only) That this user for delegation is any services (Nathema only) That this user for delegation is any services (Nathema only) That this user for delegation is any services (Nathema only) That this user for delegation is any services (Nathema only) That this user for delegation is any services (Nathema only) That this user for delegation is any services (Nathema only) That this user for delegation is any services (Nathema only) That this user for delegation is any services (Nathema only) That this user for delega
<u>x</u>	Stathaer User Stafferder Earberts Test	OK Cercel rec





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



Testing the setup



- Logon to CLIENT machine as testuser.
- Open IE and nativate to <u>http://server03.domain.lab/kerberos/</u>
- 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 <u>http://server03.domain.lab/siteminderagent/creds.kcc?xxxx</u> 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
 <u>FILE:///C:/WINDOWS/krb5.ini</u> 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.

